I

(Wetgevingshandelingen)

VERORDENINGEN

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

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van de Europese Centrale Bank ([1]),

Gezien het advies van het Europees Economisch en Sociaal Comité ([2]),

Handelend volgens de gewone wetgevingsprocedure ([3]),

Overwegende hetgeen volgt:

(1) In het digitale tijdperk ondersteunt informatie- en communicatietechnologie (ICT) complexe systemen die worden gebruikt voor dagelijkse activiteiten. ICT houdt belangrijke sectoren van onze economie draaiende, waaronder de financiële sector, en verbetert de werking van de interne markt. Meer digitalisering en onderlinge verwevenheid vergroten ook het ICT-risico, waardoor de samenleving als geheel, en het financiële stelsel in het bijzonder, kwetsbaarder wordt voor cyberdreigingen of ICT-verstoringen. Hoewel het alomtegenwoordige gebruik van ICT-systemen en een hoge mate van digitalisering en connectiviteit tegenwoordig belangrijke kenmerken zijn van de activiteiten van financiële entiteiten in de Unie, moet hun digitale weerbaarheid nog beter worden aangepakt en in hun ruimere operationele kaders worden ingebouwd.

(2) Het gebruik van ICT heeft in de afgelopen decennia een centrale rol gekregen in de verlening van financiële diensten, zodat ICT nu van cruciaal belang is voor de werking van typische dagelijkse functies van alle financiële entiteiten. Digitalisering komt tegenwoordig onder andere naar voren bij bijvoorbeeld betalingen, die steeds minder met op contant geld en papier gebaseerde methoden plaatsvinden en steeds vaker met behulp van digitale oplossingen plaatsvinden, alsook effectenclearing en -afwikkeling, elektronische en algoritmische handel, lenings- en financieringsverrichtingen, peer-to-peerfinanciering, kredietbeoordeling, schadebeheer en backofficeverrichtingen.

([1]) PB C 343 van 26.8.2021, blz. 1.
([2]) PB C 155 van 30.4.2021, blz. 38.
([3]) Standpunt van het Europees Parlement van 10 november 2022 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 28 november 2022.

De verzekeringssector is ook getransformeerd door het gebruik van ICT-technologie, van de opkomst van verzekeringstussenpersonen die met InsurTech werken en hun diensten online aanbieden tot het digitaal afsluiten van verzekeringen. Niet alleen is het geldwezen in de hele sector grotendeels digitaal geworden, maar digitalisering heeft ook gezorgd voor sterkere onderlinge verbanden en afhankelijkheden binnen de financiële sector en met derde aanbieders van infrastructuur en diensten.

(3) Het Europees Comité voor systeemrisico's (ESRB) heeft in een in 2020 uitgebracht verslag over systemisch cyberrisico bevestigd hoe de bestaande hoge mate van verwevenheid tussen financiële entiteiten, financiële markten en financiëlemarktinfrastructuren, en met name de onderlinge afhankelijkheid van hun ICT-systemen, een systeemkwetsbaarheid zou kunnen vormen, omdat lokale cyberincidenten zich snel van elk van de ongeveer 22 000 financiële entiteiten van de Unie zouden kunnen verspreiden naar het gehele financiële stelsel, niet gehinderd door geografische grenzen. Ernstige ICT-inbreuken die zich in de financiële sector voordoen, hebben niet alleen gevolgen voor afzonderlijke financiële entiteiten. Zij begunstigen ook de verspreiding van lokale kwetsbaarheden via de financiële transmissiekanalen en kunnen negatieve gevolgen voor de stabiliteit van het financiële stelsel van de Unie meebrengen, waaronder liquiditeitsruns en een algeheel verlies van vertrouwen in de financiële markten.

(4) De laatste jaren hebben internationale, uniale en nationale beleidsmakers, toezichthouders en normalisatie-instellingen zich beziggehouden met het ICT-risico en is geprobeerd de digitale weerbaarheid te vergroten, normen vast te stellen en regelgevings- of toezichtwerkzaamheden te coördineren. Op internationaal niveau streven het Bazels Comité voor bankentoezicht, het Comité betalingen en marktinfrastructuur, de Raad voor financiële stabiliteit, het Financial Stability Institute en de G-7 en G20 ernaar de bevoegde autoriteiten en marktdeelnemers in verschillende rechtsgebieden te voorzien van instrumenten om de weerbaarheid van hun financiële stelsels te verbeteren. Die werkzaamheden zijn ook ingegeven door de noodzaak om terdege rekening te houden met het ICT-risico in de context van een onderling zeer sterk verbonden mondiaal financieel stelsel en om te streven naar meer consistentie van relevante beste praktijken.

(5) Ondanks gerichte uniale en nationale beleids- en wetgevingsinitiatieven blijft het ICT-risico een uitdaging vormen voor de operationele weerbaarheid, prestaties en stabiliteit van het financiële stelsel van de Unie. De hervormingen die op de financiële crisis van 2008 volgden, hebben in de eerste plaats de financiële weerbaarheid van de financiële sector van de Unie versterkt en hadden als doel het concurrentievermogen en de stabiliteit van de Unie te waarborgen uit economisch, prudentieel en marktgedragsoogpunt. Hoewel ICT-beveiliging en digitale weerbaarheid deel uitmaken van operationeel risico, hebben zij in de regelgevingsagenda na de financiële crisis minder aandacht gekregen en zijn ze alleen op sommige gebieden van het financiëledienstenbeleid en het regelgevingslandschap van de Unie ontwikkeld, of slechts in een paar lidstaten.

(6) In haar mededeling van 8 maart 2018 met als titel "FinTech-actieplan: voor een meer concurrerende en innovatieve Europese financiële sector", benadrukte de Commissie dat het van het grootste belang is de financiële sector van de Unie weerbaarder te maken, onder andere vanuit operationeel oogpunt, om te zorgen voor de technologische veiligheid en goede werking ervan en voor een snel herstel van ICT-inbreuken en -incidenten, zodat uiteindelijk financiële diensten in de hele Unie doeltreffend en vlot kunnen worden verricht, ook in stresssituaties, terwijl het vertrouwen van consumenten en markten behouden blijft.

(7) In april 2019 hebben de Europese toezichthoudende autoriteit (Europese Bankautoriteit) (EBA) opgericht bij Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([4]), de Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen) (Eiopa) opgericht bij Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([5]) en de Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten) (ESMA) opgericht bij Verordening (EU) nr. 1095/2010 van het Europees

([4]) 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).

([5]) 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).

Parlement en de Raad ([6]) (gezamenlijk bekend als "Europese toezichthoudende autoriteiten" of "ETA's") gezamenlijk technische adviezen uitgebracht waarin werd opgeroepen tot een samenhangende aanpak van het ICT-risico in de financiële sector en werd aanbevolen om op evenredige wijze de digitale operationele weerbaarheid van de financiëledienstensector te versterken door middel van een sectorspecifiek initiatief van de Unie.

(8) De financiële sector van de Unie wordt gereglementeerd door een gemeenschappelijk rulebook en is onderworpen aan een Europees systeem van financieel toezicht. Niettemin zijn de bepalingen inzake digitale operationele weerbaarheid en ICT-beveiliging nog niet volledig of consistent geharmoniseerd, hoewel digitale operationele weerbaarheid cruciaal is voor de financiële stabiliteit en marktintegriteit in het digitale tijdperk, en niet minder belangrijk is dan bijvoorbeeld gemeenschappelijke prudentiële of marktgedragsnormen. Het gemeenschappelijk rulebook en het toezichtsysteem moeten daarom ook voor digitale operationele weerbaarheid worden ontwikkeld, door de mandaten van de bevoegde autoriteiten te versterken om hen in staat te stellen toezicht te houden op het beheer van het ICT-risico in de financiële sector, teneinde de integriteit en efficiëntie van de interne markt te beschermen en de ordelijke werking ervan te vergemakkelijken.

(9) Verschillen in wetgeving en ongelijke nationale regelgevings- of toezichtsbenaderingen met betrekking tot het ICT-risico leiden tot obstakels voor de werking van de interne markt voor financiële diensten die de vlotte uitoefening van de vrijheid van vestiging en het verlenen van diensten belemmeren voor financiële entiteiten die grensoverschrijdend actief zijn. De concurrentie tussen hetzelfde type financiële entiteiten in verschillende lidstaten zou ook kunnen worden verstoord. Dit is in het bijzonder het geval op gebieden waar de harmonisatie op Unieniveau zeer beperkt is gebleven, zoals bij het testen van de digitale operationele weerbaarheid, of geheel ontbreekt, zoals bij het monitoren van het ICT-risico van derde aanbieders. Verschillen als gevolg van geplande ontwikkelingen op nationaal niveau zouden verdere belemmeringen voor de werking van de interne markt meebrengen, ten nadele van de marktdeelnemers en de financiële stabiliteit.

(10) Doordat ICT-risico tot nu toe slechts ten dele op Unieniveau is aangepakt, bestaan op belangrijke gebieden — zoals het melden van ICT-gerelateerde incidenten en het testen van digitale operationele weerbaarheid — lacunes of overlappingen, alsook inconsistenties als gevolg van uiteenlopende nationale regels of kosteninefficiënte toepassing van overlappende regels. Dit is met name nadelig voor een ICT-intensieve gebruiker als de financiële sector, aangezien technologische risico's zich niet door grenzen laten tegenhouden en de financiële sector zijn diensten op brede grensoverschrijdende schaal binnen en buiten de Unie verleent. Individuele financiële entiteiten die grensoverschrijdend actief zijn of over meerdere vergunningen beschikken (een financiële entiteit kan bijvoorbeeld vergunningen als bank, als beleggingsonderneming en als betalingsinstelling hebben die elk zijn afgegeven door verschillende bevoegde autoriteiten in een of meer lidstaten) hebben te maken met operationele uitdagingen wanneer zij zelf op samenhangende en kosteneffectieve manier het ICT-risico moeten aanpakken en de negatieve gevolgen van ICT-incidenten moeten beperken.

(11) Aangezien het gemeenschappelijk rulebook niet vergezeld ging van een uitgebreid kader voor ICT- of operationeel risico, is verdere harmonisatie van essentiële vereisten inzake digitale operationele weerbaarheid voor alle financiële entiteiten geboden. Indien financiële entiteiten op basis van die essentiële vereisten hun ICT-capaciteiten en algehele weerbaarheid opbouwden om operationele storingen te weerstaan, zou dit helpen om de stabiliteit en integriteit van de financiële markten van de Unie te behouden en aldus bijdragen tot het waarborgen van een hoog niveau van bescherming van beleggers en consumenten in de Unie. Aangezien deze verordening beoogt bij te dragen tot de vlotte werking van de interne markt, moet zij gebaseerd zijn op de bepalingen van artikel 114 van het Verdrag betreffende de werking van de Europese Unie ("VWEU"), geïnterpreteerd in overeenstemming met de vaste rechtspraak van het Hof van Justitie van de Europese Unie ("Hof van Justitie").

(12) Deze verordening is gericht op het consolideren en verbeteren van de vereisten inzake ICT-risico die deel uitmaken van de vereisten inzake operationeel risico, en welke tot dusver afzonderlijk zijn behandeld in verschillende rechtshandelingen van de Unie. Hoewel de belangrijkste categorieën financiële risico's (bv. kredietrisico, marktrisico, tegenpartijkredietrisico en liquiditeitsrisico, marktgedragrisico) in die rechtshandelingen aan bod kwamen, werden ten tijde van de vaststelling ervan niet alle componenten van operationele weerbaarheid behandeld. In de regels inzake operationeel risico die in die rechtshandelingen van de Unie verder zijn uitgewerkt, is vaak gekozen voor een traditionele kwantitatieve aanpak van risico's (namelijk de vaststelling van een kapitaalvereiste om het ICT-risico te

([6]) 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).

dekken), in plaats van gerichte kwalitatieve regels voor bescherming, opsporing, inperking, herstel en reparatie bij ICT-gerelateerde incidenten of voor capaciteit inzake rapportage en digitale tests. Die handelingen waren in de eerste plaats bedoeld om essentiële regels inzake prudentieel toezicht, marktintegriteit of marktgedrag vast te stellen en deze bij te werken. Door de verschillende regels inzake ICT-risico te consolideren en bij te werken, zouden alle bepalingen met betrekking tot digitaal risico in de financiële sector voor de eerste keer op consistente wijze in één wetgevingshandeling moeten worden samengebracht. Deze verordening vult dus leemten op in sommige van de eerdere rechtshandelingen of neemt inconsistenties daarin weg, ook wat betreft de daarin gebruikte terminologie, en verwijst expliciet naar ICT-risico door middel van gerichte regels inzake ICT-risicobeheercapaciteiten, rapportage van incidenten, tests van de operationele weerbaarheid en bewaking van het ICT-risico van derde aanbieders. Deze verordening moet dus ook het bewustzijn inzake het ICT-risico vergroten en erkennen dat ICT-incidenten en een gebrek aan operationele weerbaarheid de gezondheid van financiële entiteiten in gevaar kunnen brengen.

(13) Financiële entiteiten moeten, rekening houdend met hun omvang en algeheel risicoprofiel en de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen, dezelfde benadering en dezelfde op beginselen gebaseerde regels volgen wanneer zij ICT-risico aanpakken. Consistentie draagt bij tot een groter vertrouwen in het financiële stelsel en tot het behoud van de stabiliteit ervan, met name in tijden van grote afhankelijkheid van ICT-systemen, -platforms en -infrastructuren, waardoor het digitale risico stijgt. De inachtneming van elementaire cyberhygiëne kan ook grote schade voor de economie voorkomen door de gevolgen en kosten van ICT-verstoringen tot een minimum te beperken.

(14) Een verordening helpt de complexiteit van de regelgeving te verminderen, bevordert de convergentie van het toezicht en vergroot de rechtszekerheid, en draagt ook bij tot het beperken van de nalevingskosten, vooral voor financiële entiteiten die grensoverschrijdend actief zijn, en tot het verminderen van concurrentieverstoringen. Voor de vaststelling van een gemeenschappelijk kader voor de digitale operationele weerbaarheid van financiële entiteiten kan daarom het best een verordening worden gekozen om te zorgen voor een homogene en coherente toepassing van alle componenten van het ICT-risicobeheer door de financiële sector van de Unie.

(15) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([7]) was het eerste horizontale kader voor cyberbeveiliging dat op Unieniveau werd vastgesteld en dat ook van toepassing is op drie soorten financiële entiteiten, namelijk kredietinstellingen, handelsplatformen en centrale tegenpartijen. Aangezien Richtlijn (EU) 2016/1148 voorziet in een mechanisme voor de identificatie op nationaal niveau van aanbieders van essentiële diensten, werden echter alleen bepaalde door de lidstaten geïdentificeerde kredietinstellingen, handelsplatformen en centrale tegenpartijen in de praktijk binnen het toepassingsgebied ervan gebracht zodat zij moeten voldoen aan de daarin vastgestelde vereisten inzake ICT-beveiliging en melding van incidenten. Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([8]) stelt een uniform criterium vast om te bepalen welke entiteiten binnen het toepassingsgebied ervan vallen (size-capregel) en behoudt ook de drie soorten financiële entiteiten binnen dat toepassingsgebied.

(16) Aangezien deze verordening het niveau van harmonisatie van de verschillende onderdelen van digitale weerbaarheid verhoogt door vereisten inzake ICT-risicobeheer en rapportage van ICT-gerelateerde incidenten in te voeren die strenger zijn dan die welke in het huidige Unierecht inzake financiële diensten zijn opgenomen, komt dit hogere niveau echter ook neer op een grotere harmonisatie in vergelijking met de vereisten van Richtlijn (EU) 2022/2555. Deze verordening is dus een *lex specialis* ten opzichte van Richtlijn (EU) 2022/2555. Tegelijkertijd is het cruciaal om een sterke relatie tussen de financiële sector en het thans in Richtlijn (EU) 2022/2555 vastgelegde horizontale cyberbeveiligingskader van de Unie te handhaven, teneinde te zorgen voor samenhang met de door de lidstaten ingevoerde cyberbeveiligingsstrategieën, en financiële toezichthouders te kunnen wijzen op cyberincidenten die gevolgen hebben voor de andere sectoren die onder die Richtlijn vallen.

([7]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

([8]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (zie bladzijde 80 van dit Publicatieblad).

(17) Overeenkomstig artikel 4, lid 2, van het Verdrag betreffende de Europese Unie en onverminderd de rechterlijke toetsing door het Hof van Justitie, mag deze verordening geen afbreuk doen aan de verantwoordelijkheid van de lidstaten met betrekking tot essentiële staatsfuncties op het gebied van openbare veiligheid, defensie en de bescherming van de nationale veiligheid, bijvoorbeeld met betrekking tot het verstrekken van informatie die in strijd zou zijn met de bescherming van de nationale veiligheid.

(18) Om sectoroverschrijdend leren mogelijk te maken en daadwerkelijk gebruik te maken van de ervaringen van andere sectoren bij de aanpak van cyberdreigingen, moeten de in Richtlijn (EU) 2022/2555 bedoelde financiële entiteiten deel blijven uitmaken van het "ecosysteem" van die richtlijn (bijvoorbeeld de samenwerkingsgroep en *computer security incident response teams* (CSIRT's)). De ETA's en nationale bevoegde autoriteiten moeten in staat zijn deel te nemen aan de strategische beleidsdiscussies en de technische werkzaamheden van de samenwerkingsgroep uit hoofde van die richtlijn, en daarnaast moeten zij in staat zijn informatie uit te wisselen en te blijven samenwerken met de overeenkomstig die richtlijn aangewezen of ingestelde centrale contactpunten. De bevoegde autoriteiten in de zin van deze verordening moeten ook overleg plegen en samenwerken met de CSIRT's. De bevoegde autoriteiten moeten ook technisch advies kunnen inwinnen bij de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten, en samenwerkingsovereenkomsten kunnen sluiten om te zorgen voor coördinatiemechanismen voor doeltreffende en snelle respons.

(19) Gezien de sterke verwevenheid tussen de digitale en de fysieke weerbaarheid van financiële entiteiten behoeft deze verordening en Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad ([9]) een coherente aanpak met betrekking tot de weerbaarheid van kritieke entiteiten. Aangezien de fysieke weerbaarheid van financiële entiteiten breed wordt aangepakt door de in deze verordening genoemde verplichtingen inzake ICT-risicobeheer en -rapportage, mogen de in de hoofdstukken III en IV van Richtlijn (EU)2022/2557/ vastgelegde verplichtingen niet van toepassing zijn op financiële entiteiten die binnen het toepassingsgebied van die richtlijn vallen.

(20) Aanbieders van cloudcomputingdiensten zijn een van de categorieën digitale infrastructuur die onder Richtlijn (EU) 2022/2555 vallen. Het bij deze verordening vastgestelde oversightkader van de Unie (oversightkader) is van toepassing op alle kritieke derde aanbieders van ICT-diensten, waaronder aanbieders van cloudcomputingdiensten die ICT-diensten aan financiële entiteiten verlenen, en moet als complementair aan het krachtens Richtlijn (EU) 2022/2555 verrichte toezicht worden beschouwd. Bovendien moet het bij deze verordening vastgestelde oversightkader betrekking hebben op aanbieders van cloudcomputingdiensten, gezien het ontbreken van een horizontaal kader van de Unie tot oprichting van een autoriteit voor digitale oversight.

(21) Om het ICT-risico volledig onder controle te houden, moeten financiële entiteiten beschikken over alomvattende capaciteiten die een krachtig en doeltreffend ICT-risicobeheer mogelijk maken, evenals specifieke mechanismen en beleidsmaatregelen voor de respons op alle ICT-gerelateerde incidenten en voor het melden van ernstige ICT-gerelateerde incidenten. Evenzo moeten financiële entiteiten beschikken over beleidsmaatregelen voor het testen van ICT-systemen, -controles en -procedés en voor het beheren van het ICT-risico van derde aanbieders. Het referentieniveau voor de digitale operationele weerbaarheid van financiële entiteiten moet worden verhoogd, terwijl eveneens een evenredige toepassing van de vereisten mogelijk moet zijn voor bepaalde financiële entiteiten, in het bijzonder micro-ondernemingen, evenals financiële entiteiten die onderworpen zijn aan een vereenvoudigd kader voor ICT-risicobeheer. Om een efficiënt toezicht op instellingen voor bedrijfspensioenvoorziening te bewerkstelligen dat evenredig is en de administratieve lasten voor de bevoegde autoriteiten vermindert, moet in de betrokken nationale toezichtregelingen voor dergelijke financiële entiteiten rekening worden gehouden met hun omvang en algeheel risicoprofiel en met de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen, zelfs wanneer de in artikel 5 van Richtlijn (EU) 2016/2341 van het Europees Parlement en de Raad ([10]) vastgestelde drempels worden overschreden. De toezichtactiviteiten moeten in de eerste plaats gericht zijn op de noodzaak om ernstige risico's in verband met het ICT-risicobeheer van een bepaalde entiteit aan te pakken.

([9]) Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (zie bladzijde 164 van dit Publicatieblad).

([10]) Richtlijn (EU) 2016/2341 van het Europees Parlement en de Raad van 14 december 2016 betreffende de werkzaamheden van en het toezicht op instellingen voor bedrijfspensioenvoorziening (IBPV's) (PB L 354 van 23.12.2016, blz. 37).

De bevoegde autoriteiten moeten ook een waakzame maar evenredige aanpak hanteren met betrekking tot het toezicht op instellingen voor bedrijfspensioenvoorziening die overeenkomstig artikel 31 van Richtlijn (EU) 2016/2341 een aanzienlijk deel van hun kernactiviteiten, zoals vermogensbeheer, actuariële berekeningen, boekhouding en gegevensbeheer, uitbesteden aan dienstverleners.

(22) De drempels en taxonomieën voor de rapportage van ICT-gerelateerde incidenten variëren aanzienlijk op nationaal niveau. Hoewel via de relevante werkzaamheden van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), dat is opgericht bij Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([11]), en de samenwerkingsgroep uit hoofde van Richtlijn (EU) 2022/2555 overeenstemming kan worden bereikt, kunnen voor de overige financiële entiteiten verschillende benaderingen inzake het bepalen van de drempels en het gebruik van taxonomieën bestaan of ontstaan. Die verschillen brengen met zich mee dat financiële entiteiten aan vele vereisten moeten voldoen, vooral wanneer zij in verschillende lidstaten actief zijn en wanneer zij deel uitmaken van een financiële groep. Bovendien kunnen dergelijke verschillen een belemmering vormen voor de totstandbrenging van verdere uniforme of gecentraliseerde mechanismen van de Unie die het rapportageproces versnellen en een snelle en vlotte uitwisseling van informatie tussen bevoegde autoriteiten ondersteunen, wat cruciaal is voor het aanpakken van het ICT-risico in geval van grootschalige aanvallen met potentieel systemische gevolgen.

(23) Om de administratieve lasten en mogelijk overlappende rapportageverplichtingen voor bepaalde financiële entiteiten te verminderen, mag de verplichting tot melding van incidenten krachtens Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad ([12]) niet langer van toepassing zijn op betalingsdienstaanbieders die binnen het toepassingsgebied van deze verordening vallen. Bijgevolg moeten kredietinstellingen, instellingen voor elektronisch geld, betalingsinstellingen en aanbieders van rekeninginformatiediensten, als bedoeld in artikel 33, lid 1, van die richtlijn, vanaf de datum van inwerkingtreding van deze verordening, krachtens deze verordening alle betalingsgerelateerde operationele of beveiligingsincidenten melden die eerder op grond van die richtlijn werden gemeld, ongeacht of dergelijke incidenten ICT-gerelateerd zijn.

(24) Om de bevoegde autoriteiten in staat te stellen toezicht te houden met behulp van een volledig overzicht van de aard, de frequentie, het belang en de impact van ICT-gerelateerde incidenten en om de uitwisseling van informatie tussen relevante overheidsinstanties, waaronder rechtshandhavingsinstanties en afwikkelingsautoriteiten, te bevorderen, moet bij deze verordening een robuuste regeling voor het melden van ICT-gerelateerde incidenten worden vastgesteld met voorschriften die tekortkomingen in het recht inzake financiële diensten aanpakken en tevens, ter verlichting van de kosten, bestaande overlappingen en doublures wegnemen. Het is essentieel de regeling voor het melden van ICT-gerelateerde incidenten te harmoniseren door te bepalen dat de rapportage van alle financiële entiteiten aan hun bevoegde autoriteiten gebeurt via één enkel gestroomlijnd kader zoals uiteengezet in deze verordening. Daarnaast moeten de ETA's de bevoegdheid krijgen om voor de rapportage van ICT-gerelateerde incidenten relevante elementen nader uit te werken, zoals taxonomie, tijdschema's, datasets, modellen en toepasselijke drempels. Ten behoeve van volledige overeenstemming met Richtlijn (EU) 2022/2555 moeten financiële entiteiten op vrijwillige basis significante cyberdreigingen aan de relevante bevoegde autoriteit kunnen melden wanneer zij van oordeel zijn dat de cyberdreiging relevant is voor het financiële stelsel, gebruikers van diensten of cliënten.

(25) In bepaalde financiële subsectoren zijn voorschriften voor het testen van de digitale operationele weerbaarheid ontwikkeld, leidend tot niet altijd volledig op elkaar afgestemde kaders. Dit kan voor grensoverschrijdende financiële entiteiten leiden tot dubbele kosten en maakt de wederzijdse erkenning van de resultaten van digitale-operationele-weerbaarheidtests complex, wat dan weer tot versnippering van de interne markt kan leiden.

([11]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

([12]) 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).

(26) Bovendien blijven, wanneer ICT-tests niet verplicht zijn, kwetsbaarheden onontdekt, waardoor de financiële entiteit aan ICT-risico's wordt blootgesteld en uiteindelijk de financiële sector een groter stabiliteits- en integriteitsrisico loopt. Zonder optreden van de Unie blijft het testen van de digitale operationele weerbaarheid inconsistent en komt er geen systeem voor de wederzijdse erkenning van testresultaten tussen verschillende rechtsgebieden. Daarnaast is het onwaarschijnlijk dat andere financiële subsectoren op betekenisvolle schaal testregelingen invoeren, waardoor zij verstoken blijven van de potentiële voordelen van een testkader als het gaat om het onthullen van ICT-kwetsbaarheden en -risico's en het testen van verdedigingscapaciteiten en bedrijfscontinuïteit, zaken die helpen het vertrouwen van klanten, leveranciers en zakenpartners te vergroten. Om die overlappingen, verschillen en leemten te verhelpen, moeten regels worden vastgesteld voor een gecoördineerde testregeling door financiële entiteiten en bevoegde autoriteiten, zodat de wederzijdse erkenning van geavanceerde tests voor financiële entiteiten die de criteria van deze verordening vervullen, wordt vergemakkelijkt.

(27) Dat financiële entiteiten sterk op het gebruik van ICT-diensten leunen, komt deels doordat zij zich moeten aanpassen aan een opkomende concurrerende digitale mondiale economie, zij hun bedrijfsefficiëntie moeten verbeteren, en zij voldoen moeten aan de vraag van de consument. De aard en de omvang van die afhankelijkheid is de laatste jaren voortdurend in beweging, resulterend in een daling van de kosten van financiële bemiddeling en in mogelijkheden tot bedrijfsuitbreiding en schaalbaarheid bij de ontplooiing van financiële activiteiten, en in een breed aanbod aan ICT-instrumenten voor de aansturing van complexe interne processen.

(28) Het grootschalige gebruik van ICT-diensten komt tot uiting in complexe contractuele overeenkomsten, waarbij financiële entiteiten vaak moeilijkheden ondervinden om te onderhandelen over contractuele voorwaarden die zijn afgestemd op de prudentiële normen of andere regelgevingsvereisten waaraan zij onderworpen zijn. Het kan ook moeilijk zijn specifieke rechten af te dwingen, zoals toegangsrechten of auditrechten, zelfs wanneer deze laatste contractueel zijn vastgelegd. Bovendien voorzien veel van die contractuele overeenkomsten niet in voldoende waarborgen voor de volwaardige monitoring van onderaannemingsprocessen, zodat de financiële entiteit niet langer in staat is de bijbehorende risico's te beoordelen. Aangezien derde aanbieders van ICT-diensten vaak gestandaardiseerde diensten aanbieden aan verschillende soorten klanten, houden de contractuele overeenkomsten ook niet altijd voldoende rekening met de individuele of specifieke behoeften van actoren uit de financiële sector.

(29) Het Unierecht inzake financiële diensten bevat enkele algemene voorschriften voor uitbesteding, maar daarmee is de monitoring van de contractuele dimensie nog niet volledig in het Unierecht verankerd. Bij ontstentenis van duidelijke, op maat gesneden Unienormen voor contractuele overeenkomsten met derde aanbieders van ICT-diensten wordt de externe bron van ICT-risico niet grondig aangepakt. Het is bijgevolg zaak bepaalde kernbeginselen vast te stellen als leidraad voor het beheer van ICT-risico's van derden door financiële entiteiten. Die beginselen zijn des te belangrijker wanneer financiële entiteiten ter ondersteuning van kritieke of belangrijke functies een beroep op derde aanbieders van ICT-diensten doen. Aan die beginselen moet een reeks contractuele basisrechten worden gehangen met betrekking tot verschillende elementen van de uitvoering en beëindiging van contractuele overeenkomsten, teneinde bepaalde minimumwaarborgen te verstrekken die het vermogen van de financiële entiteiten moeten versterken om alle mogelijke ICT-risico's op het niveau van derde aanbieders van diensten doeltreffend te monitoren. Die beginselen vormen een aanvulling op het voor uitbestedingen geldende sectorale recht.

(30) De homogeniteit en convergentie met betrekking tot de monitoring van het ICT-risico van derde aanbieders en de ICT-afhankelijkheden van derde partijen laat momenteel te wensen over. Ondanks inspanningen op het vlak van uitbestedingen, zoals de EBA-richtsnoeren inzake uitbesteding van 2019 en de ESMA-richtsnoeren over uitbesteding aan aanbieders van clouddiensten van 2021, komt de bredere kwestie van de bestrijding van systeemrisico's die kunnen voortvloeien uit de blootstelling van de financiële sector aan een beperkt aantal kritieke derde aanbieders van ICT-diensten, in het Unierecht onvoldoende aan de orde. Dit wordt nog verergerd door het ontbreken van nationale regelgeving inzake mandaten en instrumenten waarmee financiële toezichthouders zich een goed inzicht in de afhankelijkheden van derden op ICT-gebied zouden kunnen verschaffen en de uit de concentratie van dergelijke afhankelijkheden voortvloeiende risico's adequaat monitoren.

(31) Rekening houdend met de potentiële systeemrisico's die de toegenomen uitbesteding en de concentratie van ICT bij derden meebrengen, en met het feit dat nationale mechanismen financiële toezichthouders onvoldoende middelen bieden om de gevolgen van het ICT-risico bij kritieke derde aanbieders van ICT-diensten te kunnen kwantificeren, kwalificeren en herstellen, moet een passend oversightkader tot stand worden gebracht voor de voortdurende monitoring van activiteiten van voor financiële entiteiten kritieke derde aanbieders van ICT-diensten, daarbij zorgend voor vertrouwelijkheid en veiligheid van klanten die geen financiële entiteiten zijn. Aan ICT-dienstverlening binnen een financiële groep zijn specifieke risico's en voordelen verbonden die evenwel niet automatisch aangemerkt mogen worden als minder risicovol dan ICT-dienstverlening door externe aanbieders. Interne ICT-dienstverlening moet derhalve aan hetzelfde regelgevingskader worden onderworpen. Dat neemt niet weg dat bij interne ICT-dienstverlening vanuit de financiële groep zelf, financiële entiteiten een betere grip op intragroepaanbieders zouden kunnen hebben, iets waarmee bij de algehele risicobeoordeling rekening gehouden moet worden.

(32) Aangezien ICT-risico's steeds complexer en geavanceerder worden, staan of vallen goede opsporings- en preventiemaatregelen op het vlak van ICT-risico grotendeels met regelmatige uitwisseling van inlichtingen over dreigingen en kwetsbaarheid tussen financiële entiteiten. Uitwisseling van inlichtingen helpt de bewustwording over cyberdreigingen te vergroten. Dit helpt dan weer het vermogen van financiële entiteiten om te voorkomen dat cyberdreigingen tot werkelijke ICT-gerelateerde incidenten uitgroeien te vergroten, en ook kunnen financiële entiteiten dan de impact van ICT-gerelateerde incidenten beter beheersen en sneller ervan herstellen. Bij ontstentenis van richtsnoeren op Unieniveau zijn er verschillende factoren die een dergelijke informatie-uitwisseling lijken te verhinderen, met name onzekerheid over de verenigbaarheid met de regels inzake gegevensbescherming, antitrust en aansprakelijkheid.

(33) Voorts leidt twijfel over het soort informatie dat met andere marktdeelnemers of niet-toezichthoudende autoriteiten (zoals Enisa voor analytische input of Europol voor rechtshandhavingsdoeleinden) mag worden uitgewisseld, ertoe dat nuttige informatie wordt achtergehouden. De informatie-uitwisseling blijft derhalve zowel qua omvang als qua kwaliteit vooralsnog beperkt en gefragmenteerd, waarbij relevante uitwisselingen meestal lokaal plaatsvinden (via nationale initiatieven) zonder samenhangende Uniebrede regelingen voor informatie-uitwisseling die zijn toegesneden op de behoeften van een geïntegreerd financieel stelsel. Het is daarom belangrijk dat die communicatiekanalen versterkt worden.

(34) Financiële entiteiten moeten worden aangemoedigd informatie en inlichtingen over cyberdreigingen tussen elkaar uit te wisselen, en hun individuele kennis en praktische ervaring op strategisch, tactisch en operationeel niveau collectief te benutten, om zo via deelname in informatie-uitwisselingsregelingen beter in staat te zijn cyberdreigingen adequaat te beoordelen, te monitoren, af te weren en aan te pakken. Op Unieniveau moeten er derhalve mechanismen voor vrijwillige informatie-uitwisseling mogelijk worden gemaakt die, wanneer zij in vertrouwde omgevingen worden uitgevoerd, de gehele financiële sector helpen cyberdreigingen te voorkomen en collectief aan te pakken door de verspreiding van ICT-risico snel te beperken en mogelijke besmetting via de financiële kanalen te verhinderen. Die mechanismen moeten in overeenstemming zijn met de toepasselijke mededingingsregels van de Unie uiteengezet in de mededeling van de Commissie van 14 januari 2011 met als titel "Richtsnoeren inzake de toepasselijkheid van artikel 101 van het Verdrag betreffende de werking van de Europese Unie op horizontale samenwerkingsovereenkomsten", en met haar gegevensbeschermingsregels, meer in het bijzonder Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([13]). Ook moeten ze gevestigd worden op een of meer van de in artikel 6 van die verordening vastgestelde rechtsgrondslagen, zoals in de context van de verwerking van persoonsgegevens die noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verwerkingsverantwoordelijke of van een derde, als bedoeld in artikel 6, lid 1, punt f), van die verordening, alsmede in de context van de verwerking van persoonsgegevens die noodzakelijk is om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke onderworpen is, noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, als bedoeld in artikel 6, lid 1, punt c) respectievelijk punt e), van die verordening.

([13]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

(35) Voor een hoog niveau van digitale operationele weerbaarheid in de hele financiële sector en om daarbij gelijke tred te kunnen houden met de technologische ontwikkelingen, moet deze verordening betrekking hebben op risico's die uit alle soorten ICT-diensten voortvloeien. Daartoe moet in de context van deze verordening de definitie van ICT-diensten breed worden opgevat en aldus mede digitale en gegevensdiensten omvatten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden geleverd. Die definitie moet onder meer betrekking hebben op zogeheten over-the-topdiensten, die onder de categorie elektronische-communicatiediensten vallen. Uitsluitend de beperkte categorie bestaande uit traditionele, als PSTN-diensten (*Public Switched Telephone Network services*) aan te merken analoge telefoondiensten, vaste telefoondiensten, verouderde telefoondiensten (*Plain Old Telephone Service* — POTS), en vastelijntelefoondiensten moet ervan worden uitgesloten.

(36) Ondanks de brede dekking waarin deze verordening voorziet, moet bij de toepassing van de regels inzake digitale operationele weerbaarheid rekening worden gehouden met aanzienlijke verschillen tussen financiële entiteiten qua omvang en qua algeheel risicoprofiel. Als algemeen beginsel geldt dat financiële entiteiten, wanneer zij middelen en capaciteiten vrijmaken voor de uitvoering van het kader voor ICT-risicobeheer, hun ICT-gerelateerde behoeften naar behoren moeten afstemmen op hun omvang en algeheel risicoprofiel, en op de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen terwijl de bevoegde autoriteiten de daarbij gehanteerde benadering moeten blijven beoordelen en evalueren.

(37) Aanbieders van rekeninginformatiediensten, in de zin van artikel 33, lid 1, van Richtlijn (EU) 2015/2366, vallen uitdrukkelijk onder het toepassingsgebied van deze verordening, rekening houdend met de specifieke aard van hun activiteiten en de daaruit voortvloeiende risico's. Onder het toepassingsgebied van deze verordening vallen tevens alle instellingen voor elektronisch geld en betalingsinstellingen die krachtens artikel 9, lid 1, van Richtlijn 2009/110/EG van het Europees Parlement en de Raad ([14]) en artikel 32, lid 1, van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad zijn vrijgesteld, zelfs indien zij niet over een vergunning overeenkomstig Richtlijn 2009/110/EG voor de uitgifte van elektronisch geld beschikken, of over een vergunning overeenkomstig Richtlijn (EU) 2015/2366 voor het aanbieden en uitvoeren van betalingsdiensten. Postcheque- en girodiensten als bedoeld in artikel 2, lid 5, punt 3, van Richtlijn 2013/36/EU van het Europees Parlement en de Raad ([15]) zijn evenwel uitgesloten van het toepassingsgebied van deze verordening. De bevoegde autoriteit die is aangewezen overeenkomstig artikel 22 van Richtlijn (EU) 2015/2366, dient de bevoegde autoriteit te zijn voor betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld, voor instellingen voor elektronisch geld die zijn vrijgesteld krachtens Richtlijn 2009/110/EG, en voor aanbieders van rekeninginformatiediensten als bedoeld in artikel 33, lid 1, van Richtlijn (EU) 2015/2366.

(38) Aangezien grotere financiële entiteiten over meer middelen zouden kunnen beschikken en snel financiële middelen kunnen inzetten om governancestructuren te ontwikkelen en diverse bedrijfsstrategieën op te zetten, moeten alleen financiële entiteiten die geen micro-ondernemingen in de zin van deze verordening zijn, verplicht worden complexere governanceregelingen op te zetten. Dergelijke entiteiten zijn met name beter toegerust om specifieke beheersfuncties op te zetten voor het toezicht op regelingen met derde aanbieders van ICT-diensten of voor crisisbeheer, om hun ICT-risicobeheer te organiseren volgens het model van drie verdedigingslinies, of om een intern risicobeheer- en controlemodel op te zetten en hun ICT-risicobeheerkader aan interne audits te onderwerpen.

(39) Sommige financiële entiteiten zijn uit hoofde van het desbetreffende sectorspecifieke Unierecht vrijgesteld of aan een zeer licht regelgevingskader onderworpen. Het gaat daarbij onder meer om beheerders van alternatieve beleggingsfondsen als bedoeld in artikel 3, lid 2, van Richtlijn 2011/61/EU van het Europees Parlement en de Raad ([16]), verzekerings- en herverzekeringsondernemingen als bedoeld in artikel 4 van Richtlijn 2009/138/EG van het Europees Parlement en de Raad ([17]), en instellingen voor bedrijfspensioenvoorziening die pensioenregelingen

([14]) Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PB L 267 van 10.10.2009, blz. 7).

([15]) 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).

([16]) Richtlijn 2011/61/EU van het Europees Parlement en de Raad van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 1095/2010 (PB L 174 van 1.7.2011, blz. 1).

([17]) 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).

uitvoeren die samen niet meer dan 15 deelnemers tellen. In het licht van die vrijstellingen zou het niet evenredig zijn de betroffen financiële entiteiten onder het toepassingsgebied van deze verordening te laten vallen. Bovendien erkent deze verordening de specifieke kenmerken van de verzekeringsbemiddelingsmarktstructuur, om welke reden verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen die als micro-ondernemingen of als kleine of middelgrote ondernemingen kunnen worden aangemerkt, niet onder deze verordening dienen te vallen.

(40) Aangezien de in artikel 2, lid 5, punten 4 tot en met 23, van Richtlijn 2013/36/EU bedoelde entiteiten niet onder het toepassingsgebied van die richtlijn vallen, moeten de lidstaten ervoor kunnen kiezen dit soort op hun respectieve grondgebied gevestigde entiteiten vrij te stellen van de toepassing van deze verordening.

(41) Om deze verordening in overeenstemming te brengen met het toepassingsgebied van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([18]), is het tevens passend natuurlijke en rechtspersonen als bedoeld in de artikelen 2 en 3 van die richtlijn die zonder een vergunning uit hoofde van Richtlijn 2014/65/EU beleggingsdiensten mogen verrichten, van het toepassingsgebied van deze verordening uit te sluiten. Artikel 2 van Richtlijn 2014/65/EU sluit echter ook entiteiten die voor de toepassing van deze verordening als financiële entiteiten kwalificeren, zoals centrale effectenbewaarinstellingen, instellingen voor collectieve belegging of verzekerings- en herverzekeringsondernemingen, uit van het toepassingsgebied van die richtlijn. De uitsluiting van de in de artikelen 2 en 3 van die richtlijn bedoelde personen en entiteiten van het toepassingsgebied van deze verordening mag niet gelden voor die centrale effectenbewaarinstellingen, instellingen voor collectieve belegging of verzekerings- en herverzekeringsondernemingen.

(42) Op grond van sectorspecifiek Unierecht gelden voor sommige financiële entiteiten lichtere eisen of vrijstellingen om redenen die verband houden met hun omvang of de door hen verleende diensten. Die categorie van financiële entiteiten betreft onder meer kleine en niet-verweven beleggingsondernemingen, kleine instellingen voor bedrijfspensioenvoorziening die door de betrokken lidstaat van het toepassingsgebied van Richtlijn (EU) 2016/2341 kunnen worden uitgesloten onder de voorwaarden van artikel 5 van die richtlijn en die pensioenregelingen met bij elkaar niet meer dan 100 deelnemers uitvoeren, alsmede instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld. Het is derhalve overeenkomstig het evenredigheidsbeginsel en met het oog op de geest van het sectorspecifieke Unierecht, tevens passend die financiële entiteiten aan een vereenvoudigd kader voor ICT-risicobeheer in het kader van deze verordening te onderwerpen. Het evenredige karakter van het kader voor ICT-risicobeheer dat die financiële entiteiten bestrijkt, mag niet worden gewijzigd bij de door de ETA's te ontwikkelen technische reguleringsnormen. Bovendien is het, overeenkomstig het evenredigheidsbeginsel, passend tevens betalingsinstellingen als bedoeld in artikel 32, lid 1, van Richtlijn (EU) 2015/2366 en instellingen voor elektronisch geld als bedoeld in artikel 9 van Richtlijn 2009/110/EG die overeenkomstig het nationale recht tot omzetting van die rechtshandelingen van de Unie zijn vrijgesteld, aan een vereenvoudigd kader voor ICT-risicobeheer uit hoofde van deze verordening te onderwerpen, waarbij zij aangetekend dat betalingsinstellingen en instellingen voor elektronisch geld die niet zijn vrijgesteld overeenkomstig hun respectieve nationale recht tot omzetting van sectoraal Unierecht wel in overeenstemming met het algemene kader van deze verordening moeten zijn.

(43) Evenzo mogen financiële entiteiten die als micro-ondernemingen worden aangemerkt of onder het vereenvoudigde kader voor ICT-risicobeheer in het kader van deze verordening vallen, niet worden verplicht om een functie in te stellen voor het toezicht op hun regelingen met derde aanbieders van ICT-diensten inzake het gebruik van ICT-diensten, of om een lid van het hoger management aan te wijzen dat verantwoordelijk is voor het toezicht op de desbetreffende risicoblootstelling en relevante documentatie; noch om de verantwoordelijkheid voor het beheer van en het toezicht op het ICT-risico aan een controlefunctie toe te wijzen en te zorgen voor passende onafhankelijkheid van die controlefunctie ter voorkoming van belangenconflicten; noch om het kader voor ICT-risicobeheer ten minste eenmaal per jaar te documenteren en te evalueren; noch om het kader voor ICT-risicobeheer regelmatig aan een interne audit te onderwerpen; noch om diepgaande analyses uit te voeren na grote veranderingen in hun infrastructuur en processen voor netwerk- en informatiesystemen; noch om regelmatig risicoanalyses uit te voeren voor legacy-ICT-systemen; noch om de uitvoering van de ICT-respons- en herstelplannen aan een onafhankelijke interne audit te onderwerpen; noch om over een crisisbeheersfunctie te beschikken, noch om de tests van bedrijfscontinuïteit en -respons en herstelplannen uit te breiden om rekening te houden met de scenario's voor de overschakeling tussen primaire ICT-infrastructuur en de reservefaciliteiten; noch om bevoegde autoriteiten die

([18]) 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).

hierom verzoeken een raming te verstrekken van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van ernstige ICT-gerelateerde incidenten, noch om overbodige ICT-capaciteiten in stand te houden; noch om de nationale bevoegde autoriteiten in kennis te stellen van wijzigingen op basis van evaluaties naar aanleiding van ICT-gerelateerde incidenten; noch om voortdurend toezicht te houden op relevante technologische ontwikkelingen, noch om als integraal onderdeel van het kader voor ICT-risicobeheer waarin deze verordening voorziet een alomvattend programma voor het testen van digitale operationele weerbaarheid op te zetten, of om een strategie inzake ICT-risico's van derden vast te stellen en regelmatig te evalueren. Daarnaast moet van micro-ondernemingen uitsluitend worden gevraagd op basis van hun risicoprofiel na te gaan of dergelijke overbodige ICT-capaciteiten behouden moeten worden. Voor micro-ondernemingen moet een flexibelere regeling worden ontworpen wat programma's voor het testen van digitale operationele weerbaarheid betreft. Bij het bepalen van het type uit te voeren tests en de frequentie van die tests, moeten zij een goede afweging maken tussen de doelstelling een hoge digitale operationele weerbaarheid te handhaven, de beschikbare middelen en hun algehele risicoprofiel. Micro-ondernemingen en financiële entiteiten die onder het vereenvoudigde kader voor ICT-risicobeheer uit hoofde van deze verordening vallen, moeten worden vrijgesteld van de verplichting om ICT-instrumenten, -systemen en -processen aan geavanceerde tests op basis van dreigingsgestuurde penetratietests (*threat led penetration testing* — TLPT) te onderwerpen, aangezien alleen financiële entiteiten die de criteria van deze verordening vervullen verplicht moeten worden dergelijke tests uit te voeren. Gezien hun beperkte mogelijkheden moeten micro-ondernemingen met hun derde aanbieder van ICT-diensten kunnen overeenkomen de rechten van toegang, inspectie en audit van de financiële entiteit te delegeren aan een door de derde aanbieder aan te wijzen onafhankelijke derde partij, op voorwaarde dat de financiële entiteit te allen tijde alle relevante informatie en zekerheid met betrekking tot de prestaties van de derde aanbieder van ICT-diensten bij de respectieve onafhankelijke derde partij kan opvragen.

(44) Aangezien alleen die financiële entiteiten die worden aangemerkt voor geavanceerde tests op digitale weerbaarheid verplicht moeten zijn om dreigingsgestuurde penetratietests uit te voeren, moeten de administratieve processen en de financiële kosten die de uitvoering van dergelijke tests meebrengt, gedragen worden door een klein percentage van de financiële entiteiten.

(45) Om te zorgen voor volledige afstemming en algehele samenhang tussen de bedrijfsstrategieën van financiële entiteiten enerzijds en de uitvoering van ICT-risicobeheer anderzijds, moeten de leidinggevende organen van de financiële entiteit worden verplicht een centrale en actieve rol te blijven spelen bij het sturen en aanpassen van het kader voor ICT-risicobeheer en de algemene strategie voor digitale operationele weerbaarheid. De door de leidinggevende organen te volgen aanpak moet niet alleen gericht zijn op middelen ter waarborging van de weerbaarheid van de ICT-systemen, maar ook op personen en processen. Daarvoor dient een reeks beleidsmaatregelen die alle niveaus van de organisatie en bij alle personeelsleden een sterk bewustzijn van cyberrisico's bevorderen en de wil ondersteunen om op alle niveaus een strikte cyberhygiëne in acht te nemen. Een overkoepelend beginsel van die alomvattende aanpak moet zijn dat het leidinggevend orgaan de uiteindelijke verantwoordelijkheid draagt voor het beheer van het ICT-risico van een financiële entiteit, vertaald in een voortdurende betrokkenheid van het leidinggevend orgaan bij de controle van de monitoring van het ICT-risicobeheer.

(46) Het beginsel dat het leidinggevend orgaan de volledige en uiteindelijke verantwoordelijkheid draagt voor het beheer van het ICT-risico van de financiële entiteit, betekent bovendien dat moet worden gezorgd voor voldoende ICT-gerelateerde investeringen en een budget waarmee de financiële entiteit grote digitale operationele weerbaarheid kan verwezenlijken.

(47) Deze verordening, die geïnspireerd is op relevante internationale, nationale en sectorale beste praktijken, normen, richtsnoeren, aanbevelingen en benaderingen ten aanzien van het beheer van het cyberrisico, bevordert een reeks beginselen die de algemene structurering van het ICT-risicobeheer ondersteunen. Dat betekent dat zolang de belangrijkste door financiële entiteiten gecreëerde capaciteiten de uiteenlopende functies in het ICT-risicobeheer (identificatie, bescherming en voorkoming, detectie, respons en herstel, scholing en ontwikkeling en communicatie) ten goede komen, het de financiële entiteiten vrij zou moeten staan om anders opgezette of gecategoriseerde modellen voor ICT-risicobeheer te gebruiken.

(48) Om gelijke tred te houden met ontwikkelingen in het cyberdreigingslandschap, moeten financiële entiteiten geactualiseerde ICT-systemen in stand houden die betrouwbaar zijn en niet alleen de gegevensverwerking kunnen garanderen die nodig is voor hun dienstverlening, maar die ook voor voldoende technologische weerbaarheid zorgen, opdat zij adequaat kunnen inspelen op extra verwerkingsbehoeften als gevolg van gespannen marktomstandigheden of andere ongunstige situaties.

(49) Er zijn efficiënte bedrijfscontinuïteits- en herstelplannen nodig om financiële entiteiten in staat te stellen ICT-gerelateerde incidenten snel op te lossen, met name cyberaanvallen, door overeenkomstig hun backupbeleid de schade te beperken en prioriteit te geven aan de hervatting van activiteiten en aan herstelmaatregelen. Een dergelijke hervatting mag echter op geen enkele wijze ten koste gaan van de integriteit en veiligheid van de netwerk- en informatiesystemen of de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens.

(50) Hoewel deze verordening financiële entiteiten toestaat op flexibele wijze hun eigen hersteltijd- en herstelpuntdoelstellingen vast te stellen en daarbij derhalve ten volle rekening te houden met de aard en het kritieke karakter van de betrokken functies en met eventuele specifieke bedrijfsbehoeften, moeten zij bij deze verordening verplicht worden om bij het vaststellen van dergelijke doelstellingen toch ook het mogelijke algemene effect op de marktefficiëntie te evalueren.

(51) Daders van cyberaanvallen zijn doorgaans op zoek naar financieel gewin rechtstreeks aan de bron, met alle verregaande gevolgen voor financiële entiteiten van dien. Om te voorkomen dat ICT-systemen aan integriteit inboeten of onbeschikbaar worden, en dus om inbreuken op gegevens en schade aan fysieke ICT-infrastructuur te voorkomen, moet de rapportage van ernstige ICT-gerelateerde incidenten door financiële entiteiten aanzienlijk worden verbeterd en gestroomlijnd. De rapportage van ICT-gerelateerde incidenten moet worden geharmoniseerd door alle financiële entiteiten te verplichten rechtstreeks aan hun desbetreffende bevoegde autoriteiten te rapporteren. Staat een financiële entiteit onder toezicht van meer dan één nationale bevoegde autoriteit, dan bepaalt de lidstaat aan welke ene daarvan de rapportage gericht moet worden. Kredietinstellingen die overeenkomstig artikel 6, lid 4, van Verordening (EU) nr. 1024/2013 van de Raad ([19]) als significant zijn geclassificeerd, moeten deze rapportage indienen bij de nationale bevoegde autoriteiten, die het verslag vervolgens aan de Europese Centrale Bank (ECB) toezenden.

(52) De rechtstreekse rapportage moet het financiële toezichthouders mogelijk maken zich onmiddellijke toegang tot informatie over ernstige ICT-gerelateerde incidenten te verschaffen. Financiële toezichthouders moeten op hun beurt bijzonderheden over ernstige ICT-gerelateerde incidenten doorgeven aan publieke niet-financiële autoriteiten (bijvoorbeeld bevoegde autoriteiten en centrale contactpunten uit hoofde van Richtlijn (EU) 2022/2555, nationale gegevensbeschermingsautoriteiten en rechtshandhavingsautoriteiten voor ernstige ICT-gerelateerde incidenten van criminele aard), teneinde die autoriteiten bewuster van dergelijke incidenten te maken en, wat CSIRT's betreft, om in voorkomend geval snelle bijstand aan financiële entiteiten te faciliteren. Voorts moeten de lidstaten financiële entiteiten kunnen verplichten dergelijke informatie zelf aan overheidsinstanties buiten het financiëledienstengebied te verstrekken. Dankzij die informatiestromen moeten financiële entiteiten snel hun voordeel kunnen doen met relevante technische input, advies over corrigerende maatregelen en daaropvolgende follow-up door deze overheidsinstanties. De informatie over ernstige ICT-gerelateerde incidenten moet onderling worden gedeeld: de financiële toezichthouders moeten de financiële entiteit alle nodige feedback of richtsnoeren geven, en de ETA's moeten geanonimiseerde gegevens over cyberdreigingen en -kwetsbaarheden in verband met een incident delen, dit alles met het oog op een bredere collectieve verdediging.

(53) Hoewel van alle financiële entiteiten moet worden vereist dat zij incidenten melden, wordt niet verwacht dat dit vereiste hen alle op dezelfde wijze treft. Relevante materialiteitsdrempels en rapportagetermijnen moeten immers naar behoren worden aangepast in het kader van gedelegeerde handelingen die gebaseerd zijn op de door de ETA's te ontwikkelen technische reguleringsnormen, zodat alleen ernstige ICT-incidenten worden bestreken. Bovendien moet bij het vastleggen van termijnen voor rapportageverplichtingen rekening worden gehouden met de specifieke kenmerken van financiële entiteiten.

(54) Deze verordening moet kredietinstellingen, betalingsinstellingen, dienstverleners van rekeninginformatie en instellingen voor elektronisch geld verplichten, alle betalingsgerelateerde operationele of beveiligingsincidenten — die voorheen werden gemeld uit hoofde van Richtlijn (EU) 2015/2366 — te rapporteren, ongeacht de ICT-aard van het incident.

([19]) Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen (PB L 287 van 29.10.2013, blz. 63).

(55) De ETA's moeten worden belast met het beoordelen van de haalbaarheid van en de voorwaarden voor een mogelijke centralisatie van rapporten over ICT-incidenten op Unieniveau. Een dergelijke centralisatie zou kunnen bestaan uit één EU-hub voor de melding van ernstige ICT-incidenten; deze ontvangt ofwel rechtstreeks rapporten en stelt de nationale bevoegde autoriteiten daarvan automatisch in kennis, ofwel ontvangt de hub slechts de relevante rapporten die hem door de nationale autoriteiten worden toegezonden, bewaart hij deze centraal en heeft hij zodoende een coördinerende rol. De ETA's moeten belast worden met de opstelling, in overleg met de ECB en Enisa, van een gezamenlijk verslag waarin wordt nagegaan of het haalbaar is één EU-hub op te richten.

(56) Om een hoog niveau van digitale operationele weerbaarheid te bereiken, en in overeenstemming met zowel de relevante internationale normen (bv. de fundamentele elementen van de G-7 voor dreigingsgestuurde penetratietests) als de in de Unie gebruikte kaders zoals Tiber-EU, moeten financiële entiteiten hun ICT-systemen en hun personeel dat ICT-taken heeft, regelmatig testen op de effectiviteit van hun preventie-, detectie-, respons- en herstelcapaciteiten, om zo potentiële ICT-kwetsbaarheden aan het licht te brengen en te verhelpen. Gelet op de verschillende niveaus van cyberbeveiligingsparaatheid die tussen en binnen de verschillende financiële subsectoren van financiële entiteiten bestaan, moeten de tests verschillende instrumenten en acties omvatten, variërend van de beoordeling van basisvereisten (bv. kwetsbaarheidsbeoordelingen en -scans, open-sourceanalyses, beoordelingen van netwerkbeveiliging, kloofanalyses, fysieke beveiligingsonderzoeken, vragenlijsten, oplossingen voor scanningsoftware, beoordelingen van broncodes indien mogelijk, op scenario's gebaseerde tests, compatibiliteitstests, prestatietests en end-to-endtests) tot geavanceerdere tests door middel van dreigingsgestuurde penetratietests. Zulke geavanceerde tests zouden alleen vereist moeten zijn voor financiële entiteiten die in ICT-opzicht voldoende ontwikkeld zijn om deze tests redelijkerwijs uit te kunnen voeren. Het testen van de digitale operationele weerbaarheid dat uit hoofde van deze verordening vereist is, moet dus strenger zijn voor die financiële entiteiten die de criteria van deze verordening vervullen (bijvoorbeeld grote, systemische en in ICT-opzicht ontwikkelde kredietinstellingen, effectenbeurzen, centrale effectenbewaarinstellingen en centrale tegenpartijen) dan voor andere financiële entiteiten. Het testen van digitale operationele weerbaarheid door middel van dreigingsgestuurde penetratietests moet worden toegespitst op financiële entiteiten die actief zijn in subsectoren van de belangrijkste financiële diensten en die een systemische rol hebben (bijvoorbeeld betalingen, bankieren, en clearing en afwikkeling) en minder van toepassing zijn op andere subsectoren (bijvoorbeeld vermogensbeheerders en kredietbeoordelaars).

(57) Financiële entiteiten die werkzaam zijn in activiteiten over de grenzen heen en gebruikmaken van de vrijheid van vestiging of dienstverrichting binnen de Unie, moeten in hun lidstaat van herkomst voldoen aan één reeks geavanceerde testvereisten (d.w.z. dreigingsgestuurde penetratietests). Deze tests moeten uitgevoerd worden in de ICT-infrastructuur in alle rechtsgebieden waar de grensoverschrijdende financiële groep binnen de Unie actief is. Dit moet ervoor zorgen dat deze groepen in slechts één rechtsgebied ICT-testkosten hoeven te maken.

(58) Om gebruik te maken van de deskundigheid die sommige instanties reeds in huis hebben — met name in de uitvoering van het Tiber-EU-kader — moet deze verordening de lidstaten de mogelijkheid bieden één overheidsinstantie aan te wijzen als nationaal verantwoordelijke dienst voor alle dreigingsgestuurde penetratietests in de financiële sector, dan wel verschillende instanties die, indien er niet één enkele overheidsinstantie wordt aangewezen, de uitoefening van de met dreigingsgestuurde penetratietests verband houdende taken delegeren aan een andere bevoegde nationale financiële autoriteit.

(59) Aangezien deze verordening niet vereist dat financiële entiteiten alle kritieke of belangrijke functies in één enkele dreigingsgestuurde penetratietest dekken, moeten financiële entiteiten vrijelijk kunnen bepalen welke en hoeveel kritieke of belangrijke functies in een dergelijke test worden opgenomen.

(60) Gebundeld testen in de zin van deze Verordening (dat wil zeggen: verschillende financiële entiteiten nemen deel aan een dreigingsgestuurde penetratietest, en een derde aanbieder van ICT-diensten kan rechtstreeks contractuele overeenkomsten treffen met een externe tester) mag alleen worden toegestaan indien redelijkerwijs kan worden verwacht dat de kwaliteit of de beveiliging van de diensten die door de derde aanbieder van ICT-diensten worden geleverd aan klanten die buiten het toepassingsgebied van deze verordening vallende entiteiten zijn, of de vertrouwelijkheid van de gegevens met betrekking tot dergelijke diensten, negatief worden beïnvloed. Gebundeld testen moet ook onderworpen zijn aan waarborgen (leiding in handen van één aangewezen financiële entiteit, ijking van het aantal deelnemende financiële entiteiten) om zo voor de betrokken financiële entiteiten een rigoureuze testoefening te garanderen die voldoet aan de doelstellingen van de dreigingsgestuurde penetratie uit hoofde van deze verordening.

(61) Om te kunnen gebruikmaken van interne middelen op bedrijfsniveau moet deze verordening het gebruik van interne testers voor een dreigingsgestuurde penetratie toestaan, op voorwaarde dat er toestemming van de toezichthouder is, er geen belangenconflicten zijn, en het gebruik van interne testers periodiek (dat wil zeggen: ten minste om de drie tests) wordt afgewisseld met het gebruik van externe testers; daarbij moet ook worden geëist dat de verstrekker van de inlichtingen over dreigingen in de dreigingsgestuurde penetratie altijd extern is ten opzichte van de geteste financiële entiteit. De verantwoordelijkheid voor de uitvoering van dreigingsgestuurde penetraties moet volledig bij de financiële entiteit blijven berusten. Attesten die door de autoriteiten worden verstrekt, mogen uitsluitend wederzijdse erkenning tot doel hebben en niet in de weg staan van eventuele vervolgmaatregelen die nodig zijn om het ICT-risico te verhelpen waaraan de financiële entiteit is blootgesteld. Dergelijke attesten mogen ook niet worden beschouwd als een goedkeuring door de toezichthouder van het vermogen van een financiële entiteit ICT-risico's te beheersen en te beperken.

(62) Voor een gedegen bewaking van het ICT-derdenrisico in de financiële sector moet een reeks op beginselen gebaseerde regels worden vastgelegd als leidraad voor financiële entiteiten bij de bewaking van risico's die ontstaan in functies die zijn uitbesteed aan derde aanbieders van ICT-diensten. Dit geldt met name voor ICT-diensten die kritieke of belangrijke functies ondersteunen, alsmede meer in het algemeen voor alle vormen van afhankelijkheid van ICT-derden.

(63) Gelet op de complexiteit van de verschillende bronnen van ICT-risico en de veelheid en diversiteit van verleners van technologische oplossingen die een soepele verlening van financiële diensten mogelijk maken, moet deze verordening dienovereenkomstig betrekking hebben op een veelheid van derde aanbieders van ICT-diensten, waaronder verleners van cloudcomputingdiensten, software, diensten voor data-analyse en verleners van datacentrumdiensten. Aangezien financiële entiteiten op effectieve en coherente wijze alle soorten risico's moeten kennen en beheersen — ook bij ICT-diensten die binnen een financiële groep worden aanbesteed — moet het duidelijk zijn dat ook ondernemingen die deel uitmaken van een financiële groep en die hoofdzakelijk ICT-diensten verlenen aan hun moederonderneming, aan dochterondernemingen of aan bijkantoren van hun moederonderneming, alsmede financiële entiteiten die ICT-diensten verlenen aan andere financiële entiteiten, moeten worden beschouwd als derde aanbieders van ICT-diensten in de zin van deze verordening. Tot slot moeten, in het licht van de zich ontwikkelende markt voor betalingsdiensten die steeds afhankelijker worden van complexe technische oplossingen, en in het licht van opkomende betalingsdiensten en betalingsoplossingen, deelnemers in het geheel van betalingsdiensten die betalingsverwerkingsactiviteiten verrichten of betalingsinfrastructuren exploiteren, ook worden beschouwd als derde aanbieders van ICT-diensten in de zin van deze verordening; een uitzondering geldt voor centrale banken wanneer deze betalings- of effectenafwikkelingen verrichten, en overheidsinstanties wanneer deze ICT-diensten verlenen in het kader van de verrichting van overheidsfuncties.

(64) Een financiële entiteit moet te allen tijde volledig verantwoordelijk blijven voor de naleving van haar in deze verordening vervatte verplichtingen. Financiële entiteiten moeten een evenredige benadering hanteren van de monitoring van de risico's die zich voordoen op het niveau van derde aanbieders van ICT-diensten, en wel door terdege te letten op de aard, de omvang, de complexiteit en het belang van hun ICT-afhankelijkheden, alsook op het kritieke karakter of het belang van de diensten, processen of functies die onder de contractuele overeenkomsten vallen. Tot slot dient de monitoring gebaseerd te zijn op een zorgvuldige beoordeling van de mogelijke impact op de continuïteit en de kwaliteit van de financiële diensten die zij verlenen aan individuen en groepen, naargelang het geval.

(65) De monitoring moet een strategische benadering volgen van het ICT-risico dat bestaat wanneer derde dienstverleners in de arm worden genomen. Deze benadering moet geformaliseerd worden doordat het leidinggevend orgaan van de financiële entiteit een specifieke strategie voor het ICT-risico van derde dienstverleners heeft die is gebaseerd op een continue screening van alle ICT-afhankelijkheden van derden. Om ervoor te zorgen dat toezichthouders zich beter bewust zijn van de afhankelijkheden van ICT-derden en om de werkzaamheden in verband met het bij deze verordening ingestelde oversightkader verder te ondersteunen, moeten alle financiële entiteiten worden verplicht een register bij te houden met informatie over alle contractuele overeenkomsten inzake het gebruik van ICT-diensten die door derde aanbieders van ICT-diensten worden geleverd. Financiële toezichthouders moeten het volledige register kunnen opvragen of om bepaalde delen daarvan kunnen verzoeken om zo essentiële informatie te kunnen verkrijgen waarmee zij een beter inzicht kunnen krijgen in de ICT-afhankelijkheden van financiële entiteiten.

(66) Een grondige analyse voorafgaand aan het sluiten van contracten moet de basis vormen voor en voorafgaan aan de formele sluiting van contractuele overeenkomsten. De analyse moet zich met name richten op elementen als het kritieke karakter en het belang van de diensten waarop het beoogde ICT-contract betrekking heeft, de nodige goedkeuringen door de toezichthouder, eventuele andere voorwaarden, en het mogelijke concentratierisico van de contracten. Ook moet aandacht worden geschonken aan zorgvuldigheidseisen bij de selectie en beoordeling van derde aanbieders van ICT-diensten en aan mogelijke belangenconflicten. Bij contractuele overeenkomsten die kritieke of belangrijke functies betreffen, moeten financiële entiteiten letten op het gebruik door derde aanbieders van ICT-diensten van de meest actuele en hoogste normen voor informatiebeveiliging. De beëindiging van

contractuele overeenkomsten zou in ieder geval het gevolg kunnen zijn van een reeks omstandigheden waaruit tekortkomingen op het niveau van de derde aanbieder van ICT-diensten blijken; met name valt te denken aan ernstige inbreuken op wetten of contractuele voorwaarden, omstandigheden waaruit een mogelijke wijziging van de uitvoering van de in de contractuele overeenkomsten voorziene functies blijkt, aanwijzingen dat er zwakke punten zijn bij de derde aanbieder van ICT-diensten in diens algemene ICT-risicobeheer, of omstandigheden die erop wijzen dat de relevante bevoegde autoriteit niet in staat is daadwerkelijk toezicht uit te oefenen op de financiële entiteit.

(67) Om de systemische impact van het risico van concentratie van ICT-derden te beperken, wordt in deze verordening een evenwichtige aanpak bepleit door middel van een flexibele en geleidelijke aanpak van zulk concentratierisico. Het opleggen van onwrikbare risicoplafonds of strikte beperkingen zou immers de bedrijfsvoering kunnen belemmeren en de contractvrijheid kunnen beperken. Financiële entiteiten moeten de contractuele overeenkomsten die zij willen sluiten, grondig onderzoeken om na te gaan hoe groot de kans is dat een dergelijk risico zich zal voordoen, onder meer door overeenkomsten tot onderaanbesteding onder de loep te nemen, met name indien die worden gesloten met derde aanbieders van ICT-diensten die in een derde land zijn gevestigd. Ten behoeve van een billijk evenwicht tussen contractuele vrijheid en financiële stabiliteit wordt het op dit ogenblik niet wenselijk geacht te voorzien in regels betreffende strikte plafonds voor en beperkingen van ICT-blootstellingen aan derden. Een lead overseer die conform deze verordening wordt aangewezen, moet in het kader van het oversightkader bijzondere aandacht schenken aan kritieke derde aanbieders van ICT-diensten en dient een volledig beeld te krijgen van de omvang van onderlinge afhankelijkheden, specifieke gevallen aan het licht te brengen waarin een hoge mate van concentratie van kritieke derde aanbieders van ICT-diensten in de Unie waarschijnlijk de stabiliteit en integriteit van het financiële stelsel van de Unie onder druk zal zetten, en, wanneer zo'n specifiek risico wordt ontdekt, in dialoog treden met de betrokken kritieke derde aanbieders van ICT-diensten.

(68) Om regelmatig het vermogen te evalueren en te monitoren van een derde aanbieder van ICT-diensten, veilig diensten aan een financiële entiteit te verlenen zonder nadelige gevolgen voor de digitale operationele weerbaarheid van een financiële entiteit, moeten een aantal belangrijke elementen in de contractuele overeenkomsten met derde aanbieders van ICT-diensten worden geharmoniseerd. Dergelijke harmonisatie moet minimumgebieden bestrijken die cruciaal zijn voor een volledige monitoring door de financiële entiteit van de risico's die gepaard kunnen gaan met het in de arm nemen van derde aanbieders van ICT-diensten. Dit gelet op de noodzaak voor een financiële entiteit om haar digitale weerbaarheid veilig te stellen; een financiële entiteit is immers sterk afhankelijk van de stabiliteit, de functionaliteit, de beschikbaarheid en de veiligheid van de ICT-diensten die haar worden verleend.

(69) Indien er opnieuw moet worden onderhandeld over contractuele overeenkomsten om deze af te stemmen op de vereisten van deze verordening, moeten financiële entiteiten en derde aanbieders van ICT-diensten ervoor zorgen dat de belangrijkste contractuele bepalingen die deze verordening voorschrijft, in de nieuwe overeenkomsten worden opgenomen.

(70) De definitie van "kritieke of belangrijke functie" in deze verordening omvat de "kritieke functies" als bedoeld in artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU van het Europees Parlement en de Raad ([20]). Dienovereenkomstig worden functies die overeenkomstig Richtlijn 2014/59/EU als kritiek worden beschouwd, opgenomen in de definitie van kritieke functies in de zin van deze verordening.

(71) Ongeacht het kritieke karakter of het belang van de door ICT-diensten ondersteunde functie, moeten contractuele overeenkomsten met name de volledige beschrijvingen bevatten van functies en diensten, van de locaties waar dergelijke functies worden geleverd en waar data worden verwerkt, alsmede een indicatie van de beschrijvingen van het dienstverleningsniveau. Andere cruciale elementen om de monitoring door de financiële entiteit van het ICT-risico van derde aanbieders mogelijk te maken, zijn: contractuele bepalingen waarin wordt gespecificeerd hoe derde aanbieders van ICT-diensten de toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens verzekeren, bepalingen tot vaststelling van de relevante garanties inzake de toegang, het herstel en de teruggave in geval van insolventie, afwikkeling of stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten. Ook belangrijk zijn contractuele bepalingen waarin van de derde aanbieder van ICT-

([20]) Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 82/891/EEG van de Raad en de Richtlijnen 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU en 2013/36/EU en de Verordeningen (EU) nr. 1093/2010 en (EU) nr. 648/2012 van het Europees Parlement en de Raad (PB L 173 van 12.6.2014, blz. 190).

diensten wordt verlangd dat deze assistentie biedt bij ICT-incidenten in verband met de diensten die hij verleent, en wel zonder extra kosten of tegen kosten die van tevoren zijn afgesproken, alsmede contractuele bepalingen waarin de derde aanbieder van ICT-diensten wordt verplicht volledig samen te werken met de bevoegde autoriteiten en de afwikkelingsautoriteiten van de financiële entiteit, en bepalingen inzake beëindigingsrechten en de bijbehorende minimumopzegtermijnen voor de beëindiging van de contractuele overeenkomsten, in overeenstemming met de verwachtingen van de bevoegde autoriteiten en de afwikkelingsautoriteiten.

(72) Benevens dergelijke contractuele bepalingen, en om ervoor te zorgen dat financiële entiteiten de volledige controle behouden over alle ontwikkelingen op het niveau van derde partijen die hun ICT-beveiliging in het gedrang kunnen brengen, moeten de contracten voor de levering van ICT-diensten die kritieke of belangrijke functies ondersteunen, ook voorzien in het volgende: specificatie van de volledige beschrijvingen van het dienstenniveau, met precieze kwantitatieve en kwalitatieve prestatiedoelstellingen, opdat zonder onnodige vertraging corrigerende maatregelen kunnen worden getroffen indien de overeengekomen dienstenniveaus niet gehaald worden; de relevante kennisgevingsperioden en rapportageverplichtingen van de derde aanbieder van ICT-diensten in geval van ontwikkelingen met een potentiële materiële impact op het vermogen van de derde aanbieder van ICT-diensten om hun respectieve ICT-diensten daadwerkelijk te leveren; een verplichting voor de derde aanbieder van ICT-diensten om bedrijfsnoodplannen uit te voeren en te testen en te beschikken over ICT-beveiligingsmaatregelen, -instrumenten en -beleidsmaatregelen die een veilige dienstverlening mogelijk maken, en om deel te nemen aan en volledig mee te werken aan de TLPT die door de financiële entiteit wordt uitgevoerd.

(73) Contracten voor het leveren van ICT-diensten ter ondersteuning van kritieke of belangrijke functies moeten tevens bepalingen bevatten inzake rechten van toegang, inspectie en audit door de financiële entiteit of een aangewezen derde, alsook het recht om kopieën te maken. Dit zijn cruciale instrumenten voor de permanente monitoring door de financiële entiteit van de prestaties van de derde aanbieder van ICT-diensten, evenals de volledige medewerking van de dienstverlener tijdens inspecties. Evenzo moet de autoriteit van de financiële entiteit het recht hebben om, na kennisgeving, de derde aanbieder van ICT-diensten te inspecteren en te auditen, onder het voorbehoud van de bescherming van vertrouwelijke informatie.

(74) Dergelijke contractuele overeenkomsten moeten ook voorzien in specifieke exitstrategieën die met name verplichte overgangsperioden mogelijk maken waarin de derde aanbieder van ICT-diensten de relevante diensten moeten blijven verrichten om zo het risico op verstoringen bij de financiële entiteit te beperken, dan wel de financiële entiteit in staat te stellen daadwerkelijk over te stappen naar andere derde aanbieders van ICT-diensten, of anders over te gaan op interne oplossingen, een en ander in overeenstemming met de complexiteit van de verleende ICT-dienst. Bovendien moeten financiële entiteiten die binnen het toepassingsgebied van Richtlijn 2014/59/EU vallen, ervoor zorgen dat de relevante contracten voor ICT-diensten degelijk en volledig afdwingbaar zijn in geval van afwikkeling van die financiële entiteiten. Daarom moeten die financiële entiteiten erop toezien dat, in overeenstemming met de verwachtingen van de afwikkelingsautoriteiten, hun contracten voor ICT-diensten afwikkelingsbestendig zijn. Zolang zij aan hun betalingsverplichtingen blijven voldoen, moeten die financiële entiteiten er onder meer voor zorgen dat hun contracten voor ICT-diensten clausules bevatten voor niet-beëindiging, niet-opschorting en niet-wijziging op grond van herstructurering of afwikkeling.

(75) Bovendien kan het vrijwillige gebruik van modelcontractbepalingen die door overheidsinstellingen of de instellingen van de Unie zijn ontwikkeld, en in het bijzonder het gebruik van door de Commissie ontwikkelde bepalingen inzake cloudcomputingdiensten, de financiële entiteiten en derde aanbieders van ICT-diensten meer zekerheid bieden doordat zij meer rechtszekerheid hebben over het gebruik van cloudcomputingdiensten in de financiële sector, in volledige overeenstemming met de vereisten en verwachtingen van het Unierecht inzake financiële diensten. De ontwikkeling van modelcontractbepalingen bouwt voort op maatregelen die al waren gepland in het FinTech-actieplan uit 2018. Daarin werd het voornemen van de Commissie aangekondigd om de ontwikkeling van modelcontractbepalingen voor de uitbesteding van cloudcomputingdiensten door financiële entiteiten aan te moedigen en te vergemakkelijken, waarbij gebruik wordt gemaakt van sectoroverschrijdende inspanningen van belanghebbenden op het gebied van cloudcomputingdiensten, die de Commissie met hulp van de financiële sector heeft vergemakkelijkt.

(76) Om de convergentie en efficiëntie van de verschillende benaderingen voor toezicht op risico's bij derde aanbieders van ICT-diensten in de financiële sector te bevorderen, alsmede om de digitale operationele weerbaarheid te versterken van financiële entiteiten die afhankelijk zijn van kritieke derde aanbieders van ICT-diensten voor het verlenen van ICT-diensten die het leveren van financiële diensten ondersteunen, en zo bij te dragen aan het behoud van de stabiliteit van het financiële stelsel van de Unie en de integriteit van de interne markt voor financiële diensten, moeten kritieke derde aanbieders van ICT-diensten onderworpen zijn aan een oversightkader van de Unie. Hoewel de oprichting van het oversightkader gerechtvaardigd is door de toegevoegde waarde van maatregelen op het

niveau van de Unie en door de inherente rol en specifieke kenmerken van het gebruik van ICT-diensten bij de verlening van financiële diensten, moet tegelijkertijd in herinnering worden gebracht dat deze oplossing alleen geschikt lijkt in het kader van deze verordening, die specifiek betrekking heeft op digitale operationele weerbaarheid in de financiële sector. Dit oversightkader mag echter niet worden beschouwd als een nieuw model voor Unietoezicht op andere gebieden van financiële diensten en activiteiten.

(77) Het oversightkader moet alleen van toepassing zijn op kritieke derde aanbieders van ICT-diensten. Daarom moet er een aanwijzingsregeling komen waarmee de omvang en de aard van de afhankelijkheid van de financiële sector van dergelijke derde aanbieders van ICT-diensten kan worden beoordeeld. Die regeling moet kwantitatieve en kwalitatieve criteria omvatten om de kritische parameters vast te stellen op basis waarvan entiteiten al dan niet onder het oversightkader vallen. Om de nauwkeurigheid van die beoordeling te waarborgen, en ongeacht de bedrijfsstructuur van de derde aanbieder van ICT-diensten, moet in deze criteria in het geval van een derde aanbieder van ICT-diensten die deel uitmaakt van een grotere groep, gekeken worden naar de gehele groepsstructuur van de derde aanbieder van ICT-diensten. Enerzijds moeten kritieke derde aanbieders van ICT-diensten die niet automatisch worden aangewezen op grond van de toepassing van die criteria, de mogelijkheid hebben om vrijwillig deel te nemen aan het oversightkader. Anderzijds moeten derde aanbieders van ICT-diensten die reeds onderworpen zijn aan oversightregelingen die de uitvoering van de taken van het Europees Stelsel van centrale banken als bedoeld in artikel 127, lid 2, VWEU, steunen, worden vrijgesteld.

(78) Evenzo moeten financiële entiteiten die ICT-diensten verlenen aan andere financiële entiteiten, en die weliswaar behoren tot de categorie van derde aanbieders van ICT-diensten als bedoeld in deze verordening, ook van het oversightkader worden vrijgesteld. Zij zijn immers reeds onderworpen zijn aan toezichtsregelingen die zijn opgericht bij het desbetreffende Unierecht inzake financiële diensten. In voorkomend geval moeten de bevoegde autoriteiten bij hun toezichtactiviteiten letten op het ICT-risico voor financiële entiteiten dat uitgaat van financiële entiteiten die zelf ICT-diensten verlenen. Evenzo moet, gelet op de reeds bestaande regelingen voor risicobewaking op groepsniveau, dezelfde vrijstelling gelden voor derde aanbieders van ICT-diensten die hoofdzakelijk diensten verlenen aan entiteiten van hun eigen groep. Derde aanbieders van ICT-diensten die uitsluitend in één lidstaat ICT-diensten verlenen aan financiële entiteiten die ook uitsluitend in die lidstaat actief zijn, moeten ook van de aanwijzingsregeling worden vrijgesteld wegens het beperkte karakter van hun activiteiten en het ontbreken van gevolgen over de grenzen heen.

(79) De digitale transformatie in de financiële dienstverlening heeft geleid tot een ongekende mate van gebruik van en afhankelijkheid van ICT-diensten. Aangezien het ondenkbaar is geworden dat financiële diensten worden verleend zonder gebruik te maken van cloudcomputingdiensten, softwareoplossingen en datadiensten, is het financiële ecosysteem van de Unie intrinsiek afhankelijk geworden van bepaalde ICT-diensten die door leveranciers van die diensten worden verleend. Sommige van die leveranciers die innovatoren zijn in de ontwikkeling en toepassing van op ICT gebaseerde technologieën, spelen een belangrijke rol bij de levering van financiële diensten of zijn geïntegreerd in de waardeketen van financiële diensten. Zo zijn zij kritiek geworden voor de stabiliteit en integriteit van het financiële stelsel van de Unie. Deze wijdverbreide afhankelijkheid van diensten van kritieke derde aanbieders van ICT-diensten, in combinatie met de onderlinge afhankelijkheid van de informatiesystemen van verschillende marktdeelnemers, creëert een rechtstreeks en potentieel ernstig risico voor het systeem van financiële diensten van de Unie en voor de continuïteit van de verlening van financiële diensten indien kritieke derde aanbieders van ICT-diensten zouden worden getroffen door operationele verstoringen of belangrijke cyberincidenten. Cyberincidenten kunnen zich bij uitstek veel sneller in het gehele financiële stelsel vermenigvuldigen en zich daarin in een aanzienlijk sneller tempo verspreiden dan andere soorten risico's die in de financiële sector worden gemonitord. Ook kunnen cyberincidenten zich over meerdere sectoren en over geografische grenzen heen uitstrekken. Zij kunnen uitgroeien tot een systemische crisis waarin het vertrouwen in het financiële stelsel wordt uitgehold door de verstoring van functies die de reële economie ondersteunen, of door aanzienlijke financiële verliezen die een niveau kunnen bereiken waar het financiële stelsel niet tegen bestand is of waarvoor zware maatregelen ter schokabsorptie moeten worden genomen. Om dit soort scenario's die de financiële stabiliteit en integriteit van de Unie in gevaar te brengen, te voorkomen, is het essentieel de praktijken inzake toezicht op ICT-risico's bij derden in de financiële sector meer op één lijn te brengen, met name door middel van nieuwe regels die oversight van de Unie op kritieke derde aanbieders van ICT-diensten mogelijk maken.

(80) Het oversightkader is grotendeels afhankelijk van de mate van samenwerking tussen de lead overseer en de kritieke derde aanbieder van ICT-diensten die aan financiële entiteiten diensten levert die van invloed zijn op de verlening van financiële diensten door deze entiteiten. Succesvol oversight is onder meer gebaseerd op het vermogen van de lead overseer, daadwerkelijk monitoringmissies en -inspecties uit te voeren om de regels, de controles en de processen die door kritieke derde aanbieders van ICT-diensten worden gebruikt, te beoordelen, alsook de potentiële cumulatieve impact van hun activiteiten op de financiële stabiliteit en de integriteit van het financiële stelsel te beoordelen. Tegelijkertijd is het cruciaal dat kritieke derde aanbieders van ICT-diensten de aanbevelingen van de lead overseer opvolgen en diens bevindingen op zorgwekkende punten ter harte nemen. Aangezien een gebrek aan medewerking van een kritieke derde aanbieder van ICT-diensten die diensten verleent welke van invloed zijn op de verlening van financiële diensten, zoals een weigering om toegang te verlenen tot zijn kantoren of informatie te verstrekken, uiteindelijk de lead overseer essentiële instrumenten voor de beoordeling van ICT-risico's van derden zou ontnemen, alsook negatieve gevolgen zou kunnen hebben voor de financiële stabiliteit en de integriteit van het financiële stelsel, moet ook worden voorzien in een sanctieregeling die past bij een eventuele weigering om mee te werken.

(81) Tegen deze achtergrond mag de noodzaak voor de lead overseer om dwangsommen op te leggen, waarmee kritieke derde aanbieders van ICT-diensten kunnen worden gedwongen te voldoen aan de transparantie- en toegangsverplichtingen van deze verordening, niet in gevaar komen door moeilijkheden bij de inning van deze dwangsommen wanneer het kritieke derde aanbieders van ICT-diensten betreft die in derde landen zijn gevestigd. Ten behoeve van de afdwingbaarheid van dergelijke sancties en om een snelle inzet mogelijk te maken van procedures waarbij de rechten van verdediging van kritieke derde aanbieders van ICT-diensten in het kader van de aanwijzingsregeling en de uitvaardiging van aanbevelingen worden gehandhaafd, moeten die kritieke derde aanbieders van ICT-diensten, die diensten aan financiële entiteiten verlenen welke van invloed zijn op de verlening van financiële diensten, worden verplicht een adequate zakelijke aanwezigheid in de Unie te hebben. Gezien de aard van het oversight en het ontbreken van vergelijkbare regelingen in andere rechtsgebieden, zijn er geen geschikte alternatieve mechanismen om deze doelstelling te waarborgen door middel van doeltreffende samenwerking met financiële toezichthouders in derde landen bij de monitoring van de impact van digitale operationele risico's van systemische derde aanbieders van ICT-diensten die worden aangemerkt als kritieke derde aanbieders van ICT-diensten die in derde landen zijn gevestigd. Om ICT-diensten aan financiële entiteiten in de Unie te kunnen blijven verlenen, moet een in een derde land gevestigde derde aanbieder van ICT-diensten die overeenkomstig deze verordening als cruciaal is aangewezen, binnen twaalf maanden na aanwijzing al het nodige doen om ervoor te zorgen dat hij een aanwezigheid in de Unie heeft door een dochteronderneming op te richten, zoals gedefinieerd in het acquis van de Unie, namelijk in Richtlijn 2013/34/EU van het Europees Parlement en de Raad ([21]).

(82) De eis om een dochteronderneming op te richten in de Unie mag de kritieke derde aanbieder van ICT-diensten niet beletten ICT-diensten en de daarmee verband houdende technische ondersteuning te verlenen vanuit faciliteiten en infrastructuur die zich buiten de Unie bevinden. Deze verordening legt geen verplichting tot datalokalisatie op, aangezien de verordening niet voorziet in opslag of verwerking van data binnen de Unie.

(83) Kritieke derde aanbieders van ICT-diensten moeten in staat zijn overal ter wereld ICT-diensten aan te bieden, dus niet noodzakelijk of niet alleen vanuit bedrijfsruimten die zich in de Unie bevinden. Oversightactiviteiten moeten eerst worden uitgevoerd in bedrijfsruimten binnen de Unie en door interactie met in de Unie gevestigde entiteiten, met inbegrip van de dochterondernemingen die zijn opgericht door kritieke derde aanbieders van ICT-diensten op grond van deze verordening. Het is evenwel denkbaar dat dit soort acties in de Unie ontoereikend zijn om de lead overseer in staat te stellen zijn taken uit hoofde van deze verordening volledig en doeltreffend uit te voeren. De lead overseer moet daarom ook in derde landen toezicht kunnen uitoefenen. De uitoefening van zijn bevoegdheid tot oversight in derde landen moet de lead overseer in staat stellen de faciliteiten te onderzoeken van waaruit de ICT-diensten of de technische ondersteuningsdiensten daadwerkelijk door de kritieke derde aanbieder van ICT-diensten worden geleverd of beheerd; ook moet dit oversight de lead overseer een volledig en operationeel inzicht bieden in het ICT-risicobeheer van de kritieke derde aanbieder van ICT-diensten. De mogelijkheid voor de lead overseer om, in zijn hoedanigheid van agentschap van de Unie, bevoegdheden uit te oefenen buiten het grondgebied van de Unie moet naar behoren aan voorwaarden zijn gebonden, met name de toestemming van de betrokken kritieke derde aanbieder van ICT-diensten. Evenzo moeten de relevante autoriteiten van het derde land in kennis worden gesteld van de uitoefening van de activiteiten van de lead overseer op hun grondgebied en moeten zij daartegen geen

([21]) Richtlijn 2013/34/EU van het Europees Parlement en van de Raad van 26 juni 2013 betreffende de jaarlijkse financiële overzichten, geconsolideerde financiële overzichten en aanverwante verslagen van bepaalde ondernemingsvormen, tot wijziging van Richtlijn 2006/43/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijnen 78/660/EEG en 83/349/EEG van de Raad (PB L 182 van 29.6.2013, blz. 19).

bezwaar hebben gemaakt. Gelet op het belang van een efficiënte uitvoering van deze activiteiten, en onverminderd de bevoegdheden van de instellingen van de Unie en van de lidstaten op dit terrein, moeten de bevoegdheden van de lead overseer tevens ten volle worden verankerd in regelingen voor administratieve samenwerking met de betrokken autoriteiten van het derde land. Daarom moet deze verordening de ETA's in staat stellen met de autoriteiten in derde landen regelingen voor administratieve samenwerking te treffen die voor het overige geen wettelijke verplichtingen voor de Unie of de lidstaten mogen creëren.

(84) Om de communicatie met de lead overseer te vergemakkelijken en een passende vertegenwoordiging te waarborgen, moeten kritieke derde aanbieders van ICT-diensten die deel uitmaken van een groep, één rechtspersoon als hun coördinatiepunt aanwijzen.

(85) Het oversightkader mag geen afbreuk doen aan de bevoegdheid van de lidstaten om hun eigen oversight- of monitoringtaken uit te voeren met betrekking tot derde aanbieders van ICT-diensten die niet als kritiek zijn aangewezen in de zin van deze verordening, maar die op nationaal niveau belangrijk worden geacht.

(86) Om de meerlagige institutionele architectuur op het gebied van financiële diensten te benutten, moet het Gemengd Comité van de ETA's blijven zorgen voor algehele sectoroverschrijdende coördinatie van alle aangelegenheden die verband houden met ICT-risico's, in overeenstemming met de taken van het Comité op het gebied van cyberbeveiliging. Het Comité moet worden ondersteund door een nieuw subcomité (het oversightforum) dat voorbereidende werkzaamheden verricht voor zowel de afzonderlijke besluiten die gericht zijn tot kritieke derde aanbieders van ICT-diensten als voor het doen van collectieve aanbevelingen, met name in verband met het benchmarken van de oversightprogramma's voor kritieke derde aanbieders van ICT-diensten en het in kaart brengen van beste praktijken voor het omgaan van ICT-concentratierisico's.

(87) Om ervoor te zorgen dat op het niveau van de Unie adequaat en doeltreffend toezicht wordt uitgeoefend op kritieke derde aanbieders van ICT-diensten, wordt in deze verordening bepaald dat ieder van de drie ETA's kan worden aangewezen als lead overseer. De individuele toewijzing van een kritieke derde aanbieder van ICT-diensten aan een van de drie ETA's moet gebaseerd zijn op een beoordeling van de dominerende positie van financiële entiteiten die actief zijn in de financiële sectoren waarvoor die ETA verantwoordelijk is. Deze benadering moet leiden tot een evenwichtige verdeling van taken en verantwoordelijkheden over de drie ETA's die oversightfuncties hebben, en leiden tot een optimaal gebruik van personele middelen en technische expertise die in ieder van de drie ETA's voorhanden zijn.

(88) Lead overseers moeten de nodige bevoegdheden krijgen om onderzoeken te verrichten, inspecties ter plaatse en daarbuiten uit te voeren in de gebouwen en op de locaties van kritieke derde aanbieders van ICT-diensten, en volledige en actuele informatie te verkrijgen. Die bevoegdheden moeten de lead overseer in staat stellen een gedegen inzicht te krijgen in het soort, de omvang en de impact van het ICT-risico van derden voor financiële entiteiten en, uiteindelijk, voor het financiële stelsel van de Unie. De ETA's moeten de leiding over het oversight krijgen. Dit is een voorwaarde voor een goed begrip van en een betere greep op de systemische dimensie van ICT-risico's in de financiële sector. De impact van kritieke derde aanbieders van ICT-diensten op de financiële sector in de Unie en de mogelijke problemen als gevolg van het daaraan verbonden ICT-concentratierisico vragen om een gezamenlijke aanpak op het niveau van de Unie. De gelijktijdige en afzonderlijke uitvoering van meerdere audits en toegangsrechten door een reeks van bevoegde autoriteiten, zonder enige of slechts met weinig coördinatie, zou het de financiële toezichthouders onmogelijk maken een volledig en alomvattend overzicht te krijgen van het ICT-risico van derden in de Unie. Ook zou dit leiden tot redundantie, extra lasten en complexiteit voor kritieke derde aanbieders van ICT-diensten, die immers zouden worden onderworpen aan tal van verzoeken om monitoring en inspectie.

(89) Gezien de aanzienlijke gevolgen voor de derde aanbieder van ICT-diensten die als kritiek wordt aangewezen, moet deze verordening ervoor zorgen dat de rechten van eenmaal aangewezen derde aanbieders van ICT-diensten gedurende de gehele tenuitvoerlegging van het oversightkader worden geëerbiedigd. Voordat een dienstverlener als kritiek wordt aangewezen, moet deze bijvoorbeeld het recht hebben een gemotiveerde verklaring in te dienen bij de lead overseer met alle informatie die relevant is voor de beoordeling in verband met de eventuele aanwijzing. Aangezien de lead overseer de bevoegdheid moet hebben om aanbevelingen over ICT-risico's te doen en oplossingen daarvoor aan te dragen — waaronder de bevoegdheid zich te verzetten tegen contractueleovereenkomsten die uiteindelijk gevolgen zullen hebben voor de stabiliteit van de financiële entiteit of zelfs van het gehele financiële stelsel — moeten kritieke derde aanbieders van ICT-diensten ook de mogelijkheid krijgen om voorafgaand aan de definitieve opstelling van deze aanbevelingen uitleg te geven over de verwachte gevolgen van de

in de aanbeveling opgenomen oplossingen voor klanten die entiteiten zijn welke buiten het toepassingsgebied van deze verordening vallen en om oplossingen te formuleren om risico's te mitigeren. Kritieke derde aanbieders van ICT-diensten die het niet eens zijn met de aanbevelingen, moeten de gelegenheid hebben een gemotiveerde uitleg te geven van hun voornemen om de aanbevelingen niet te onderschrijven. Indien zulk een gemotiveerde toelichting niet wordt gegeven of ontoereikend wordt bevonden, moet de lead overseer een openbare kennisgeving van de niet-naleving doen.

(90) In het kader van het prudentieel toezicht op financiële entiteiten moeten de bevoegde autoriteiten naar behoren nagaan of de aanbevelingen van de lead overseer inhoudelijk worden nageleefd. De bevoegde autoriteiten moeten van financiële entiteiten kunnen vereisen dat zij aanvullende maatregelen nemen om de in de aanbevelingen van de lead overseer genoemde risico's te verhelpen, en dat zij te zijner tijd bericht doen uitgaan dat dit gebeurd is. Indien de lead overseer aanbevelingen richt tot kritieke derde aanbieders van ICT-diensten die onder toezicht staan uit hoofde van Richtlijn (EU) 2022/2555 , moeten de bevoegde autoriteiten op vrijwillige basis en alvorens aanvullende maatregelen te nemen de bevoegde autoriteiten uit hoofde van die richtlijn kunnen raadplegen om zo een gecoördineerde aanpak van de betrokken kritieke derde aanbieders van ICT-diensten te bevorderen.

(91) Bij de uitoefening van het oversight moeten drie operationele beginselen gelden, die gericht zijn op: a) nauwe coördinatie tussen de ETA's in hun rol van lead overseer, en wel via een gezamenlijk oversightnetwerk (*joint oversight network* — JON); b) consistentie met het kader dat is vastgelegd in Richtlijn (EU) 2022/2555 (door middel van een vrijwillige raadpleging van organen uit hoofde van die richtlijn om zo overlapping van maatregelen ten aanzien van kritieke derde aanbieders van ICT-diensten te voorkomen, en c) het toepassen van zorgvuldigheid om het potentiële risico te beperken van verstoring van diensten die door kritieke derde aanbieders van ICT-diensten worden verleend aan klanten die entiteiten zijn welke buiten het toepassingsgebied van deze verordening vallen.

(92) Het oversightkader mag niet in de plaats komen van, noch op enigerlei wijze of ten enigen dele in de plaats treden van het vereiste voor financiële entiteiten om zelf de risico's te beheren die voortvloeien uit het gebruik van derde aanbieders van ICT-diensten, óók hun verplichting om permanent de contractuele overeenkomsten te monitoren die zijn gesloten met kritieke derde aanbieders van ICT-diensten. Evenzo mag het oversightkader geen afbreuk doen aan de volledige verantwoordelijkheid van financiële entiteiten voor de naleving en de kwijting van alle wettelijke verplichtingen die zijn vastgelegd in deze verordening en in het desbetreffende recht inzake financiële diensten.

(93) Om doublures en overlappingen te voorkomen, moeten de bevoegde autoriteiten ervan afzien, zelf maatregelen te nemen om de risico's van de kritieke derde aanbieder van ICT-diensten te monitoren. Zij moeten in dit verband vertrouwen op de beoordeling van de lead overseer in kwestie. Alle maatregelen moeten in ieder geval van tevoren worden gecoördineerd en overeengekomen met de lead overseer, gelet op de uitoefening van diens taken in het oversightkader.

(94) Om convergentie op internationaal niveau inzake het gebruik van beste praktijken bij de toetsing en monitoring van digitaal risicobeheer bij derde aanbieders van ICT-diensten te bevorderen, moeten de ETA's worden aangemoedigd samenwerkingsregelingen te sluiten met toezichthoudende en regelgevende autoriteiten van derde landen die op dit terrein werkzaam zijn.

(95) Om de specifieke vaardigheden, de technische expertise en de expertise van deskundigen op het gebied van operationele en ICT-risico's binnen de bevoegde autoriteiten, de drie ETA's, en, op vrijwillige basis, de uit hoofde van Richtlijn (EU) 2022/2555 bevoegde autoriteiten ten volle te benutten, moet de lead overseer gebruikmaken van nationale toezichtcapaciteiten en -kennis, en specifieke onderzoeksteams oprichten voor iedere kritieke derde aanbieder van ICT-diensten. Multidisciplinaire teams moeten worden samengebracht ter ondersteuning van de voorbereiding en de uitvoering van oversightactiviteiten, inclusief algemene onderzoeken en inspecties ter plaatse bij kritieke derde aanbieders van ICT-diensten, alsook ter ondersteuning van eventuele follow-up hiervan indien dit nodig is.

(96) Hoewel het de bedoeling is dat de kosten van oversighttaken volledig worden gefinancierd uit vergoedingen die worden aangerekend aan kritieke derde aanbieders van ICT-diensten, zullen de ETA's waarschijnlijk vóór de start van het oversightkader kosten maken voor de implementatie van specifieke ICT-systemen ter ondersteuning van het aanstaande oversight, aangezien deze specifieke systemen vooraf moeten worden ontwikkeld en uitgerold. Deze verordening voorziet daarom in een hybride financieringsmodel: het oversightkader moet volledig worden gefinancierd uit vergoedingen, terwijl de ontwikkeling van de ICT-systemen van de ETA's moet worden gefinancierd uit bijdragen van de Unie en de bevoegde nationale autoriteiten.

(97) De bevoegde autoriteiten moeten over alle toezicht-, onderzoeks- en sanctiebevoegdheden beschikken die vereist zijn willen zij de taken uit hoofde van deze verordening naar behoren kunnen uitvoeren. Zij moeten in beginsel de administratieve strafmaatregelen die zij opleggen, bekendmaken. Aangezien financiële entiteiten en derde aanbieders van ICT-diensten gevestigd kunnen zijn in verschillende lidstaten en kunnen ressorteren onder het toezicht van verschillende bevoegde autoriteiten, moet de toepassing van deze verordening vergemakkelijkt worden via, enerzijds, nauwe samenwerking tussen de relevante bevoegde autoriteiten, waaronder de ECB wat betreft de specifieke taken die de bank bij Verordening (EU) nr. 1024/2013 van de Raad zijn opgedragen, en, anderzijds, overleg met de ETA's via wederzijdse uitwisseling van informatie en verlening van bijstand bij relevante toezichtactiviteiten.

(98) Om de criteria voor de aanwijzing van derde aanbieders van ICT-diensten tot kritieke dienstverleners kwantitatief en kwalitatief aan te scherpen en om de oversightvergoedingen te harmoniseren, moet aan de Commissie de bevoegdheid worden gedelegeerd om overeenkomstig artikel 290 VWEU handelingen vast te stellen ter aanvulling van deze verordening, en wel door nader te specificeren welke systemische impact een storing of een operationele uitval van een derde aanbieder van ICT-diensten zou kunnen hebben voor de financiële entiteiten waaraan deze derde aanbieder ICT-diensten verleent, het aantal mondiaal systeemrelevante instellingen (MSI's) of andere systeemrelevante instellingen (ASI's) die afhankelijk zijn van de derde aanbieder van ICT-diensten in kwestie, het aantal derde aanbieders van ICT-diensten dat op een bepaalde markt actief is, de kosten van de migratie van data en de ICT-werkbelasting naar een andere derde aanbieder van ICT-diensten, alsook het bedrag van de oversightvergoedingen en de wijze waarop deze moeten worden betaald. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat deze raadplegingen plaatsvinden in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([22]). Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen moeten het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip ontvangen als de deskundigen van de lidstaten, en moeten hun deskundigen systematisch toegang hebben tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(99) Technische reguleringsnormen moeten een consistente harmonisatie van de in deze verordening neergelegde voorschriften bewerkstelligen. In hun rol van organen met hooggespecialiseerde expertise moeten de ETA's ontwerpen van technische reguleringsnormen ontwikkelen die geen beleidskeuzen inhouden en die aan de Commissie moeten worden voorgelegd. Er moeten technische reguleringsnormen worden ontwikkeld op het gebied van ICT-risicobeheer, rapportage van ernstige ICT-incidenten, tests, en op het gebied van essentiële vereisten voor een degelijke monitoring van het ICT-risico van derde dienstverleners. De Commissie en de ETA's dienen ervoor te zorgen dat deze normen en vereisten door alle financiële entiteiten kunnen worden toegepast op een wijze die in verhouding staat tot hun omvang en algehele risicoprofiel, alsook de aard, de omvang en de complexiteit van de entiteiten en hun activiteiten. De Commissie dient bevoegd te zijn deze technische uitvoeringsnormen vast te stellen bij gedelegeerde handeling, krachtens artikel 290 VWEU en in overeenstemming met artikel 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

(100) Om de vergelijkbaarheid van meldingen van ernstige ICT-incidenten en van ernstige betalingsgerelateerde operationele of beveiligingsincidenten te vergemakkelijken en om te zorgen voor transparantie inzake contractuele overeenkomsten voor het gebruik van derde aanbieders van ICT-diensten moeten de ETA's technische uitvoeringsnormen ontwikkelen waarin gestandaardiseerde templates, formulieren en procedures voor het melden van ernstige ICT-incidenten en van ernstige betalingsgerelateerde operationele of beveiligingsincidenten door financiële entiteiten worden vastgelegd, alsook gestandaardiseerde templates voor het informatieregister. Bij het ontwikkelen van deze normen moeten de ETA's letten op de omvang en het algemene risicoprofiel van de financiële entiteit, alsook met de aard, de schaal en de complexiteit van haar diensten en activiteiten. De Commissie dient bevoegd te zijn bij uitvoeringshandeling deze technische uitvoeringsnormen vast te stellen, krachtens artikel 291 VWEU en in overeenstemming met artikel 15 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

([22]) PB L 123 van 12.5.2016, blz. 1.

(101) Aangezien verdere vereisten reeds zijn vastgesteld bij gedelegeerde en uitvoeringshandelingen op basis van technische regulerings- en uitvoeringsnormen in de Verordeningen (EG) nr. 1060/2009 ([23]), (EU) nr. 648/2012 ([24]), (EU) nr. 600/2014 ([25]) en (EU) nr. 909/2014 van het Europees Parlement en de Raad ([26]), is het passend de ETA's, afzonderlijk of gezamenlijk via het Gemengd Comité, opdracht te geven bij de Commissie technische regulerings- of uitvoeringsnormen in te dienen met het oog op de vaststelling van gedelegeerde en uitvoeringshandelingen waarin de bestaande regels voor ICT-risicobeheer worden overgenomen en bijgewerkt.

(102) Aangezien deze verordening, samen met Richtlijn (EU) 2022/2556 van het Europees Parlement en de Raad ([27]) , een consolidatie inhoudt van de bepalingen inzake ICT-risicobeheer in verschillende verordeningen en richtlijnen van het acquis van de Unie op het gebied van financiële diensten, onder meer de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, en (EU) nr. 909/2014 en Verordening (EU) 2016/1011 van het Europees Parlement en de Raad ([28]), moeten deze verordeningen ten behoeve van volledige consistentie worden gewijzigd om te verduidelijken dat de relevante bepalingen inzake ICT-risico's in de onderhavige verordening zijn opgenomen.

(103) Bijgevolg moet de werkingssfeer van de relevante artikelen in verband met operationele risico's, waarvoor in de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 machtigingen zijn verleend om gedelegeerde handelingen en uitvoeringshandelingen vast te stellen, worden beperkt teneinde alle bepalingen betreffende de aspecten van digitale operationele weerbaarheid die thans deel uitmaken van genoemde verordeningen, over te nemen in de onderhavige verordening.

(104) Het potentiële systemische cyberrisico bij het gebruik van ICT-infrastructuren die de exploitatie van betalingssystemen en de verrichting van activiteiten ter betalingsverwerking mogelijk maken, moet op het niveau van de Unie naar behoren worden aangepakt door middel van geharmoniseerde regels inzake digitale weerbaarheid. Daartoe moet de Commissie onverwijld beoordelen of het toepassingsgebied van deze verordening moet worden herzien en moet zij deze evaluatie afstemmen op de resultaten van de uitgebreide evaluatie waarin Richtlijn (EU) 2015/2366 voorziet. Talrijke grootschalige aanvallen in de afgelopen tien jaar tonen aan hoe betalingssystemen kwetsbaar zijn geworden voor cyberdreigingen. Betalingssystemen en activiteiten inzake betalingsverwerkingen vormen de belangrijkste schakel van de keten van betalingsdiensten en zijn sterk verweven met het algemene financiële stelsel, waardoor zij van cruciaal belang zijn geworden voor de werking van de financiële markten van de Unie. Cyberaanvallen op dergelijke systemen kunnen ernstige operationele bedrijfsverstoringen veroorzaken met rechtstreekse gevolgen voor belangrijke economische functies, zoals het faciliteren van betalingen, en met indirecte gevolgen voor de daaraan gerelateerde economische processen. Totdat op Unieniveau een geharmoniseerde regeling en het toezicht op exploitanten van betalingssystemen en verwerkingsentiteiten zijn ingevoerd, kunnen de lidstaten, met het oog op de toepassing van soortgelijke marktpraktijken, inspiratie putten uit de in deze verordening vastgestelde vereisten inzake digitale operationele weerbaarheid wanneer zij regels toepassen op exploitanten van betalingssystemen en op verwerkingsentiteiten die onder toezicht staan in hun eigen rechtsgebied.

([23]) Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus (PB L 302 van 17.11.2009, blz. 1).

([24]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).

([25]) 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).

([26]) Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012 (PB L 257 van 28.8.2014, blz. 1).

([27]) Richtlijn (EU) 2022/2556 van het Europees Parlement en de Raad van 14 december 2022 tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector (zie bladzijde 153 van dit Publicatieblad).

([28]) Verordening (EU) 2016/1011 van het Europees Parlement en de Raad van 8 juni 2016 betreffende indices die worden gebruikt als benchmarks voor financiële instrumenten en financiële overeenkomsten of om de prestatie van beleggingsfondsen te meten en tot wijziging van Richtlijnen 2008/48/EG en 2014/17/EU en Verordening (EU) nr. 596/2014 (PB L 171 van 29.6.2016, blz. 1).

(105) Daar de doelstelling van deze verordening, te weten het bereiken van een hoog niveau van digitale operationele weerbaarheid voor gereguleerde financiële entiteiten, niet voldoende door de lidstaten kan worden verwezenlijkt, omdat zulks de harmonisatie vereist van een aantal verschillende voorschriften van Unie- en nationaal recht, maar vanwege de omvang en de gevolgen ervan beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstelling te verwezenlijken.

(106) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([29]) is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 10 mei 2021 heeft hij een advies uitgebracht ([30]),

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

Algemene bepalingen

Artikel 1

Onderwerp

1. Om een hoog gemeenschappelijk niveau van digitale operationele weerbaarheid te bereiken, worden in deze verordening uniforme vereisten vastgesteld met betrekking tot de beveiliging van netwerk- en informatiesystemen ter ondersteuning van bedrijfsprocessen van financiële entiteiten, te weten:

a) vereisten die van toepassing zijn op financiële entiteiten met betrekking tot:

   i) het risicobeheer op het gebied van informatie- en communicatietechnologie (ICT);

   ii) de melding van ernstige ICT-gerelateerde incidenten en, op vrijwillige basis, van significante cyberdreigingen aan de bevoegde autoriteiten;

   iii) de melding van ernstige betalingsgerelateerde operationele of beveiligingsincidenten aan de bevoegde autoriteiten door de financiële entiteiten als bedoeld in artikel 2, lid 1, punten a) tot en met d);

   iv) het testen van de digitale operationele weerbaarheid;

   v) de uitwisseling van informatie en inlichtingen met betrekking tot cyberdreigingen en -kwetsbaarheden;

   vi) maatregelen voor het goede beheer van het ICT-risico van derde aanbieders;

b) vereisten met betrekking tot de contractuele overeenkomsten tussen derde aanbieders van ICT-diensten en financiële entiteiten;

c) regels voor de vaststelling en het beheren van het oversightkader voor kritieke derde aanbieders van ICT-diensten bij het verlenen van diensten aan financiële entiteiten;

d) regels inzake samenwerking tussen bevoegde autoriteiten en regels inzake toezicht en handhaving door bevoegde autoriteiten met betrekking tot alle aangelegenheden die onder deze verordening vallen.

2. Met betrekking tot de financiële entiteiten die overeenkomstig de nationale voorschriften tot omzetting van artikel 3 van Richtlijn (EU) 2022/2555 als essentiële of belangrijke entiteiten zijn aangewezen, wordt deze verordening voor de toepassing van artikel 4 van die richtlijn beschouwd als een sectorspecifieke rechtshandeling van de Unie.

3. Deze verordening laat de verantwoordelijkheid van de lidstaten inzake essentiële staatsfuncties op het gebied van de openbare veiligheid, defensie en nationale veiligheid overeenkomstig het Unierecht onverlet.

([29]) 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).

([30]) PB C 229 van 15.6.2021, blz. 16.

Artikel 2

Toepassingsgebied

1. Onverminderd de leden 3 en 4 is deze verordening van toepassing op de volgende entiteiten:

a) kredietinstellingen;

b) betalingsinstellingen, met inbegrip van bij Richtlijn (EU) 2015/2366 vrijgestelde betalingsinstellingen;

c) aanbieders van rekeninginformatiediensten;

d) instellingen voor elektronisch geld, met inbegrip van krachtens Richtlijn 2009/110/EG vrijgestelde instellingen voor elektronisch geld;

e) beleggingsondernemingen;

f) aanbieders van cryptoactivadiensten met een vergunning op grond van een Verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937 ("de verordening betreffende markten in cryptoactiva") en emittenten van asset-referenced tokens;

g) centrale effectenbewaarinstellingen;

h) centrale tegenpartijen;

i) handelsplatformen;

j) transactieregisters;

k) beheerders van alternatieve beleggingsinstellingen;

l) beheermaatschappijen;

m) aanbieders van datarapporteringsdiensten;

n) verzekerings- en herverzekeringsondernemingen;

o) verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen;

p) instellingen voor bedrijfspensioenvoorziening;

q) ratingbureaus;

r) beheerders van kritieke benchmarks;

s) aanbieders van crowdfundingdiensten;

t) securitisatieregisters;

u) derde aanbieders van ICT-diensten.

2. Voor de toepassing van deze verordening worden de in lid 1, punten a) tot en met t), bedoelde entiteiten "financiële entiteiten" genoemd.

3. Deze verordening is niet van toepassing op:

a) beheerders van alternatieve beleggingsinstellingen, als bedoeld in artikel 3, lid 2, van Richtlijn 2011/61/EU;

b) verzekerings- en herverzekeringsondernemingen, als bedoeld in artikel 4 van Richtlijn 2009/138/EG;

c) instellingen voor bedrijfspensioenvoorzieningen die pensioenregelingen uitvoeren die samen niet meer dan 15 leden hebben;

d) bij de artikelen 2 en 3 van Richtlijn 2014/65/EU vrijgestelde natuurlijke of rechtspersonen;

e) verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen die micro-ondernemingen, dan wel kleine of middelgrote ondernemingen zijn;

f) postcheque- en girodiensten als bedoeld in artikel 2, lid 5, punt 3), van Richtlijn 2013/36/EU.

4. De lidstaten kunnen entiteiten als bedoeld in artikel 2, lid 5, punten 4) tot en met 23), van Richtlijn 2013/36/EU die op hun respectieve grondgebied gevestigd zijn, uitsluiten van het toepassingsgebied van deze verordening. Wanneer een lidstaat van deze mogelijkheid gebruikmaakt, stelt hij de Commissie daarvan in kennis, alsmede van alle latere wijzigingen in dat verband. De Commissie maakt die informatie openbaar op haar website of via andere gemakkelijk toegankelijke middelen.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) "digitale operationele weerbaarheid": het vermogen van een financiële entiteit om haar operationele integriteit en betrouwbaarheid op te bouwen, te waarborgen en te evalueren, door direct of indirect via gebruik van diensten die door derde aanbieders van ICT-diensten worden verleend te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die nodig zijn voor de beveiliging van de netwerk- en informatiesystemen waarvan een financiële entiteit gebruikmaakt, en die de permanente verlening van financiële diensten en de kwaliteit ervan, onder meer gedurende storingen, ondersteunen;

2) "netwerk- en informatiesysteem": een netwerk- en informatiesysteem in de zin van artikel 6, punt 1, van Richtlijn (EU) 2022/2555 ;

3) "legacy-ICT-systeem": een ICT-systeem dat het einde van zijn levenscyclus (einde van de levensduur) heeft bereikt, dat om technologische of commerciële redenen niet geschikt is voor upgrades of reparaties, of dat niet langer wordt ondersteund door de leverancier of een derde aanbieder van ICT-diensten, maar dat nog steeds in gebruik is en de functies van de financiële entiteit ondersteunt;

4) "beveiliging van netwerk- en informatiesystemen": beveiliging van netwerk- en informatiesystemen in de zin van artikel 6, punt 2, van Richtlijn (EU) 2022/2555 ;

5) "ICT-risico": elke redelijkerwijs aan te wijzen omstandigheid met betrekking tot het gebruik van netwerk- en informatiesystemen die, indien zij zich voordoet, de beveiliging van het netwerk- en informatiesysteem, van technologieafhankelijke instrumenten of processen, van verrichtingen en processen, of van de levering van de diensten in gevaar kan brengen, door schadelijke effecten met zich mee te brengen in de digitale of fysieke omgeving;

6) "informatieactief": een reeks, al dan niet tastbare, gegevens die beschermenswaardig zijn;

7) "ICT-actief": een software- of hardwareactief in de netwerk- en informatiesystemen die door de financiële entiteit worden gebruikt;

8) "ICT-gerelateerd incident": één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de financiële entiteit zijn gepland en die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of op de door de financiële entiteit verleende diensten;

9) "betalingsgerelateerd operationeel of beveiligingsincident": één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de in artikel 2, lid 1, punten a) tot en met d), bedoelde financiële entiteiten gepland zijn, die al dan niet ICT-gerelateerd zijn, en die een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van betalingsgerelateerde gegevens, of op de door de financiële entiteit verleende betalingsgerelateerde diensten;

10) "ernstig ICT-gerelateerd incident": een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen;

11) "ernstig betalingsgerelateerd operationeel of beveiligingsincident": een betalingsgerelateerd operationeel of beveiligingsincident dat een groot negatief effect heeft op de verleende betalingsgerelateerde diensten;

12) "cyberdreiging": cyberdreiging in de zin van artikel 2, punt 8), van Verordening (EU) 2019/881;

13) "significante cyberdreiging": een cyberdreiging waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ernstig ICT-gerelateerd incident of een ernstig betalingsgerelateerd operationeel of beveiligingsincident;

14) "cyberaanval": een kwaadwillig ICT-gerelateerd incident dat het gevolg is van een door een dreigingsactor gepleegde poging om een actief te vernietigen, bloot te stellen, te veranderen, buiten werking te stellen, te stelen of er ongeoorloofde toegang toe te verkrijgen of er ongeoorloofd gebruik van te maken;

15) "inlichtingen over dreigingen": informatie die is geaggregeerd, getransformeerd, geanalyseerd, geïnterpreteerd of verrijkt om de noodzakelijke achtergrond voor besluitvorming te bieden en om relevant en toereikend inzicht te verschaffen om de gevolgen van een ICT-gerelateerd incident of van een cyberdreiging te beperken, met inbegrip van de technische details van een cyberaanval, de voor de aanval verantwoordelijke personen en hun werkwijze en motieven;

16) "kwetsbaarheid": een zwakte, gevoeligheid of tekortkoming in een actief, systeem, proces of controle die kan worden misbruikt;

17) "dreigingsgestuurde penetratietest" (*threat led penetration testing* — TLPT): een kader waarin de tactiek, technieken en procedures van levensechte, als een reële cyberdreiging ervaren dreigingsactoren worden nagebootst en waarin een gecontroleerde, op maat gesneden, door inlichtingen gestuurde (red team) test van de kritieke reëel bestaande productiesystemen van de financiële entiteit wordt voorgebracht;

18) "ICT-risico van derde aanbieders": een ICT-risico dat voor een financiële entiteit kan ontstaan met betrekking tot het gebruik van ICT-diensten die door derde aanbieders van ICT-diensten of door onderaannemers daarvan, onder meer via onderaanbestedingsovereenkomsten, worden verleend;

19) "derde aanbieder van ICT-diensten": een onderneming die ICT-diensten verleent;

20) "aanbieder van ICT-diensten binnen een groep": een onderneming die deel uitmaakt van een financiële groep en hoofdzakelijk ICT-diensten verleent aan financiële entiteiten binnen dezelfde groep of aan financiële entiteiten die tot hetzelfde institutionele protectiestelsel behoren, met inbegrip van hun moedermaatschappijen, dochterondernemingen, bijkantoren of andere entiteiten die gezamenlijk eigendom zijn of onder gezamenlijke zeggenschap staan;

21) "ICT-diensten": digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten;

22) "kritieke of belangrijke functie": een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten;

23) "kritieke derde aanbieder van ICT-diensten": een derde aanbieder van ICT-diensten die overeenkomstig artikel 31 is aangewezen als cruciaal;

24) "in een derde land gevestigde derde aanbieder van ICT-diensten": een derde aanbieder van ICT-diensten die een in een derde land gevestigde rechtspersoon is en die een contractuele overeenkomst met een financiële entiteit heeft gesloten voor de levering van ICT-diensten;

25) "dochteronderneming": een dochteronderneming in de zin van artikel 2, punt 10), en artikel 22 van Richtlijn 2013/34/EU;

26) "groep": een groep in de zin van artikel 2, punt 11), van Richtlijn 2013/34/EU;

27) "moederonderneming": een moederonderneming in de zin van artikel 2, punt 9), en artikel 22 van Richtlijn 2013/34/EU;

28) "in een derde land gevestigde ICT-subcontractant": een ICT-subcontractant die een in een derde land gevestigde rechtspersoon is en die een contractuele overeenkomst heeft gesloten met een derde aanbieder van ICT-diensten of met een in een derde land gevestigde derde aanbieder van ICT-diensten;

29) "ICT-concentratierisico": een blootstelling aan individuele of aan meerdere onderling verbonden kritieke derde aanbieders van ICT-diensten, waardoor een bepaalde mate van afhankelijkheid ten aanzien van deze aanbieders ontstaat, zodat de onbeschikbaarheid, het falen of een ander soort tekortkoming van deze aanbieder het vermogen van een financiële entiteit om kritieke of belangrijke functies te vervullen in gevaar kan brengen, ertoe kan leiden dat zij andere soorten nadelige effecten, waaronder grote verliezen, ondervindt, of de financiële stabiliteit van de Unie in haar geheel in gevaar kan brengen;

30) "leidinggevend orgaan": een leidinggevend orgaan in de zin van artikel 4, lid 1, punt 36), van Richtlijn 2014/65/EU, artikel 3, lid 1, punt 7), van Richtlijn 2013/36/EU, artikel 2, lid 1, punt s), van Richtlijn 2009/65/EG van het Europees Parlement en de Raad ([31]), artikel 2, lid 1, punt 45), van Verordening (EU) nr. 909/2014, artikel 3, lid 1, punt 20), van Verordening (EU) 2016/1011, en in de relevante bepaling van de verordening betreffende markten in cryptoactiva, of de gelijkwaardige personen die de entiteit daadwerkelijk besturen of sleutelfuncties vervullen overeenkomstig het toepasselijke Unie- of nationale recht;

31) "kredietinstelling": een kredietinstelling in de zin van artikel 4, lid 1, punt 1, van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ([32]);

32) "bij Richtlijn 2013/36/EU vrijgestelde instelling": een entiteit zoals vermeld in artikel 2, lid 5, punten 4) tot en met 23), van Richtlijn 2013/36/EU;

33) "beleggingsonderneming": een beleggingsonderneming in de zin van artikel 4, lid 1, punt 1, van Richtlijn 2014/65/EU;

34) "kleine en niet-verweven beleggingsonderneming": een beleggingsonderneming die voldoet aan de voorwaarden in artikel 12, lid 1, van Verordening (EU) 2019/2033 van het Europees Parlement en de Raad ([33]);

35) "betalingsinstelling": een betalingsinstelling in de zin van artikel 4, punt 4), van Richtlijn (EU) 2015/2366;

36) "bij Richtlijn (EU) 2015/2366 vrijgestelde betalingsinstelling": een betalingsinstelling die is vrijgesteld op grond van artikel 32, lid 1, van Richtlijn (EU) 2015/2366;

37) "aanbieder van rekeninginformatiediensten": een aanbieder van rekeninginformatiediensten als bedoeld in artikel 33, lid 1, van Richtlijn (EU) 2015/2366;

38) "instelling voor elektronisch geld": een instelling voor elektronisch geld in de zin van artikel 2, punt 1), van Richtlijn 2009/110/EG van het Europees Parlement en de Raad;

39) "bij Richtlijn 2009/110/EG vrijgestelde instelling voor elektronisch geld": een instelling voor elektronisch geld waaraan een ontheffing is verleend als bedoeld in artikel 9, lid 1, van Richtlijn 2009/110/EG;

40) "centrale tegenpartij": een centrale tegenpartij in de zin van artikel 2, punt 1), van Verordening (EU) nr. 648/2012;

41) "transactieregister": een transactieregister in de zin van artikel 2, punt 2), van Verordening (EU) nr. 648/2012;

42) "centrale effectenbewaarinstelling": een centrale effectenbewaarinstelling in de zin van artikel 2, lid 1, punt 1), van Verordening (EU) nr. 909/2014;

43) "handelsplatform" een handelsplatform in de zin van artikel 4, lid 1, punt 24, van Richtlijn 2014/65/EU;

44) "beheerder van alternatieve beleggingsinstellingen": een beheerder van alternatieve beleggingsinstellingen in de zin van artikel 4, lid 1, punt b), van Richtlijn 2011/61/EU;

45) "beheermaatschappij": een beheermaatschappij in de zin van artikel 2, lid 1, punt b), van Richtlijn 2009/65/EG;

46) "aanbieder van datarapporteringsdiensten": een aanbieder van datarapporteringsdiensten in de zin van Verordening (EU) nr. 600/2014, als bedoeld in artikel 2, lid 1, punten 34 tot en met 36, van die verordening;

47) "verzekeringsonderneming": een verzekeringsonderneming in de zin van artikel 13, punt 1, van Richtlijn 2009/138/EG;

48) "herverzekeringsonderneming": een herverzekeringsonderneming in de zin van artikel 13, punt 4, van Richtlijn 2009/138/EG;

([31]) Richtlijn 2009/65/EG van het Europees Parlement en de Raad van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe's) (PB L 302 van 17.11.2009, blz. 32).

([32]) Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).

([33]) Verordening (EU) 2019/2033 van het Europees Parlement en de Raad van 27 november 2019 betreffende prudentiële vereisten voor beleggingsondernemingen en tot wijziging van Verordeningen (EU) nr. 1093/2010, (EU) nr. 575/2013, (EU) nr. 600/2014 en (EU) nr. 806/2014 (PB L 314 van 5.12.2019, blz. 1).

49) "verzekeringstussenpersoon": een verzekeringstussenpersoon in de zin van artikel 2, lid 1, punt 3, van Richtlijn (EU) 2016/97 van het Europees Parlement en de Raad ([34]);

50) "nevenverzekeringstussenpersoon": een nevenverzekeringstussenpersoon in de zin van artikel 2, lid 1, punt 4, van Richtlijn (EU) 2016/97;

51) "herverzekeringstussenpersoon": een herverzekeringstussenpersoon in de zin van artikel 2, lid 1, punt 5, van Richtlijn (EU) 2016/97;

52) "instelling voor bedrijfspensioenvoorziening": een instelling voor bedrijfspensioenvoorziening in de zin van artikel 6, punt 1), van Richtlijn (EU) 2016/2341;

53) "kleine instelling voor bedrijfspensioenvoorziening": een instelling voor bedrijfspensioenvoorziening die pensioenregelingen uitvoert die samen minder dan 100 leden hebben;

54) "ratingbureau": een ratingbureau in de zin van artikel 3, lid 1, punt b), van Verordening (EG) nr. 1060/2009;

55) "aanbieder van cryptoactivadiensten": een aanbieder van cryptoactivadiensten in de zin van de relevante bepaling van de verordening betreffende markten in cryptoactiva;

56) "emittent van asset-referenced tokens": een emittent van asset-referenced tokens in de zin van de relevante bepaling van de verordening betreffende markten in cryptoactiva;

57) "beheerder van kritieke benchmarks": een beheerder van kritieke benchmarks in de zin van artikel 3, lid 1, punt 25), van Verordening (EU) 2016/1011;

58) "crowdfundingdienstverlener": een crowdfundingdienstverlener in de zin van artikel 2, lid 1, punt e), van Verordening (EU) 2020/1503 van het Europees Parlement en de Raad ([35]);

59) "securitisatieregister": een securitisatieregister in de zin van artikel 2, punt 23), van Verordening (EU) 2017/2402 van het Europees Parlement en de Raad ([36]);

60) "micro-onderneming": een financiële entiteit die geen handelsplatform, centrale tegenpartij, transactieregister of centrale effectenbewaarinstelling is, en waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet en/of het jaarlijkse balanstotaal niet hoger liggen dan 2 miljoen EUR;

61) "lead overseer": de overeenkomstig artikel 31, lid 1, punt b), van deze verordening aangewezen Europese toezichthoudende autoriteit;

62) "Gemengd Comité": het in artikel 54 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 bedoelde comité;

63) "kleine onderneming": een financiële entiteit met 10 of meer werknemers, maar minder dan 50 werknemers, en een jaaromzet en/of een jaarlijks balanstotaal van meer dan 2 miljoen EUR, maar van ten hoogste 10 miljoen EUR;

64) "middelgrote onderneming": een financiële entiteit die geen kleine onderneming is, minder dan 250 personen in dienst heeft en een jaaromzet van ten hoogste 50 miljoen EUR en/of een jaarlijkse balans van ten hoogste 43 miljoen EUR heeft;

65) "overheidsinstantie": een regerings- of andere overheidsinstantie, met inbegrip van nationale centrale banken.

([34]) Richtlijn (EU) 2016/97 van het Europees Parlement en de Raad van 20 januari 2016 betreffende verzekeringsdistributie (PB L 26 van 2.2.2016, blz. 19).

([35]) Verordening (EU) 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937 (PB L 347 van 20.10.2020, blz. 1).

([36]) Verordening (EU) 2017/2402 van het Europees Parlement en de Raad van 12 december 2017 tot vaststelling van een algemeen kader voor securitisatie en tot instelling van een specifiek kader voor eenvoudige, transparante en gestandaardiseerde securitisatie, en tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG en 2011/61/EU en de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 648/2012 (PB L 347 van 28.12.2017, blz. 35).

Artikel 4

Evenredigheidsbeginsel

1. Financiële entiteiten passen de bij hoofdstuk II ingevoerde regels toe overeenkomstig het evenredigheidsbeginsel, rekening houdend met hun omvang, algehele risicoprofiel en de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen.

2. Daarnaast staat de toepassing door financiële entiteiten van de hoofdstukken III en IV en hoofdstuk V, afdeling I, in verhouding tot hun omvang en algehele risicoprofiel en tot de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen, zoals specifiek bepaald in de desbetreffende regels van die hoofdstukken.

3. De bevoegde autoriteiten houden rekening met de toepassing van het evenredigheidsbeginsel door financiële entiteiten wanneer zij de consistentie van het kader voor ICT-risicobeheer toetsen op basis van de verslagen die op verzoek van de bevoegde autoriteiten krachtens artikel 6, lid 5, en artikel 16, lid 2, zijn ingediend.

HOOFDSTUK II

ICT-risicobeheer

Afdeling I

Artikel 5

Governance en organisatie

1. Financiële entiteiten beschikken over een intern governance- en controlekader dat een doeltreffend en prudent beheer van het ICT-risico waarborgt, overeenkomstig artikel 6, lid 4, teneinde een hoog niveau van digitale operationele weerbaarheid te verkrijgen.

2. Het leidinggevend orgaan van een financiële entiteit bepaalt alle regelingen met betrekking tot het in artikel 6, lid 1, bedoelde kader voor ICT-risicobeheer, keurt deze goed, houdt toezicht op de uitvoering ervan en is ervoor verantwoordelijk.

Voor de toepassing van de eerste alinea is het leidinggevend orgaan belast met:

a) de eindverantwoordelijkheid voor het beheer van het ICT-risico van de financiële entiteit;

b) de invoering van beleidslijnen die erop gericht zijn de handhaving van hoge normen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens te waarborgen;

c) de vaststelling van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies en van passende governanceregelingen om te zorgen voor doeltreffende en tijdige communicatie, samenwerking en coördinatie tussen die functies;

d) de algemene verantwoordelijkheid voor het vaststellen en goedkeuren van de strategie voor digitale operationele weerbaarheid als bedoeld in artikel 6, lid 8, met inbegrip van de bepaling van het passende risicotolerantieniveau voor het ICT-risico van de financiële entiteit, als bedoeld in artikel 6, lid 8, punt b);

e) de goedkeuring van, het toezicht op en de periodieke evaluatie van de uitvoering van het beleid inzake ICT-bedrijfscontinuïteit en van de ICT-respons- en herstelplannen van de financiële entiteit, als bedoeld in respectievelijk artikel 11, leden 1 en 3, die kunnen worden aangenomen als een specifiek afzonderlijk beleid en als integrerend onderdeel van het ruimere beleid inzake bedrijfscontinuïteit en het respons- en herstelplan van de financiële entiteit;

f) de goedkeuring en de periodieke evaluatie van de interne ICT-auditplannen en ICT-audits van de financiële entiteit en materiële wijzigingen daarvan;

g) de toewijzing en de periodieke evaluatie van het passende budget om te voldoen aan de behoeften inzake digitale operationele weerbaarheid van de financiële entiteit met betrekking tot alle soorten middelen, waaronder relevante bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid zoals bedoeld in artikel 13, lid 6, en ICT-vaardigheden voor al het personeel;

h) de goedkeuring en de periodieke evaluatie van het beleid van de financiële entiteit inzake regelingen betreffende het gebruik van ICT-diensten die door derde aanbieders van ICT-diensten worden verleend;

i) het opzetten van meldingskanalen op bedrijfsniveau die het in staat stellen informatie in te winnen over:

   i) overeenkomsten met derde aanbieders van ICT-diensten inzake het gebruik van ICT-diensten;

   ii) elke relevante geplande materiële wijziging betreffende de derde aanbieders van ICT-diensten;

   iii) de potentiële effecten van deze veranderingen voor de kritieke of belangrijke functies die onder die overeenkomsten vallen, inclusief door middel van een samenvatting van de risicoanalyse om het effect te beoordelen van die veranderingen en op zijn minst ernstige ICT-gerelateerde incidenten en de gevolgen daarvan, alsook respons-, herstel- en corrigerende maatregelen.

3. Andere financiële entiteiten dan micro-ondernemingen stellen een taak vast om de overeenkomsten met derde aanbieders van ICT-diensten met betrekking tot het gebruik van deze diensten te monitoren, of wijzen een lid van het hoger leidinggevend personeel aan dat verantwoordelijk is voor het toezicht op de desbetreffende risicoblootstelling en de relevante documentatie.

4. De leden van het leidinggevend orgaan van de financiële entiteit onderhouden actief voldoende kennis en vaardigheden om ICT-risico en de gevolgen daarvan voor de verrichtingen van de financiële entiteit te begrijpen en te beoordelen, onder meer door regelmatig specifieke opleidingen te volgen die in verhouding staan tot het te beheren ICT-risico.

Afdeling II

Artikel 6

Kader voor ICT-risicobeheer

1. Financiële entiteiten beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer, als onderdeel van hun algemeen risicobeheersysteem, dat hen in staat stelt ICT-risico snel, efficiënt en zo volledig mogelijk aan te pakken en een hoog niveau van digitale operationele weerbaarheid te waarborgen.

2. Het kader voor ICT-risicobeheer omvat ten minste strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle informatie- en ICT-activa, met inbegrip van computersoftware, hardware, servers naar behoren en toereikend te beschermen, en om alle relevante fysieke elementen en infrastructuur**,** zoals gebouwen en terreinen, datacentra en als gevoelig aangewezen gebieden te beschermen, teneinde te waarborgen dat alle informatie- en ICT-activa toereikend worden beschermd tegen risico's, waaronder schade, ongeoorloofde toegang en ongeoorloofd gebruik.

3. Overeenkomstig hun kader voor ICT-risicobeheer beperken financiële entiteiten de impact van ICT-risico tot een minimum door passende strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten in te zetten. Op verzoek van de bevoegde autoriteiten verstrekken zij aan die autoriteiten volledige en geactualiseerde informatie over ICT-risico en over hun kader voor ICT-risicobeheer.

4. Andere financiële entiteiten dan micro-ondernemingen wijzen de verantwoordelijkheid voor het beheer van en toezicht op ICT-risico toe aan een controlefunctie en waarborgen een passend niveau van onafhankelijkheid van die controlefunctie om belangenconflicten te voorkomen. Financiële entiteiten waarborgen een passende scheiding en onafhankelijkheid van ICT-risicobeheerfuncties, controlefuncties en interne auditfuncties, overeenkomstig het model van de drie verdedigingslijnen of een model voor intern risicobeheer en -controle.

5. Het kader voor ICT-risicobeheer wordt ten minste eenmaal per jaar, of periodiek in het geval van micro-ondernemingen, gedocumenteerd en geëvalueerd, alsook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en na toezichtinstructies of -conclusies die voortvloeien uit relevante tests of auditprocessen op het gebied van digitale operationele weerbaarheid. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen. Aan de bevoegde autoriteit wordt een verslag bezorgd over de evaluatie van het kader voor ICT-risicobeheer indien zij daarom verzoekt.

6. Het kader voor ICT-risicobeheer van andere financiële entiteiten dan micro-ondernemingen wordt regelmatig onderworpen aan een interne audit door auditors, in overeenstemming met het auditplan van de financiële entiteiten. Deze auditors beschikken over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico en over de nodige onafhankelijkheid. De frequentie en de focus van de ICT-audits staan in verhouding tot het ICT-risico van de financiële entiteit.

7. Op basis van de conclusies van de interne audit stellen financiële entiteiten een formeel follow-upproces vast, met regels voor de tijdige verificatie en remediëring van kritieke ICT-auditbevindingen.

8. Het kader voor ICT-risicobeheer omvat een strategie voor digitale operationele weerbaarheid waarin de wijze van tenuitvoerlegging van het kader wordt vastgesteld. Daartoe omvat de strategie voor digitale operationele weerbaarheid methoden om ICT-risico aan te pakken en specifieke ICT-doelstellingen te verwezenlijken, door:

a) toe te lichten hoe het kader voor ICT-risicobeheer de bedrijfsstrategie en -doelstellingen van de financiële entiteit ondersteunt;

b) het risicotolerantieniveau voor ICT-risico vast te stellen in overeenstemming met de risicobereidheid van de financiële entiteit, en de tolerantie ten aanzien van de effecten van ICT-storingen te analyseren;

c) duidelijke informatiebeveiligingsdoelstellingen vast te stellen, met inbegrip van kernprestatie-indicatoren en kernrisico-maatstaven;

d) de ICT-referentiearchitectuur toe te lichten alsmede eventuele wijzigingen daarin die noodzakelijk zijn om specifieke bedrijfsdoelstellingen te bereiken;

e) de verschillende mechanismen te beschrijven die zijn ingesteld om ICT-gerelateerde incidenten op te sporen, de effecten ervan te voorkomen en te voorzien in beveiliging tegen deze effecten;

f) de huidige situatie op het gebied van digitale operationele weerbaarheid aan te tonen op basis van het aantal gemelde ernstige ICT-gerelateerde incidenten en de doeltreffendheid van preventieve maatregelen;

g) tests te verrichten van de digitale operationele weerbaarheid, overeenkomstig hoofdstuk IV van deze verordening;

h) en een communicatiestrategie uit te stippelen in het geval van ICT-gerelateerde incidenten die overeenkomstig artikel 14 openbaar moeten worden gemaakt.

9. Financiële entiteiten kunnen, in het kader van de in lid 8 bedoelde strategie voor digitale operationele weerbaarheid, op groeps- of entiteitsniveau een holistische multivendorstrategie op ICT-gebied vaststellen, waarin belangrijke afhankelijkheden van derde aanbieders van ICT-diensten worden aangegeven en de motivering voor de mix van aanbestedingen bij derde aanbieders van ICT-diensten wordt toegelicht.

10. Financiële entiteiten kunnen, in overeenstemming met het Unie- en nationale sectorale recht, de verificatietaken inzake naleving van de vereisten op het gebied van ICT-risicobeheer uitbesteden aan intragroeps- of externe ondernemingen. In het geval van een dergelijke uitbesteding blijft de financiële entiteit volledig verantwoordelijk voor de controle op de naleving van de vereisten inzake ICT-risicobeheer.

Artikel 7

ICT-systemen, -protocollen en -instrumenten

Om ICT-risico aan te pakken en te beheren, gebruiken en onderhouden financiële entiteiten geactualiseerde ICT-systemen, -protocollen en -instrumenten die:

a) geschikt zijn gezien de omvang van de verrichtingen ter ondersteuning van hun activiteiten, in overeenstemming met het evenredigheidsbeginsel als bedoeld in artikel 4;

b) betrouwbaar zijn;

c) voldoende capaciteit hebben voor een nauwkeurige verwerking van de gegevens die nodig zijn voor de uitvoering van activiteiten en de tijdige verlening van diensten, en om zo nodig volumepieken in orders, orderberichten of transacties op te vangen, onder meer wanneer nieuwe technologie wordt ingevoerd;

d) technologisch gezien voldoende weerbaar zijn om indien nodig in gespannen marktomstandigheden of andere ongunstige situaties naar behoren te voorzien in bijkomende gegevensverwerking.

Artikel 8

Identificatie

1. In het kader van het in artikel 6, lid 1, bedoelde kader voor ICT-risicobeheer identificeren, classificeren en documenteren financiële entiteiten naar behoren alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden, de informatie- en ICT-activa die deze functies ondersteunen, en hun taken en afhankelijkheden met betrekking tot ICT-risico's. Financiële entiteiten evalueren indien nodig en ten minste eenmaal per jaar of deze classificatie en de relevante documentatie adequaat is.

2. Financiële entiteiten identificeren permanent alle bronnen van ICT-risico, met name de wederzijdse risicoblootstelling ten aanzien van andere financiële entiteiten, en beoordelen de cyberdreigingen en ICT-kwetsbaarheden die relevant zijn voor hun door ICT ondersteunde bedrijfsfuncties en informatie- en ICT-activa. Financiële entiteiten evalueren regelmatig en ten minste eenmaal per jaar de risicoscenario's die op hen van invloed zijn.

3. Andere financiële entiteiten dan micro-ondernemingen verrichten een risicobeoordeling bij elke belangrijke wijziging in de netwerk- en informatiesysteeminfrastructuur en in de processen of procedures die van invloed zijn op hun door ICT ondersteunde bedrijfsfuncties en informatie- of ICT-activa.

4. Financiële entiteiten identificeren alle informatie- en ICT-activa, met inbegrip van die welke zich op afgelegen locaties bevinden, netwerkmiddelen en hardware-uitrusting, en inventariseren die welke zij cruciaal achten. Zij inventariseren de configuratie van de informatie- en ICT-activa en de verbanden en onderlinge afhankelijkheden tussen de verschillende informatie- en ICT-activa.

5. Financiële entiteiten identificeren en documenteren alle processen die afhankelijk zijn van derde aanbieders van ICT-diensten en identificeren interconnecties met derde aanbieders van ICT-diensten die diensten verlenen die kritieke of belangrijke functies ondersteunen.

6. Voor de toepassing van de leden 1, 4 en 5 houden financiële entiteiten desbetreffende inventarissen bij en actualiseren zij deze periodiek en telkens wanneer zich een belangrijke wijziging als bedoeld in lid 3 voordoet.

7. Andere financiële entiteiten dan micro-ondernemingen verrichten regelmatig en ten minste eenmaal per jaar een specifieke ICT-risicobeoordeling op alle legacy-ICT-systemen en in ieder geval voor en na de aansluiting van technologieën, toepassingen of systemen.

Artikel 9

Bescherming en voorkoming

1. Om ICT-systemen op passende wijze te beschermen en met het oog op de organisatie van responsmaatregelen monitoren en controleren financiële entiteiten voortdurend de beveiliging en werking van de ICT-systemen en -instrumenten en beperken zij de effecten van ICT-risico op ICT-systemen door de inzet van passende ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures.

2. Financiële entiteiten zorgen voor het ontwerp, de aanbesteding en de uitvoering van ICT-beveiligingsbeleidslijnen, -procedures, -protocollen en -instrumenten die er op gericht zijn de weerbaarheid, continuïteit en beschikbaarheid van ICT-systemen, met name die welke kritieke of belangrijke functies ondersteunen, te waarborgen alsmede hoge normen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, zowel in rusttoestand, bij gebruik als bij doorvoer, te handhaven.

3. Om de in lid 2 bedoelde doelstellingen te verwezenlijken, maken financiële entiteiten gebruik van ICT-technologieën en -processen die geschikt zijn overeenkomstig artikel 4. Die ICT-oplossingen en -processen:

a) waarborgen de beveiliging van de middelen voor overdracht van gegevens;

b) beperken het risico op aantasting of verlies van gegevens, ongeoorloofde toegang en technische gebreken die de bedrijfsactiviteit kunnen belemmeren;

c) voorkomen een gebrek aan beschikbaarheid, de aantasting van de authenticiteit en integriteit, de inbreuken op de vertrouwelijkheid en het verlies van gegevens;

d) zorgen ervoor dat gegevens worden beschermd tegen risico's bij het gegevensbeheer, met inbegrip van slecht bestuur, risico's bij de verwerking en menselijke fouten.

4. In het kader van het in artikel 6, lid 1, bedoelde kader voor ICT-risicobeheer zorgen financiële entiteiten voor het volgende:

a) zij ontwikkelen en documenteren een beleid inzake informatiebeveiliging waarin regels worden vastgesteld ter bescherming van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, informatie- en ICT-activa, inclusief die van hun klanten, in voorkomend geval;

b) zij voeren op grond van een op risico's gebaseerde aanpak een degelijke structuur voor netwerk- en infrastructuurbeheer in met gebruik van passende technieken, methoden en protocollen, eventueel met toepassing van geautomatiseerde mechanismen om in geval van cyberaanvallen de getroffen informatieactiva te isoleren;

c) zij voeren een beleid waarbij de fysieke of logische toegang tot informatie- en ICT-activa wordt beperkt tot hetgeen alleen voor legitieme en goedgekeurde functies en activiteiten noodzakelijk is, en voeren daartoe een reeks beleidslijnen, procedures en controles in om toegangsrechten en een degelijk beheer daarvan te waarborgen;

d) zij voeren beleidslijnen en protocollen in voor strenge authenticatiemechanismen die gebaseerd zijn op relevante normen, specifieke controlesystemen en beschermingsmaatregelen voor cryptografische sleutels, waarbij gegevens worden versleuteld uitgaande van de resultaten van goedgekeurde processen van gegevensclassificatie en ICT-risicobeoordeling;

e) zij voeren gedocumenteerde beleidslijnen, procedures en controles in voor het beheer van veranderingen in ICT, met inbegrip van veranderingen in software, hardware, firmwarecomponenten, systemen of beveiligingsparameters, die uitgaan van een op risicobeoordeling gebaseerde aanpak en integrerend deel uitmaken van het algemene veranderingsbeheerproces van de financiële entiteit, teneinde te garanderen dat alle veranderingen in ICT-systemen op gecontroleerde wijze worden geregistreerd, getest, beoordeeld, goedgekeurd, ingevoerd en geverifieerd;

f) zij beschikken over een passend en alomvattend gedocumenteerd beleid voor patches en updates.

Voor de toepassing van de eerste alinea, punt b) ontwerpen financiële entiteiten de netwerkaansluitinfrastructuur op zodanige wijze dat deze onmiddellijk kan worden afgekoppeld of gesegmenteerd teneinde besmetting te beperken en te voorkomen, met name voor onderling gekoppelde financiële processen.

Voor de toepassing van de eerste alinea, punt e) wordt het beheerproces inzake ICT-veranderingen goedgekeurd door passende beheerlijnen en voorzien van specifieke protocollen.

Artikel 10

Detectie

1. Financiële entiteiten beschikken over mechanismen om overeenkomstig artikel 17 afwijkende activiteiten zo spoedig mogelijk te detecteren, met inbegrip van kwesties op het gebied van ICT-netwerkprestaties en ICT-gerelateerde incidenten, en om potentiële zwakke fysieke punten ("single points of failure") te identificeren.

Alle in de eerste alinea bedoelde detectiemechanismen worden regelmatig getest overeenkomstig artikel 25.

2. De in lid 1 bedoelde detectiemechanismen maken meerdere controlelagen mogelijk en bepalen waarschuwingsdrempels en criteria om processen voor respons op ICT-gerelateerde incidenten in werking te stellen, met inbegrip van automatische waarschuwingsmechanismen voor de betrokken personeelsleden die belast zijn met de respons op ICT-gerelateerde incidenten.

3. Financiële entiteiten zetten voldoende middelen en capaciteiten in om toezicht te houden op activiteiten van gebruikers en het optreden van ICT-anomalieën en ICT-gerelateerde incidenten, met name cyberaanvallen.

4. Aanbieders van datarapporteringsdiensten beschikken daarnaast over systemen die transactiemeldingen doeltreffend op volledigheid kunnen controleren, omissies en aperte fouten kunnen opsporen en om hernieuwde transmissie van die meldingen kunnen verzoeken.

Artikel 11

Respons en herstel

1. Binnen het in artikel 6, lid 1, bedoelde kader voor ICT-risicobeheer en op basis van de in artikel 8 gestelde identificatievereisten voeren financiële entiteiten een alomvattend ICT-bedrijfscontinuïteitsbeleid dat kan worden aangenomen als een specifiek beleid en een integrerend onderdeel vormt van het ruimere bedrijfsbrede beleid inzake bedrijfscontinuïteit van de financiële entiteit.

2. Financiële entiteiten voeren het ICT-bedrijfscontinuïteitsbeleid uit via specifieke, aangepaste en gedocumenteerde regelingen, plannen, procedures en mechanismen die erop gericht zijn:

a) de continuïteit van de kritieke of belangrijke functies van de financiële entiteit te verzekeren;

b) op een snelle, passende en doeltreffende wijze een respons en een oplossing te bieden voor alle ICT-gerelateerde incidenten waarbij de schade wordt beperkt en prioriteit wordt verleend aan de hervatting van de activiteiten en aan herstelmaatregelen;

c) onverwijld specifieke plannen in werking te stellen om inperkingsmaatregelen, -processen en -technologieën mogelijk te maken die aangepast zijn aan elk type ICT-gerelateerd incident en waarmee verdere schade kan worden voorkomen, alsmede op maat gesneden respons- en herstelprocedures in overeenstemming met artikel 12;

d) de voorlopige effecten, schade en verliezen te ramen;

e) maatregelen voor communicatie en crisisbeheersing op te stellen die garanderen dat aan alle betrokken interne personeelsleden en externe belanghebbenden geactualiseerde informatie wordt verstrekt overeenkomstig artikel 14, en verslag uit te brengen aan de bevoegde autoriteiten overeenkomstig artikel 19.

3. Binnen het in artikel 6, lid 1, bedoelde kader voor ICT-risicobeheer voeren financiële entiteiten bijbehorende ICT-respons- en herstelplannen in die, in het geval van andere financiële entiteiten dan micro-ondernemingen, aan onafhankelijke interne audits worden onderworpen.

4. Financiële entiteiten voeren passende ICT-bedrijfscontinuïteitsplannen in, handhaven deze en zorgen voor periodieke tests, met name wat betreft kritieke of belangrijke functies die zijn uitbesteed of via contractuele overeenkomsten met derde aanbieders van ICT-diensten zijn overeengekomen.

5. In het kader van het algemene bedrijfscontinuïteitsbeleid voeren financiële entiteiten een bedrijfsimpactanalyse (*business impact analysis* — BIA) uit van hun blootstelling aan ernstige verstoringen van de bedrijfsactiviteiten. In het kader van de BIA beoordelen financiële entiteiten de potentiële gevolgen van ernstige verstoringen van de bedrijfsactiviteiten aan de hand van kwantitatieve en kwalitatieve criteria, in voorkomend geval met behulp van interne en externe gegevens en scenarioanalyse. In de BIA wordt rekening gehouden met de kritieke aard van geïdentificeerde en in kaart gebrachte bedrijfsfuncties, ondersteuningsprocessen, afhankelijkheden van derden en informatieactiva, en hun onderlinge afhankelijkheden. Financiële entiteiten zorgen ervoor dat ICT-activa en ICT-diensten worden ontworpen en gebruikt in volledige overeenstemming met de BIA, met name om de redundantie van alle kritieke onderdelen adequaat te waarborgen.

6. In het kader van hun alomvattend ICT-risicobeheer testen financiële entiteiten:

a) ten minste jaarlijks en in geval van substantiële wijzigingen in ICT-systemen die kritieke of belangrijke functies ondersteunen, de ICT-bedrijfscontinuïteitsplannen en de ICT-respons- en herstelplannen met betrekking tot ICT-systemen die kritieke of belangrijke functies ondersteunen;

b) de overeenkomstig artikel 14 opgestelde crisiscommunicatieplannen.

Voor de toepassing van de eerste alinea, punt a), nemen andere financiële entiteiten dan micro-ondernemingen in de testplannen scenario's op van cyberaanvallen en omschakelingen tussen de primaire ICT-infrastructuur en de reservecapaciteit, backups en reservefaciliteiten die noodzakelijk zijn om te voldoen aan de in artikel 12 bedoelde verplichtingen.

Financiële entiteiten evalueren regelmatig hun ICT-bedrijfscontinuïteitsbeleid en hun ICT-respons- en herstelplannen, rekening houdend met de resultaten van de overeenkomstig de eerste alinea uitgevoerde tests en de aanbevelingen die voortvloeien uit audits of toezichtbeoordelingen.

7. Andere financiële entiteiten dan micro-ondernemingen beschikken over een functie voor crisisbeheer die in geval van activering van hun ICT-bedrijfscontinuïteitsplannen of ICT-respons- en herstelplannen onder meer duidelijke procedures bepaalt voor het beheer van interne en externe crisiscommunicatie in overeenstemming met artikel 14.

8. Financiële entiteiten houden gemakkelijk toegankelijke registers bij van hun activiteiten vóór en tijdens storingen wanneer hun ICT-bedrijfscontinuïteitsplannen en ICT-respons- en herstelplannen worden geactiveerd.

9. Centrale effectenbewaarinstellingen verstrekken de bevoegde autoriteiten kopieën van de resultaten van de ICT-bedrijfscontinuïteitstests of van soortgelijke oefeningen.

10. Andere financiële entiteiten dan micro-ondernemingen verstrekken de bevoegde autoriteiten op hun verzoek een raming van de geaggregeerde jaarlijkse kosten en verliezen als gevolg van ernstige ICT-gerelateerde incidenten.

11. Overeenkomstig artikel 16 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 ontwikkelen de ETA's, via het Gemengd Comité, uiterlijk op 17 juli 2024 gemeenschappelijke richtsnoeren voor de raming van de geaggregeerde jaarlijkse kosten en verliezen als bedoeld in lid 10.

Artikel 12

Back-upbeleid en -procedures, terugzettings- en herstelprocedures en -methoden

1. Teneinde het terugzetten van ICT-systemen en gegevens te verzekeren met een minimale uitval en een beperkte verstoring en beperkt verlies, ontwikkelen en documenteren financiële entiteiten als onderdeel van hun kader voor ICT-risicobeheer:

a) back-upbeleid en -procedures waarin nader wordt bepaald op welke gegevens de back-up en de minimale frequentie van de back-up worden toegepast, op basis van het kritieke karakter van de informatie of het vertrouwelijkheidsniveau van de gegevens;

b) terugzettings- en herstelprocedures en -methoden.

2. Financiële entiteiten zetten back-upsystemen op die kunnen worden geactiveerd in overeenstemming met het back-upbeleid, de back-upprocedures, en de terugzettings- en herstelprocedures en -methoden. De activering van back-upsystemen mag de beveiliging van de netwerk- en informatiesystemen of de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens niet in gevaar brengen. De back-upprocedures en de terugzettings- en herstelprocedures en -methoden worden periodiek getest.

3. Wanneer financiële entiteiten back-upgegevens terugzetten met behulp van eigen systemen, maken zij gebruik van ICT-systemen die fysiek of logisch gescheiden zijn van het bron-ICT-systeem. De ICT-systemen zijn tegen ongeoorloofde toegang of beschadiging van ICT beveiligd en maken het mogelijk diensten indien nodig tijdig terug te zetten met gebruikmaking van gegevens en systeemback-ups.

Voor centrale tegenpartijen maken de herstelplannen het herstel mogelijk van alle transacties ten tijde van de verstoring, om de centrale tegenpartij in staat te stellen haar activiteiten met zekerheid voort te zetten en de transactie af te wikkelen op de geplande datum.

Aanbieders van datarapporteringsdiensten houden daarnaast voldoende middelen aan en beschikken over back-up- en terugzetfaciliteiten om hun diensten te allen tijde aan te bieden en te onderhouden.

4. Andere financiële entiteiten dan micro-ondernemingen houden ICT-capaciteiten in reserve met middelen, capaciteiten en functies die geschikt zijn om te voorzien in de zakelijke behoeften. Micro-ondernemingen gaan op basis van hun risicoprofiel na of dergelijke reservecapaciteiten behouden moeten worden.

5. Centrale effectenbewaarinstellingen handhaven ten minste één secundaire verwerkingslocatie, met adequate middelen, capaciteiten, functies en personeelsvoorziening om te voorzien in de zakelijke behoeften.

De secundaire verwerkingslocatie is:

a) fysiek gevestigd op een bepaalde afstand van de primaire verwerkingslocatie om te verzekeren dat de locatie een ander risicoprofiel heeft en om te voorkomen dat deze wordt getroffen door de gebeurtenis die de primaire locatie heeft getroffen;

b) in staat de continuïteit van kritieke of belangrijke functies op dezelfde manier te waarborgen als de primaire locatie of het niveau van diensten te leveren dat noodzakelijk is om ervoor te zorgen dat de financiële entiteit haar kritieke activiteiten verricht binnen het kader van de hersteldoelstellingen;

c) onmiddellijk toegankelijk voor het personeel van de financiële entiteit om de continuïteit van kritieke of belangrijke functies te waarborgen ingeval de primaire verwerkingslocatie niet langer beschikbaar is.

6. Bij het bepalen van de doelstellingen inzake hersteltijd en herstelpunt voor elke functie houden financiële entiteiten rekening met de vraag of het een kritieke of belangrijke functie betreft en met het potentiële algemene effect op de marktefficiëntie. Deze tijdsdoelstellingen zorgen ervoor dat de overeengekomen niveaus in extreme scenario's worden gehaald.

7. Bij herstel van een ICT-gerelateerd incident verrichten financiële entiteiten de benodigde controles, ook meerdere controles, waaronder afstemmingen, om ervoor te zorgen dat het hoogste niveau van gegevensintegriteit wordt gehandhaafd. Deze controles worden ook verricht bij het reconstrueren van gegevens van externe belanghebbenden om te waarborgen dat alle gegevens consistent zijn tussen de systemen.

Artikel 13

Scholing en ontwikkeling

1. Financiële entiteiten beschikken over capaciteiten en personele middelen om informatie te verzamelen over kwetsbaarheden en cyberdreigingen, ICT-gerelateerde incidenten, met name cyberaanvallen, en om de waarschijnlijke gevolgen ervan voor hun digitale operationele weerbaarheid te analyseren.

2. Financiële entiteiten verrichten ICT-gerelateerde post-incidentevaluaties na verstoringen van hun kernactiviteiten ten gevolge van een ernstig ICT-gerelateerd incident, analyseren daarbij de oorzaken van de verstoring en identificeren de verbeteringen die moeten worden aangebracht in de ICT-activiteiten of in het kader van het ICT-bedrijfscontinuïteitsbeleid als bedoeld in artikel 11.

Andere financiële entiteiten dan micro-ondernemingen delen op verzoek de bevoegde autoriteiten de wijzigingen mee die na de in de eerste alinea bedoelde ICT-gerelateerde post-incidentevaluaties zijn doorgevoerd.

In de in de eerste alinea bedoelde ICT-gerelateerde post-incidentevaluaties wordt bepaald of de vastgestelde procedures zijn gevolgd en of de genomen maatregelen doeltreffend zijn geweest, onder meer met betrekking tot:

a) de snelheid waarmee is gereageerd op veiligheidswaarschuwingen en de effecten en de ernst van ICT-gerelateerde incidenten zijn vastgesteld;

b) de kwaliteit en de snelheid bij het verrichten van een forensische analyse, indien deze passend wordt geacht;

c) de doeltreffendheid van incidentescalatie binnen de financiële entiteit;

d) de doeltreffendheid van interne en externe communicatie.

3. In het ICT-risicobeoordelingsproces wordt voortdurend naar behoren rekening gehouden met lessen die voortspruiten uit de overeenkomstig de artikelen 26 en 27 uitgevoerde tests op de digitale operationele weerbaarheid en uit ICT-gerelateerde incidenten die zich in het reële leven hebben voorgedaan, met name cyberaanvallen, alsmede met problemen die zich voordoen bij de activering van ICT-bedrijfscontinuïteitsplannen en ICT-respons- en -herstelplannen, samen met relevante informatie die met tegenpartijen wordt uitgewisseld en tijdens toetsingen in het toezicht worden beoordeeld. Die bevindingen vormen de basis voor passende herzieningen van relevante onderdelen van het kader voor ICT-risicobeheer als bedoeld in artikel 6, lid 1.

4. Financiële entiteiten zien toe erop toe dat hun strategie voor digitale operationele weerbaarheid als bedoeld in artikel 6, lid 8, op doeltreffende wijze wordt uitgevoerd. Zij inventariseren de ontwikkeling van ICT-risico's in de tijd, analyseren de frequentie, de types, de omvang en de evolutie van ICT-gerelateerde incidenten, met name cyberaanvallen en de patronen daarvan, teneinde inzicht te krijgen in het niveau van blootstelling aan ICT-risico's, met name met betrekking tot kritieke of belangrijke functies, en de maturiteit en paraatheid van de financiële entiteit ten aanzien van deze risico's te verhogen.

5. Het leidinggevend ICT-personeel brengt bij het leidinggevend orgaan ten minste jaarlijks verslag uit over de in lid 3 bedoelde bevindingen en doet aanbevelingen.

6. Financiële entiteiten ontwikkelen bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel. Die programma's en opleidingen zijn van toepassing op alle werknemers en hoger leidinggevend personeel, en hebben een niveau van complexiteit dat in verhouding staat tot hun takenpakket. In voorkomend geval nemen financiële entiteiten overeenkomstig artikel 30, lid 2, punt i), ook derde aanbieders van ICT-diensten op in hun relevante opleidingsprogramma's.

7. Andere financiële entiteiten dan micro-ondernemingen houden voortdurend toezicht op relevante technologische ontwikkelingen, ook om inzicht te krijgen in de mogelijke effecten van de invoering van deze nieuwe technologieën op de ICT-beveiligingsvereisten en de digitale operationele weerbaarheid. Zij blijven op de hoogte van de meest recente processen voor ICT-risicobeheer, om bestaande of nieuwe vormen van cyberaanvallen doeltreffend aan te pakken.

Artikel 14

Communicatie

1. Als onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 6, lid 1, beschikken financiële entiteiten over crisiscommunicatieplannen die het mogelijk maken ten minste ernstige ICT-gerelateerde incidenten of kwetsbaarheden op verantwoordelijke wijze bekend te maken aan cliënten en tegenpartijen en, in voorkomend geval, aan het publiek.

2. Als onderdeel van het kader voor ICT-risicobeheer voeren financiële entiteiten een communicatiebeleid in voor het interne personeel en externe belanghebbenden. In het communicatiebeleid voor het personeel wordt rekening gehouden met de noodzaak om een onderscheid te maken tussen personeel dat betrokken is bij het ICT-risicobeheer, met name het personeel dat verantwoordelijk is voor respons en herstel, en personeel dat moet worden geïnformeerd.

3. Ten minste één persoon in de financiële entiteit wordt belast met de uitvoering van de communicatiestrategie voor ICT-gerelateerde incidenten en vervult daartoe de rol van woordvoerder bij het publiek en de media.

Artikel 15

Verdere harmonisatie van ICT-risicobeheersinstrumenten, -methoden, -processen en -beleidslijnen

De ETA's stellen via het Gemengd Comité en in overleg met het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), gemeenschappelijke ontwerpen van technische reguleringsnormen op met het doel:

a) nadere elementen te specificeren die moeten worden opgenomen in de beleidslijnen, procedures, protocollen en instrumenten met betrekking tot ICT-beveiliging als bedoeld in artikel 9, lid 2, teneinde de veiligheid van netwerken te garanderen, passende waarborgen tegen inbreuken en misbruik van gegevens mogelijk te maken, de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, met inbegrip van cryptografische technieken, te beschermen en een nauwkeurige en snelle doorgifte van gegevens zonder ernstige verstoringen en onnodige vertragingen te waarborgen;

b) verdere onderdelen van de controle van rechten voor toegangsbeheer als bedoeld in artikel 9, lid 4, punt c), en het daarmee verband houdende personeelsbeleid te ontwikkelen, waarin de toegangsrechten en de procedures voor het toekennen en intrekken van rechten nader worden gespecificeerd, en toezicht wordt uitgeoefend op afwijkend gedrag met betrekking tot het ICT-risico via passende indicatoren, onder meer voor patronen en uren van netwerkgebruik, IT-activiteit en onbekende toestellen;

c) de mechanismen als bedoeld in artikel 10, lid 1, om een snelle detectie van afwijkende activiteiten mogelijk te maken, verder te ontwikkelen alsmede de criteria van artikel 10, lid 2, om processen voor detectie van ICT-gerelateerde incidenten en respons daarop in werking te stellen;

d) de onderdelen van het ICT-bedrijfscontinuïteitsbeleid als bedoeld in artikel 11, lid 1, verder te specificeren;

e) het testen van de ICT-bedrijfscontinuïteitsplannen als bedoeld in artikel 11, lid 6, verder te specificeren om ervoor te zorgen dat bij het testen naar behoren rekening wordt gehouden met scenario's waarin de kwaliteit van voorziening van een kritieke of belangrijke functie tot op een onaanvaardbaar niveau verslechtert of deze functie uitvalt, en de potentiële effecten van de insolventie of andere gebreken van een relevante derde aanbieder van ICT-diensten en, indien van toepassing, de politieke risico's in de rechtsgebieden van de respectieve aanbieders naar behoren in aanmerking worden genomen;

f) de onderdelen van de ICT-respons- en -herstelplannen als bedoeld in artikel 11, lid 3, verder te specificeren;

g) de inhoud en de vorm van het in artikel 6, lid 5, bedoelde evaluatieverslag van het kader voor ICT-risicobeheer verder te specificeren.

Bij het ontwikkelen van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang en het algemene risicoprofiel van de financiële entiteit en met de aard, schaal en complexiteit van de diensten, activiteiten en verrichtingen ervan, waarbij zij terdege rekening houden met elk specifiek kenmerk dat voortvloeit uit de specifieke aard van de activiteiten in verschillende financiëledienstensectoren.

De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 januari 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Artikel 16

Vereenvoudigd kader voor ICT-risicobeheer

1. De artikelen 5 tot en met 15 van deze verordening zijn niet van toepassing op kleine en niet-verweven beleggingsondernemingen, betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld; instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld en waarvoor de lidstaten hebben besloten de in artikel 2, lid 4, van deze verordening bedoelde optie niet toe te passen; instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld, en kleine instellingen voor bedrijfspensioenvoorziening.

Onverminderd de eerste alinea moeten de in de eerste alinea vermelde entiteiten:

a) een degelijk en gedocumenteerd kader voor ICT-risicobeheer tot stand brengen en handhaven, waarin de mechanismen en maatregelen worden beschreven die gericht zijn op een snel, efficiënt en alomvattend beheer van het ICT-risico, met inbegrip van de bescherming van relevante fysieke componenten en infrastructuur;

b) voortdurend toezicht houden op de beveiliging en werking van alle ICT-systemen;

c) de gevolgen van ICT-risico's tot een minimum beperken door solide, weerbare en geactualiseerde ICT-systemen, -protocollen en -instrumenten te gebruiken die geschikt zijn voor het ondersteunen van de prestaties van hun activiteiten en de verlening van diensten, en de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens in de netwerk- en informatiesystemen adequaat beschermen;

d) ervoor zorgen dat bronnen van ICT-risico's en anomalieën in de netwerk- en informatiesystemen zo spoedig mogelijk worden geïdentificeerd en gedetecteerd en ICT-gerelateerde incidenten snel kunnen worden afgehandeld;

e) de belangrijkste afhankelijkheden ten aanzien van derde aanbieders van ICT-diensten in kaart brengen;

f) de continuïteit van kritieke of belangrijke functies waarborgen door middel van bedrijfscontinuïteitsplannen en respons- en herstelmaatregelen, die ten minste back-up- en herstelmaatregelen omvatten;

g) de in punt f) bedoelde plannen en maatregelen, alsmede de doeltreffendheid van de overeenkomstig de punten a) en c) uitgevoerde controles regelmatig testen;

h) in voorkomend geval de relevante operationele conclusies die voortvloeien uit de in punt g) bedoelde tests en uit de analyse na een incident opnemen in het ICT-risicobeoordelingsproces, en overeenkomstig de behoeften en het ICT-risicoprofiel bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleiding inzake digitale operationele weerbaarheid voor personeel en leidinggevenden ontwikkelen.

2. Het in lid 1, tweede alinea, punt a), bedoelde kader voor ICT-risicobeheer wordt overeenkomstig de toezichtinstructies op gezette tijden en bij ernstige ICT-gerelateerde incidenten gedocumenteerd en geëvalueerd. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen. Een evaluatieverslag van het kader voor ICT-risicobeheer wordt op verzoek bij de bevoegde autoriteit ingediend.

3. De ETA's stellen via het Gemengd Comité en in overleg met Enisa gemeenschappelijke ontwerpen van technische reguleringsnormen op met het doel:

a) de elementen die moeten worden opgenomen in het in lid 1, tweede alinea, punt a), bedoelde kader voor ICT-risicobeheer verder te specificeren;

b) de elementen met betrekking tot systemen, protocollen en instrumenten om de effecten van het in lid 1, tweede alinea, punt c), bedoelde ICT-risico tot een minimum te beperken verder te specificeren, teneinde de veiligheid van netwerken te garanderen, passende waarborgen tegen inbreuken en misbruik van gegevens mogelijk te maken en de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens te beschermen;

c) de onderdelen van de in lid 1, tweede alinea, punt f), bedoelde ICT-bedrijfscontinuïteitsplannen verder te specificeren;

d) de regels voor het testen van bedrijfscontinuïteitsplannen verder te specificeren, de doeltreffendheid van de in lid 1, tweede alinea, punt g), bedoelde controles te waarborgen, en ervoor te zorgen dat bij dergelijke tests terdege rekening wordt gehouden met scenario's waarin de kwaliteit van voorziening van een kritieke of belangrijke functie tot op een onaanvaardbaar niveau verslechtert of deze functie uitvalt;

e) de inhoud en de vorm van het in lid 2 bedoelde evaluatieverslag van het kader voor ICT-risicobeheer verder te specificeren.

Bij het opstellen van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang en het algemene risicoprofiel van de financiële entiteit, en met de aard, schaal en complexiteit van de diensten, activiteiten en verrichtingen ervan.

De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 januari 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

HOOFDSTUK III

Beheer, classificatie en rapportage van ICT-gerelateerde incidenten

Artikel 17

Beheerproces voor ICT-gerelateerde incidenten

1. Financiële entiteiten omschrijven een beheerproces voor ICT-gerelateerde incidenten, stellen dit vast en leggen dit ten uitvoer, om ICT-gerelateerde incidenten te detecteren, te beheren en te melden.

2. Financiële entiteiten registreren alle ICT-gerelateerde incidenten en significante cyberdreigingen. Financiële entiteiten stellen passende procedures en processen vast voor een consistente en geïntegreerde monitoring, behandeling en follow-up van ICT-gerelateerde incidenten, teneinde ervoor te zorgen dat onderliggende oorzaken worden opgespoord, gedocumenteerd en weggenomen om dergelijke incidenten te voorkomen.

3. Het in lid 1 bedoelde beheerproces voor ICT-gerelateerde incidenten heeft tot doel:

a) indicatoren voor vroegtijdige waarschuwing in te voeren;

b) procedures vast te stellen om ICT-gerelateerde incidenten te identificeren, te detecteren, te categoriseren en te classificeren op basis van de prioriteit en de ernst ervan en op basis van het kritieke karakter van de getroffen diensten in overeenstemming met de criteria van artikel 18, lid 1;

c) functies en verantwoordelijkheden toe te wijzen die voor verschillende incidenttypes en -scenario's moeten worden geactiveerd;

d) plannen op te stellen voor communicatie met personeel, externe belanghebbenden en media in overeenstemming met artikel 14, en voor mededeling aan cliënten, voor interne escalatieprocedures, met inbegrip van ICT-gerelateerde klachten van cliënten, alsmede voor verstrekking van informatie, indien noodzakelijk, aan financiële entiteiten die optreden als tegenpartijen;

e) te verzekeren dat ten minste ernstige ICT-gerelateerde incidenten aan het desbetreffende hoger leidinggevend personeel worden gemeld, en het leidinggevend orgaan te informeren over ten minste ernstige ICT-gerelateerde incidenten met toelichting bij de effecten, de respons en de in te stellen aanvullende controles ten gevolge van dergelijke ICT-gerelateerde incidenten;

f) responsprocedures voor ICT-gerelateerde incidenten in te stellen om de effecten daarvan te beperken en ervoor te zorgen dat de diensten tijdig operationeel en veilig worden.

Artikel 18

Classificatie van ICT-gerelateerde incidenten en cyberdreigingen

1. Financiële entiteiten classificeren ICT-gerelateerde incidenten en bepalen de effecten daarvan op basis van de volgende criteria:

a) het aantal en/of de relevantie van cliënten of financiële tegenpartijen en, indien van toepassing, de hoeveelheid of het aantal transacties die door het ICT-gerelateerde incident zijn getroffen, en de vraag of het ICT-gerelateerde incident reputatieschade heeft veroorzaakt;

b) de duur van het ICT-gerelateerde incident, waaronder de uitvaltijd van de dienst;

c) de geografische spreiding van de gebieden die door het ICT-gerelateerde incident zijn getroffen, met name indien meer dan twee lidstaten zijn getroffen;

d) de gegevensverliezen ten gevolge van het ICT-gerelateerde incident met betrekking tot beschikbaarheid, authenticiteit, integriteit or vertrouwelijkheid van gegevens;

e) de mate waarin de getroffen diensten, waaronder de transacties en verrichtingen van de financiële entiteit, als cruciaal kunnen worden aangemerkt;

f) de economische effecten, met name directe en indirecte kosten en verliezen, van het ICT-gerelateerde incident in absolute en relatieve termen.

2. Financiële entiteiten classificeren cyberdreigingen als significant op basis van de mate waarin de risicovolle diensten, waaronder de transacties en verrichtingen van de financiële entiteit, als cruciaal kunnen worden aangemerkt, het aantal en/of de relevantie van de beoogde cliënten of financiële tegenpartijen en de geografische spreiding van de risicogebieden.

3. De ETA's stellen via het Gemengd Comité en in overleg met de ECB en Enisa gemeenschappelijke ontwerpen van technische reguleringsnormen op waarin het volgende nader wordt gespecificeerd:

a) de criteria vastgesteld in lid 1, met inbegrip van materialiteitsdrempels voor het bepalen van ernstige ICT-gerelateerde incidenten of, indien van toepassing, ernstige betalingsgerelateerde operationele of beveiligingsincidenten waarvoor de rapportageverplichting van artikel 19, lid 1, geldt;

b) de door de bevoegde autoriteiten toe te passen criteria voor de beoordeling van de relevantie van ernstige ICT-gerelateerde incidenten of, indien van toepassing, ernstige betalingsgerelateerde operationele of beveiligingsincidenten voor relevante bevoegde autoriteiten van andere lidstaten, en de nadere informatie van verslagen over ernstige ICT-gerelateerde incidenten of, indien van toepassing, ernstige betalingsgerelateerde operationele of beveiligingsincidenten die overeenkomstig artikel 19, leden 6 en 7, aan andere bevoegde autoriteiten moeten worden meegedeeld;

c) de criteria van lid 2 van dit artikel, met inbegrip van hoge materialiteitsdrempels voor het bepalen van significante cyberdreigingen.

4. Bij het opstellen van de in lid 3 van dit artikel bedoelde gemeenschappelijke ontwerpen van technische reguleringsnormen houden de ETA's rekening met de criteria van artikel 4, lid 2, en met internationale normen, richtsnoeren en specificaties die door Enisa zijn ontwikkeld en gepubliceerd, met inbegrip van, in voorkomend geval, specificaties voor andere economische sectoren. Voor de toepassing van de criteria van artikel 4, lid 2, houden de ETA's er terdege rekening mee dat micro-ondernemingen en kleine en middelgrote ondernemingen voldoende middelen en capaciteit moeten kunnen mobiliseren om ICT-gerelateerde incidenten snel onder controle te krijgen.

De ETA's leggen die gemeenschappelijke ontwerpen van technische reguleringsnormen uiterlijk op 17 januari 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in lid 3 bedoelde technische reguleringsnormen overeenkomstig de artikelen 10 tot en met 14 van Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 vast te stellen.

Artikel 19

Rapportage van ernstige ICT-gerelateerde incidenten en vrijwillige melding van significante cyberdreigingen

1. Financiële entiteiten melden overeenkomstig lid 4 van dit artikel ernstige ICT-gerelateerde incidenten aan de relevante bevoegde autoriteit als bedoeld in artikel 46.

Staat een financiële entiteit onder toezicht van meer dan een nationale bevoegde autoriteit als bedoeld in artikel 46, dan wijzen de lidstaten één bevoegde autoriteit aan als de relevante bevoegde autoriteit die verantwoordelijk is voor de uitvoering van de in dit artikel bedoelde functies en taken.

Kredietinstellingen die overeenkomstig artikel 6, lid 4, van Verordening (EU) nr. 1024/2013 als significant zijn geclassificeerd, rapporteren ernstige ICT-gerelateerde incidenten aan de relevante nationale bevoegde autoriteit die overeenkomstig artikel 4 van Richtlijn 2013/36/EU is aangewezen, die dat verslag onverwijld doorzendt aan de ECB.

Voor de toepassing van de eerste alinea stellen financiële entiteiten, na het verzamelen en analyseren van alle relevante informatie, de in lid 4 van dit artikel bedoelde eerste kennisgeving en verslagen op met gebruikmaking van de modellen als bedoeld in artikel 20, en dienen zij deze in bij de bevoegde autoriteit. Indien het technisch niet mogelijk is de eerste kennisgeving met gebruikmaking van het model in te dienen, stellen de financiële entiteiten de bevoegde autoriteit met gebruikmaking van alternatieve middelen daarvan in kennis.

De in lid 4 bedoelde eerste kennisgeving en verslagen bevatten alle informatie die de bevoegde autoriteit nodig heeft om de draagwijdte van het ernstige ICT-gerelateerde incident te bepalen en mogelijke grensoverschrijdende effecten te beoordelen.

Onverminderd de rapportage op grond van de eerste alinea door de financiële entiteit aan de relevante bevoegde autoriteit, kunnen de lidstaten ook bepalen dat sommige of alle financiële entiteiten de in lid 4 van dit artikel bedoelde eerste kennisgeving en verslagen die met gebruikmaking van de in artikel 20 bedoelde modellen zijn opgesteld, eveneens moeten worden verstrekt aan de bevoegde autoriteiten of de *computer security incident response teams* (CSIRT's) die zijn aangewezen of ingesteld overeenkomstig Richtlijn (EU) 2022/2555.

2. Financiële entiteiten kunnen significante cyberdreigingen op vrijwillige basis melden aan de relevante bevoegde autoriteit wanneer zij van oordeel zijn dat de dreiging relevant is voor het financiële stelsel, de gebruikers van diensten of de cliënten. De relevante bevoegde autoriteit kan dergelijke informatie aan de in lid 6 genoemde andere relevante autoriteiten verstrekken.

Kredietinstellingen die overeenkomstig artikel 6, lid 4, van Verordening (EU) nr. 1024/2013 als significant zijn geclassificeerd, kunnen op vrijwillige basis significante cyberdreigingen melden aan de relevante nationale bevoegde autoriteit die overeenkomstig artikel 4 van Richtlijn 2013/36/EU is aangewezen, die de melding onverwijld doorzendt aan de ECB.

De lidstaten kunnen bepalen dat de financiële entiteiten die overeenkomstig de eerste alinea op vrijwillige basis kennisgeving doen, die kennisgeving ook kunnen doorsturen naar de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde CSIRT's.

3. Wanneer een ernstig ICT-gerelateerd incident optreedt en gevolgen heeft voor de financiële belangen van cliënten, stellen financiële entiteiten, zodra zij het incident hebben opgemerkt, hun cliënten onverwijld in kennis van het ernstige ICT-gerelateerde incident en van de maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk incident te beperken.

In het geval van een significante cyberdreiging stellen financiële entiteiten, in voorkomend geval, hun cliënten die mogelijk getroffen zijn in kennis van passende beschermingsmaatregelen die zij kunnen nemen.

4. Financiële entiteiten dienen, binnen de overeenkomstig artikel 20, eerste alinea, punt a), ii), vast te stellen termijnen, bij de relevante bevoegde autoriteit het volgende in:

a) een eerste kennisgeving;

b) een tussentijds verslag na de eerste kennisgeving als bedoeld in punt a), zodra de status van het oorspronkelijke incident ingrijpend is gewijzigd of de behandeling van het ernstige ICT-gerelateerde incident is gewijzigd op basis van beschikbare nieuwe informatie, in voorkomend geval gevolgd door geactualiseerde kennisgevingen telkens wanneer een relevante actualisering van de status beschikbaar is, alsmede op specifiek verzoek van de bevoegde autoriteit;

c) een eindverslag, wanneer de analyse van de onderliggende oorzaken is voltooid, ongeacht of er reeds beperkende maatregelen zijn uitgevoerd, en wanneer de werkelijke impactcijfers beschikbaar zijn in plaats van ramingen.

5. Financiële entiteiten mogen de rapportageverplichtingen uit hoofde van dit artikel aan een derde aanbieder van diensten uitbesteden overeenkomstig Unie- en nationaal sectoraal recht. In het geval van een dergelijke uitbesteding blijft de financiële entiteit volledig verantwoordelijk voor het naleven van de vereisten inzake incidentrapportage.

6. Na ontvangst van de in lid 4 bedoelde eerste kennisgeving en verslagen verstrekt de bevoegde autoriteit tijdig nadere bijzonderheden over het ernstige ICT-gerelateerde incident aan de volgende ontvangers op basis van hun respectieve bevoegdheden:

a) de EBA, de ESMA of de Eiopa;

b) de ECB, in het geval van financiële entiteiten als bedoeld in artikel 2, lid 1, punten a), b) en d):

c) de bevoegde autoriteiten, de centrale contactpunten of de CSIRT's die overeenkomstig Richtlijn (EU) 2022/2555 zijn aangewezen of ingesteld;

d) de afwikkelingsautoriteiten, als bedoeld in artikel 3 van Richtlijn 2014/59/EU, en de Gemeenschappelijke Afwikkelingsraad (GAR) met betrekking tot de in artikel 7, lid 2, van Verordening (EU) nr. 806/2014 van het Europees Parlement en de Raad ([37]) bedoelde entiteiten, en met betrekking tot de in artikel 7, lid 4, punt b), en lid 5, van Verordening (EU) nr. 806/2014 bedoelde entiteiten en groepen, indien die bijzonderheden betrekking hebben op incidenten die een risico vormen voor het waarborgen van kritieke functies in de zin van artikel 2, lid 1, punt 35), van Richtlijn 2014/59/EU, en

e) andere relevante overheidsinstanties naar nationaal recht.

7. Na ontvangst van informatie overeenkomstig lid 6 beoordelen de EBA, de ESMA of de Eiopa en de ECB, in overleg met Enisa en in samenwerking met de relevante bevoegde autoriteit, of het ernstige ICT-gerelateerde incident relevant is voor andere bevoegde autoriteiten van andere lidstaten. Na die beoordeling stelt de EBA, de ESMA of de Eiopa de relevante bevoegde autoriteiten van andere lidstaten daarvan zo spoedig mogelijk in kennis. De ECB stelt de leden van het Europees Stelsel van centrale banken in kennis van kwesties die van belang zijn voor het betalingssysteem. Op basis van die kennisgeving nemen de bevoegde autoriteiten, in voorkomend geval, alle nodige maatregelen om de onmiddellijke stabiliteit van het financiële systeem te beschermen.

([37]) Verordening (EU) nr. 806/2014 van het Europees Parlement en de Raad van 15 juli 2014 tot vaststelling van eenvormige regels en een eenvormige procedure voor de afwikkeling van kredietinstellingen en bepaalde beleggingsondernemingen in het kader van een gemeenschappelijk afwikkelingsmechanisme en een gemeenschappelijk afwikkelingsfonds en tot wijziging van Verordening (EU) nr. 1093/2010 (PB L 225 van 30.7.2014, blz. 1).

8. De overeenkomstig lid 7 van dit artikel door de ESMA te geven kennisgeving doet geen afbreuk aan de verantwoordelijkheid van de bevoegde autoriteit om de bijzonderheden van het ernstige ICT-gerelateerde incident onverwijld aan de relevante autoriteit van de lidstaat van ontvangst door te geven, indien een centrale effectenbewaarinstelling aanzienlijke grensoverschrijdende activiteiten in de lidstaat van ontvangst heeft, het ernstige ICT-gerelateerde incident waarschijnlijk ernstige gevolgen voor de financiële markten van de lidstaat van ontvangst zal hebben en indien de bevoegde autoriteiten samenwerkingsovereenkomsten hebben gesloten voor het toezicht op financiële entiteiten.

Artikel 20

Harmonisatie van inhoud en modellen van rapportage

De ETA's ontwikkelen via het Gemengd Comité en in overleg met Enisa en de ECB:

a) gemeenschappelijke ontwerpen van technische reguleringsnormen om:

   i) de inhoud van de rapporten voor ernstige ICT-gerelateerde incidenten vast te stellen, waarbij de in artikel 18, lid 1, vastgelegde criteria worden gehanteerd en verdere elementen worden opgenomen, zoals bijzonderheden voor de vaststelling van de relevantie van rapportage voor andere lidstaten en voor het bepalen of het incident al dan niet een ernstig betalingsgerelateerd operationeel of beveiligingsincident is;

   ii) de uiterste termijnen vast te stellen voor de in artikel 19, lid 4, bedoelde eerste kennisgeving en verslagen;

   iii) de inhoud van de kennisgeving voor significante cyberdreigingen vast te stellen.

   Bij de ontwikkeling van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang en het algemene risicoprofiel van de financiële entiteit en met de aard, schaal en complexiteit van de diensten, activiteiten en verrichtingen ervan, met name om ervoor te zorgen dat voor de toepassing van deze alinea, punt a), ii), de uiterste termijnen zijn afgestemd op de eventuele specifieke kenmerken van de financiële sectoren, zonder dat afbreuk wordt gedaan aan een consistente aanpak van ICT-gerelateerde incidentrapportage op grond van deze verordening en Richtlijn (EU) 2022/2555. De ETA's motiveren eventuele afwijkingen van de in het kader van die richtlijn gevolgde aanpak;

b) gemeenschappelijke ontwerpen van technische uitvoeringsnormen tot vaststelling van de standaardformulieren, modellen en procedures voor het rapporteren van ernstige ICT-gerelateerde incidenten en het melden van significante cyberdreigingen door financiële entiteiten.

De ETA's leggen de gemeenschappelijke ontwerpen van technische reguleringsnormen bedoeld in de eerste alinea, punt a), en de gemeenschappelijke ontwerpen van technische uitvoeringsnormen bedoeld in de eerste alinea, punt b), uiterlijk op 17 juli 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea, punt a), bedoelde gemeenschappelijke technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Aan de Commissie wordt de bevoegdheid toegekend om de in de eerste alinea, punt b), bedoelde technische uitvoeringsnormen vast te stellen overeenkomstig artikel 15 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Artikel 21

Centralisatie van meldingen van ernstige ICT-gerelateerde incidenten

1. De ETA's stellen, via het Gemengd Comité en in overleg met de ECB en Enisa, een gezamenlijk verslag op waarin de haalbaarheid wordt beoordeeld van verdere centralisatie van incidentrapportage door middel van de oprichting van één EU-hub voor de melding van ernstige ICT-gerelateerde incidenten door financiële entiteiten. In het gezamenlijk verslag wordt onderzocht op welke wijze de stroom van ICT-gerelateerde incidentrapportage kan worden vergemakkelijkt, de daarmee gepaard gaande kosten kunnen worden verlaagd en thematische analyses kunnen worden onderbouwd met het oog op een grotere convergentie van het toezicht.

2. Het in lid 1 bedoelde gezamenlijk verslag bevat ten minste:

a) de vereisten voor de oprichting van een unieke EU-hub;

b) de voordelen, beperkingen en risico's, met inbegrip van de risico's in verband met de hoge concentratie van gevoelige informatie;

c) de nodige capaciteit om interoperabiliteit met andere relevante rapportagesystemen te waarborgen;

d) elementen van operationeel beheer;

e) de voorwaarden voor het lidmaatschap;

f) technische regels voor financiële entiteiten en nationale bevoegde autoriteiten om toegang tot de unieke EU-hub te verkrijgen;

g) een voorlopige beoordeling van de financiële kosten voor de oprichting van het operationele platform ter ondersteuning van de unieke EU-hub, met inbegrip van de vereiste deskundigheid.

3. De ETA's leggen het verslag bedoeld in lid 1 uiterlijk op 17 januari 2025 voor aan het Europees Parlement, de Raad en de Commissie.

Artikel 22

Feedback van toezichthouders

1. Onverminderd de technische input, het advies of de corrigerende maatregelen en de daaropvolgende follow-up die, in voorkomend geval, overeenkomstig het nationale recht door de CSIRT's kunnen worden verstrekt op grond van Richtlijn (EU) 2022/2555 , bevestigt de bevoegde autoriteit na ontvangst van de in artikel 19, lid 4, bedoelde eerste kennisgeving en verslagen, de ontvangst ervan en kan zij, waar mogelijk, tijdig relevante en evenredige feedback of richtsnoeren op hoog niveau aan de financiële entiteit verstrekken, met name door relevante geanonimiseerde informatie en inlichtingen over soortgelijke bedreigingen beschikbaar te stellen, en kan zij de op het niveau van de financiële entiteit toegepaste corrigerende maatregelen bespreken en onderzoeken hoe de nadelige effecten in de financiële sector zo veel mogelijk kunnen worden beperkt en verzacht. Onverminderd de ontvangen feedback van toezichthouders blijven financiële entiteiten volledig verantwoordelijk voor de behandeling en de gevolgen van de ICT-gerelateerde incidenten die op grond van artikel 19, lid 1, zijn gerapporteerd.

2. De ETA's brengen jaarlijks via het Gemengd Comité een geanonimiseerd en geaggregeerd verslag uit over de ernstige ICT-gerelateerde incidenten, de details waarvan door de bevoegde autoriteiten overeenkomstig artikel 19, lid 6, worden verstrekt, met vermelding van ten minste het aantal ernstige ICT-gerelateerde incidenten, de aard ervan, de gevolgen ervan voor de werking van financiële entiteiten of cliënten, de genomen corrigerende maatregelen en de kosten.

De ETA's geven waarschuwingen en stellen statistieken op hoog niveau op ter ondersteuning van ICT-dreigings- en kwetsbaarheidsbeoordelingen.

Artikel 23

Betalingsgerelateerde operationele of beveiligingsincidenten die kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatiediensten en instellingen voor elektronisch geld betreffen

De in dit hoofdstuk vastgestelde vereisten zijn ook van toepassing bij betalingsgerelateerde operationele of beveiligingsincidenten en ernstige betalingsgerelateerde operationele of beveiligingsincidenten die kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatiediensten en instellingen voor elektronisch geld betreffen.

HOOFDSTUK IV

Testen van digitale operationele weerbaarheid

Artikel 24

Algemene vereisten voor uitvoering van tests van digitale operationele weerbaarheid

1. Voor de beoordeling van de paraatheid ten aanzien van de behandeling van ICT-gerelateerde incidenten, de omschrijving van zwakheden, gebreken en lacunes in de digitale operationele weerbaarheid, en de snelle uitvoering van corrigerende maatregelen zorgen andere financiële entiteiten dan micro-ondernemingen, rekening houdend met de criteria in artikel 4, lid 2, voor het vaststellen, handhaven en evalueren van een degelijk en alomvattend programma voor het testen van de digitale operationele weerbaarheid als integrerend onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 6.

2. Het testprogramma voor digitale operationele weerbaarheid omvat een reeks beoordelingen, tests, methodologieën, praktijken en instrumenten die overeenkomstig de artikelen 25 en 26 moeten worden toegepast.

3. Bij de uitvoering van het in lid 1 van dit artikel bedoelde programma voor het testen van de digitale operationele weerbaarheid volgen andere financiële entiteiten dan micro-ondernemingen een risicogebaseerde benadering, waarbij rekening wordt gehouden met de criteria van artikel 4, lid 2, en met het veranderende landschap van het ICT-risico, eventuele specifieke risico's waaraan de betrokken financiële entiteit wordt of kan worden blootgesteld, de kritieke aard van informatieactiva en verleende diensten, alsmede alle andere factoren die de financiële entiteit passend acht.

4. Andere financiële entiteiten dan micro-ondernemingen zorgen ervoor dat de tests worden uitgevoerd door interne of externe onafhankelijke partijen. Wanneer tests worden uitgevoerd door een interne tester, zetten financiële entiteiten voldoende middelen in en zorgen zij ervoor dat belangenconflicten gedurende de hele ontwerp- en uitvoeringsfase van de test worden voorkomen.

5. Andere financiële entiteiten dan micro-ondernemingen stellen procedures en beleidslijnen vast om alle problemen die tijdens de uitvoering van de tests aan het licht zijn gekomen, te prioriteren, te classificeren en te verhelpen, en stellen interne valideringsmethoden vast om na te gaan of alle vastgestelde zwakheden, gebreken of lacunes volledig worden aangepakt.

6. Andere financiële entiteiten dan micro-ondernemingen zorgen ervoor dat ten minste eenmaal per jaar passende tests worden uitgevoerd op alle ICT-systemen en -toepassingen die kritieke of belangrijke functies ondersteunen.

Artikel 25

Testen van ICT-instrumenten en -systemen

1. Het testprogramma voor digitale operationele weerbaarheid bedoeld in artikel 24 voorziet, overeenkomstig de criteria in artikel 4, lid 2, in de uitvoering van passende tests, zoals kwetsbaarheidsbeoordelingen en -scans, opensourceanalyses, netwerkbeveiligingsbeoordelingen, kloofanalyses, beoordelingen van fysieke beveiliging, vragenlijsten en scanningsoftware-oplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests, eind-tot-eindtests en penetratietests.

2. Centrale effectenbewaarinstellingen en centrale tegenpartijen verrichten kwetsbaarheidsbeoordelingen voordat nieuwe of bestaande toepassingen en infrastructuurcomponenten, en ICT-diensten ter ondersteuning van kritieke of belangrijke functies van de financiële entiteit worden ingezet of opnieuw worden ingezet.

3. Voor de uitvoering van de in lid 1 bedoelde tests combineren de micro-ondernemingen een op risico's gebaseerde aanpak met een strategische planning van ICT-tests, en houden zij hierbij naar behoren rekening met het noodzakelijke evenwicht tussen enerzijds de hoeveelheid middelen en tijd die aan de in dit artikel bedoelde ICT-tests moet worden toegewezen, en anderzijds de urgentie, het soort risico, de kritieke aard van informatieactiva en van de geleverde diensten, alsmede alle andere relevante factoren, met inbegrip van het vermogen van de financiële entiteit om berekende risico's te nemen.

Artikel 26

Geavanceerde tests van ICT-instrumenten, -systemen en -processen op basis van TLPT

1. Overeenkomstig lid 8, derde alinea, van dit artikel aangewezen andere financiële entiteiten dan de in artikel 16, lid 1, eerste alinea, bedoelde entiteiten en dan micro-ondernemingen verrichten ten minste om de drie jaar geavanceerde tests uit door middel van TLPT. Op basis van het risicoprofiel van de financiële entiteit en rekening houdend met operationele omstandigheden kan de bevoegde autoriteit, indien nodig, de financiële entiteit verzoeken deze frequentie te verlagen of te verhogen.

2. Elke dreigingsgestuurde penetratietest heeft betrekking op meerdere of alle kritieke of belangrijke functies van een financiële entiteit en worden uitgevoerd op systemen die prestaties in het reële leven verrichten ter ondersteuning van deze functies.

Financiële entiteiten bepalen alle relevante onderliggende ICT-systemen, -processen en technologieën ter ondersteuning van kritieke of belangrijke functies en ICT-diensten, met inbegrip van die ter ondersteuning van uitbestede of met derde aanbieders van ICT-diensten contractueel overeengekomen kritieke of belangrijke functies.

Financiële entiteiten beoordelen voor welke kritieke of belangrijke functies TLPT moeten worden verricht. Het resultaat van die beoordeling bepaalt het exacte toepassingsgebied van TLPT en wordt door de bevoegde autoriteiten gevalideerd.

3. Wanneer derde aanbieders van ICT-diensten binnen het toepassingsgebied van de TLPT vallen, neemt de financiële entiteit de nodige maatregelen en waarborgen om de deelname van deze derde aanbieders van ICT-diensten aan de TLPT te waarborgen en behoudt de financiële entiteit de volledige verantwoordelijkheid voor het waarborgen van de naleving van deze verordening.

4. Onverminderd lid 2, eerste en tweede alinea, kunnen, indien redelijkerwijs mag worden verwacht dat de deelname van een derde aanbieder van ICT-diensten aan de TLPT, als bedoeld in lid 3, een negatief effect zal hebben op de kwaliteit of de beveiliging van diensten die door de derde aanbieder van ICT-diensten worden verleend aan klanten die entiteiten zijn die buiten het toepassingsgebied van deze verordening vallen, of op de vertrouwelijkheid van de gegevens met betrekking tot dergelijke diensten, de financiële entiteit en de derde aanbieder van ICT-diensten schriftelijk overeenkomen dat de derde aanbieder van ICT-diensten rechtstreeks een contractuele overeenkomst sluit met een externe tester voor de uitvoering, onder leiding van één aangewezen financiële entiteit, van een gebundelde TLPT waarbij meerdere financiële entiteiten betrokken zijn waaraan de derde aanbieder van ICT-diensten ICT-diensten verleent (gebundelde tests).

Deze gebundelde tests hebben betrekking op het relevante gamma van ICT-diensten die kritieke of belangrijke functies ondersteunen waarvoor de financiële entiteiten met de respectieve derde aanbieders van ICT-diensten een contract hebben gesloten. De gebundelde tests worden beschouwd als TLPT die worden uitgevoerd door de financiële entiteiten die aan deze tests deelnemen.

Het aantal financiële entiteiten dat deelneemt aan de gebundelde tests wordt afgestemd op de complexiteit en de aard van de betrokken diensten.

5. Met de medewerking van derde aanbieders van ICT-diensten en andere betrokken partijen, inclusief testers, maar exclusief de bevoegde autoriteiten, passen de financiële entiteiten doeltreffende risicobeheerscontroles toe om de risico's van potentiële effecten op gegevens, schade aan activa en verstoring van kritieke of belangrijke functies, diensten of activiteiten bij de financiële entiteit zelf, bij haar tegenhangers of in de financiële sector te mitigeren.

6. Na afloop van de tests, nadat overeenstemming is bereikt over verslagen en correctieplannen, verstrekken de financiële entiteit en, waar van toepassing, de externe testers aan de autoriteit een overeenkomstig de leden 9 en 10 opgestelde samenvatting van de relevante bevindingen, de correctieplannen en de documentatie waaruit blijkt dat de TLPT in overeenstemming met de vereisten is verricht.

7. Die autoriteit bezorgt een attest aan de financiële entiteit waarin wordt bevestigd dat de test in overeenstemming met de in de documentatie genoemde vereisten is verricht om de wederzijdse erkenning van dreigingsgestuurde penetratietests tussen bevoegde autoriteiten mogelijk te maken. De financiële entiteit stelt de relevante bevoegde autoriteit in kennis van het attest, de samenvatting van de relevante bevindingen en de correctieplannen.

Onverminderd een dergelijk attest, blijven financiële entiteiten te allen tijde volledig verantwoordelijk voor de gevolgen van de in lid 4 genoemde tests.

8. Financiële entiteiten stellen testers aan om TLPT te verrichten overeenkomstig artikel 27. Wanneer financiële entiteiten interne testers gebruiken om TLPT te verrichten, stellen zij om de drie tests externe testers aan.

Kredietinstellingen die overeenkomstig artikel 6, lid 4, van Verordening (EU) nr. 1024/2013 als belangrijk zijn aangemerkt, zetten alleen externe testers in overeenkomstig artikel 27, lid 1, punten a) tot en met e).

De bevoegde autoriteiten bepalen welke financiële entiteiten de verplichting opgelegd krijgen TLPT te verrichten, rekening houdend met de criteria in artikel 4, lid 2, op basis van een beoordeling van:

a) effectgerelateerde factoren, met name de mate waarin de diensten en de activiteiten van de financiële entiteit effecten hebben op de financiële sector;

b) mogelijke bezorgdheid over financiële stabiliteit, met inbegrip van het systemisch karakter van de financiële entiteit op Unieniveau of op nationaal niveau, indien van toepassing;

c) het specifieke ICT-risicoprofiel, het niveau van maturiteit inzake ICT van de financiële entiteit of de technologische kenmerken in het geding.

9. De lidstaten kunnen één enkele overheidsinstantie in de financiële sector aanwijzen die verantwoordelijk is voor TLPT-gerelateerde aangelegenheden in de financiële sector op nationaal niveau en belasten die instantie daartoe met alle nodige bevoegdheden en taken.

10. Indien een aanwijzing van één enkele overheidsinstantie overeenkomstig lid 9 van dit artikel ontbreekt, en onverminderd haar bevoegdheid te bepalen welke financiële entiteiten de verplichting krijgen opgelegd TLPT te verrichten, kan een bevoegde autoriteit de uitvoering van sommige of al de in dit artikel en artikel 27 genoemde taken aan een andere nationale autoriteit in de financiële sector delegeren.

11. De ETA's ontwikkelen, in overeenstemming met de ECB gemeenschappelijke ontwerpen van technische reguleringsnormen overeenkomstig het Tiber-EU-kader, tot nadere bepaling van:

a) de voor de toepassing van lid 8, tweede alinea, gebruikte criteria;

b) de vereisten en normen inzake het inzetten van interne testers;

c) de vereisten met betrekking tot:

   i) het toepassingsgebied van de in lid 2 bedoelde TLPT;

   ii) de te volgen testmethodologie en -aanpak voor elke specifieke fase van het testproces;

   iii) de resultaten, de afsluitings- en de correctiefase van de tests;

d) het soort samenwerking op het gebied van toezicht evenals andere relevante vormen van samenwerking die noodzakelijk zijn voor de uitvoering van TLPT en ter facilitering van wederzijdse erkenning van die tests, in het geval van financiële entiteiten die in meer dan een lidstaat actief zijn, teneinde een passend niveau van betrokkenheid van toezichthouders en een flexibele uitvoering mogelijk te maken rekening houdend met de specifieke kenmerken van financiële subsectoren of lokale financiële markten.

Bij het ontwikkelen van die ontwerpen van technische reguleringsnormen, houden de ETA's terdege rekening met elk specifiek kenmerk dat voortvloeit uit de specifieke aard van de activiteiten in verschillende financiëledienstensectoren.

De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 juli 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Artikel 27

Vereisten voor testers voor het uitvoeren van TLPT

1. Financiële entiteiten maken voor het uitvoeren van TLPT alleen gebruik van testers die:

a) in de hoogste mate geschikt en deugdelijk zijn;

b) technische en organisatorische capaciteiten bezitten en blijk geven van specifieke deskundigheid op het gebied van inlichtingen over dreigingen, penetratietests en red-teamtests;

c) door een accrediteringsinstantie in een lidstaat zijn gecertificeerd of formele gedragscodes of ethische kaders hebben onderschreven;

d) een onafhankelijke waarborg of een auditverslag verstrekken met betrekking tot het deugdelijk beheer van risico's die verbonden zijn aan de uitvoering van TLPT, met inbegrip van de gepaste bescherming van de vertrouwelijke informatie van de financiële entiteit en herstel voor de bedrijfsrisico's van de financiële entiteit;

e) naar behoren en volledig door de desbetreffende beroepsaansprakelijkheidsverzekeringen zijn gedekt, onder meer tegen het risico van fouten en nalatigheid.

2. Bij het inzetten van interne testers zorgen de financiële entiteiten ervoor dat, naast de vereisten van lid 1, de volgende voorwaarden worden vervuld:

a) dergelijk inzetten van interne testers is goedgekeurd door de relevante bevoegde autoriteit of de overeenkomstig artikel 26, leden 9 en 10, aangewezen enige overheidsinstantie;

b) de relevante bevoegde autoriteit heeft geverifieerd dat de financiële entiteit voldoende middelen heeft ingezet en heeft ervoor gezorgd dat belangenconflicten gedurende de hele ontwerp- en uitvoeringsfase van de test worden voorkomen, en

c) de verstrekker van inlichtingen over dreigingen is extern ten opzichte van de financiële entiteit.

3. Financiële entiteiten zorgen ervoor dat de contracten met externe testers een degelijk beheer van de resultaten van de TLPT opleggen en dat de gegevensverwerking daarvan, met inbegrip van het genereren, opslaan, aggregeren, ontwerpen, rapporteren, communiceren of vernietigen van resultaten, geen risico's voor de financiële entiteit meebrengt.

HOOFDSTUK V

Beheer van ICT-risico van derde aanbieders

Afdeling I

Basisbeginselen voor een degelijk beheer van het ICT-risico van derde aanbieders

Artikel 28

Algemene beginselen

1. Financiële entiteiten beheren het ICT-risico van derde aanbieders als integrerend onderdeel van het ICT-risico binnen hun kader voor ICT-risicobeheer als bedoeld in artikel 6, lid 1, en in overeenstemming met de volgende beginselen:

a) financiële entiteiten die contractuele overeenkomsten voor het gebruik van ICT-diensten voor hun bedrijfsactiviteiten hebben getroffen, blijven te allen tijde volledig verantwoordelijk voor de naleving en de verantwoording van alle verplichtingen uit hoofde van deze verordening en het toepasselijke recht inzake financiële diensten;

b) het beheer van het ICT-risico van derde aanbieders door financiële entiteiten wordt uitgevoerd aan de hand van het evenredigheidsbeginsel, rekening houdend met:

i) de aard, de schaal, de complexiteit en het belang van ICT-gerelateerde afhankelijkheden,

ii) de risico's die voortvloeien uit contractuele overeenkomsten met derde aanbieders inzake het gebruik van ICT-diensten, rekening houdend met het kritieke karakter of het belang van de respectieve diensten, processen of functies en met de potentiële gevolgen voor de continuïteit en de beschikbaarheid van financiële diensten en activiteiten, op individueel en groepsniveau.

2. Als onderdeel van hun kader voor ICT-risicobeheer stellen financiële entiteiten die geen entiteiten zijn in de zin van artikel 16, lid 1, eerste alinea, en geen micro-ondernemingen zijn, een strategie inzake ICT-risico van derde aanbieders vast en herzien zij deze regelmatig, rekening houdend met de in artikel 6, lid 9, bedoelde multi-vendorstrategie, indien van toepassing. De strategie inzake ICT-risico van derde aanbieders omvat een beleid inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen en is van toepassing op individuele basis en, in voorkomend geval, op gesubconsolideerde en geconsolideerde basis. Op basis van een beoordeling van het algehele risicoprofiel van de financiële entiteit en de schaal en complexiteit van de zakelijke diensten, evalueert het leidinggevend orgaan regelmatig de vastgestelde risico's met betrekking tot de contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen.

3. Als onderdeel van hun kader voor ICT-risicobeheer handhaven en actualiseren financiële entiteiten op het niveau van de entiteit en op gesubconsolideerd en geconsolideerd niveau een informatieregister met betrekking tot alle contractuele overeenkomsten over het gebruik van door derde aanbieders verleende ICT-diensten.

De in de eerste alinea bedoelde contractuele overeenkomsten worden naar behoren gedocumenteerd, met een onderscheid tussen die welke van toepassing zijn op ICT-diensten ter ondersteuning van kritieke of belangrijke functies en die welke daarop niet van toepassing zijn.

Financiële entiteiten rapporteren ten minste jaarlijks aan de bevoegde autoriteiten over het aantal nieuwe overeenkomsten inzake het gebruik van ICT-diensten, de categorieën van derde aanbieders van ICT-diensten, het soort contractuele overeenkomsten en de ICT-diensten en -functies die worden geleverd.

Financiële entiteiten stellen de bevoegde autoriteit op verzoek het volledige informatieregister of desgevraagd specifieke onderdelen daarvan ter beschikking, samen met alle informatie die noodzakelijk wordt geacht om doeltreffend toezicht op de financiële entiteit mogelijk te maken.

Financiële entiteiten stellen de bevoegde autoriteit tijdig in kennis van geplande contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen en van het feit dat een functie cruciaal of belangrijk is geworden.

4. Vóór het sluiten van een contractuele overeenkomst inzake het gebruik van ICT-diensten:

a) beoordelen financiële entiteiten of de contractuele overeenkomst betrekking heeft op het gebruik van ICT-diensten die een kritieke of belangrijke functie ondersteunen;

b) beoordelen zij of aan de toezichtvoorwaarden voor het sluiten van het contract is voldaan;

c) identificeren en beoordelen zij alle relevante risico's met betrekking tot de contractuele overeenkomst, met inbegrip van de mogelijkheid dat deze contractuele overeenkomst kan leiden tot een versterking van het ICT-concentratierisico als bedoeld in artikel 29;

d) verrichten zij due-diligenceonderzoeken over toekomstige derde aanbieders van ICT-diensten en waarborgen zij gedurende de gehele selectie- en beoordelingsprocedure dat de derde aanbieder van ICT-diensten geschikt is;

e) identificeren en beoordelen zij belangenconflicten die kunnen voortkomen uit de contractuele overeenkomst.

5. Financiële entiteiten mogen alleen contractuele overeenkomsten sluiten met derde aanbieders van ICT-diensten die voldoen aan passende normen op het gebied van informatiebeveiliging. Wanneer die contractuele overeenkomsten kritieke of belangrijke functies betreffen, letten financiële entiteiten er vóór het sluiten van de overeenkomsten op dat derde aanbieders van ICT-diensten gebruikmaken van de meest actuele en hoogste normen voor informatiebeveiliging.

6. Bij het uitoefenen van toegangs-, inspectie- en auditrechten ten aanzien van de derde aanbieder van ICT-diensten bepalen financiële entiteiten op basis van een risicogebaseerde benadering vooraf de frequentie van de audits en inspecties alsook de te controleren gebieden, door algemeen aanvaarde auditnormen in acht te nemen in overeenstemming met de instructies van de toezichthouder inzake het gebruik en de integratie van deze auditnormen.

Indien met derde aanbieders van ICT-diensten afgesloten contractuele overeenkomsten inzake het gebruik van ICT-diensten een hoog niveau van technische complexiteit inhouden, verifieert de financiële entiteit dat interne of externe auditors, of een pool van auditors, over passende vaardigheden en kennis beschikken om de desbetreffende audits en beoordelingen doeltreffend uit te voeren.

7. Financiële entiteiten zorgen ervoor dat contractuele overeenkomsten inzake het gebruik van ICT-diensten in elk van de volgende omstandigheden kunnen worden beëindigd:

a) bij ernstige overtreding van de toepasselijke wetten, voorschriften of contractuele voorwaarden door de derde aanbieder van ICT-diensten;

b) in omstandigheden die in de loop van de monitoring van het ICT-risico van derde aanbieders worden vastgesteld, waarvan wordt aangenomen dat deze wijzigingen kunnen brengen in de uitvoering van de functies waarin de contractuele overeenkomst voorziet, met inbegrip van materiële wijzigingen die de overeenkomst of de situatie van de derde aanbieder van ICT-diensten nadelig beïnvloeden;

c) bij klaarblijkelijke zwakheden van de derde aanbieder van ICT-diensten in verband met zijn algemeen beheer van het ICT-risico en in het bijzonder met de manier waarop hij zorgt voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van persoonlijke of anderszins gevoelige gegevens of niet-persoonsgebonden gegevens;

d) indien de bevoegde autoriteit niet langer doeltreffend toezicht kan uitoefenen op de financiële entiteit ten gevolge van de voorwaarden van of de omstandigheden in verband met de respectieve contractuele overeenkomst.

8. Voor ICT-diensten die kritieke of belangrijke functies ondersteunen, voeren financiële entiteiten exitstrategieën in. In de exitstrategieën wordt rekening gehouden met risico's die zich op het niveau van derde aanbieders van ICT-diensten kunnen voordoen, met name een mogelijk falen van deze aanbieders, een verslechtering van de kwaliteit van de geleverde ICT-diensten, verstoring van de bedrijfsactiviteiten ten gevolge van ongeschikte of falende dienstverlening van ICT-diensten of materiële risico's in verband met de passende en permanente inzet van de respectieve ICT-dienst, of de beëindiging van contractuele overeenkomsten met derde aanbieders van ICT-diensten onder een van de in lid 7 bedoelde omstandigheden.

Financiële entiteiten zorgen ervoor dat zij de mogelijkheid hebben om contractuele overeenkomsten te beëindigen:

a) zonder verstoring van hun bedrijfsactiviteiten,

b) zonder dat de naleving van de regelgevingsvereisten wordt beperkt,

c) zonder dat afbreuk wordt gedaan aan de continuïteit en de kwaliteit van aan cliënten geleverde diensten.

Exitplannen zijn alomvattend en gedocumenteerd en worden overeenkomstig de in artikel 4, lid 2, genoemde criteria voldoende getest en regelmatig geëvalueerd.

Financiële entiteiten reiken alternatieve oplossingen aan en ontwikkelen overgangsplannen die hen in staat stellen contractueel overeengekomen ICT-diensten en de desbetreffende gegevens van de derde aanbieder van ICT-diensten te verwijderen en deze veilig en integraal over te dragen aan alternatieve aanbieders of deze opnieuw in het eigen bedrijf te integreren.

Financiële entiteiten beschikken over passende noodmaatregelen om de bedrijfscontinuïteit te handhaven indien omstandigheden als bedoeld in de eerste alinea zich voordoen.

9. De ETA's ontwikkelen via het Gemengd Comité ontwerpen van technische uitvoeringsnormen voor de vaststelling van standaardmodellen ten behoeve van het in lid 3 bedoelde informatieregister, waarin informatie wordt opgenomen inzake het gebruik van ICT-diensten die voor alle contractuele overeenkomsten van toepassing is. De ETA's leggen deze ontwerpen van technische uitvoeringsnormen uiterlijk op 17 januari 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid verleend om de in de eerste alinea bedoelde technische uitvoeringsnormen vast te stellen overeenkomstig artikel 15 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

10. De ETA's ontwikkelen via het Gemengd Comité ontwerpen van technische reguleringsnormen tot nadere bepaling van de gedetailleerde inhoud van het in lid 2 bedoelde beleid met betrekking tot de contractuele overeenkomsten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen.

Bij het ontwikkelen van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang en het algehele risicoprofiel van de financiële entiteit en met de aard, schaal en complexiteit van de diensten, activiteiten en verrichtingen ervan. De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 januari 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Artikel 29

Voorlopige beoordeling van het ICT-concentratierisico op het niveau van de entiteit

1. Bij het identificeren en beoordelen van de in artikel 28, lid 4, punt c), bedoelde risico's houden financiële entiteiten eveneens rekening met de vraag of de beoogde sluiting van een contractuele overeenkomst inzake ICT-diensten die kritieke of belangrijke functies ondersteunen, zou leiden tot een van de volgende situaties waarin:

a) zij een contract sluiten met een derde aanbieder van ICT-diensten die niet gemakkelijk substitueerbaar is, of

b) zij beschikken over meerdere contractuele overeenkomsten inzake de verlening van ICT-diensten die kritieke of belangrijke functies ondersteunen, met dezelfde derde aanbieder van ICT-diensten of met nauw verbonden derde aanbieders van ICT-diensten.

Financiële entiteiten wegen de baten en kosten af van alternatieve oplossingen, zoals het gebruik van verschillende derde aanbieders van ICT-diensten, rekening houdend met de vraag of en hoe de voorgenomen oplossingen aansluiten bij de zakelijke behoeften en doelstellingen waarin hun strategie inzake digitale weerbaarheid voorziet.

2. Wanneer de contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen de mogelijkheid inhouden dat een derde aanbieder ICT-diensten die een kritieke of belangrijke functie ondersteunen verder uitbesteedt aan andere derde aanbieders van ICT-diensten, wegen de financiële entiteiten de baten en risico's af die uit een dergelijke uitbesteding kunnen voortkomen, met name in het geval van een in een derde land gevestigde ICT-subcontractant.

Indien contractuele overeenkomsten ICT-diensten betreffen die kritieke of belangrijke functies ondersteunen, houden financiële entiteiten terdege rekening met bepalingen van insolventierecht die in geval van faillissement van de derde aanbieder van ICT-diensten van toepassing zouden zijn alsook met beperkingen die zich met betrekking tot het dringende herstel van de gegevens van de financiële entiteit zouden kunnen voordoen.

Indien contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen met een in een derde land gevestigde derde aanbieder van ICT-diensten worden gesloten, houden financiële entiteiten, bovenop de in de tweede alinea bedoelde overwegingen, ook rekening met de naleving van de gegevensbeschermingsregels van de Unie en de doeltreffende handhaving van de wet in dat derde land.

Indien contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen uitbesteding mogelijk maken, beoordelen financiële entiteiten of en hoe potentieel lange of complexe uitbestedingsketens van invloed kunnen zijn op hun vermogen om de contractueel overeengekomen functies volledig te monitoren en op het vermogen van de bevoegde autoriteit om in dat verband doeltreffend toezicht uit te oefenen op de financiële entiteit.

Artikel 30

Belangrijke contractuele bepalingen

1. De rechten en plichten van de financiële entiteit en van de derde aanbieder van ICT-diensten worden duidelijk toegewezen en schriftelijk vastgesteld. Het volledige contract omvat de overeenkomsten inzake dienstverleningsniveau en wordt opgenomen in één schriftelijk document dat voor de partijen beschikbaar is op papier, of in een document met een ander, downloadbaar, duurzaam en toegankelijk formaat.

2. De contractuele overeenkomsten inzake het gebruik van ICT-diensten bevatten ten minste de volgende elementen:

a) een duidelijke en volledige beschrijving van alle door de derde aanbieder van ICT-diensten te leveren functies en ICT-diensten, met vermelding of het uitbesteden van een ICT-dienst die een kritieke of belangrijke functie ondersteunt, of van materiële onderdelen daarvan, is toegestaan en indien dit het geval is, welke voorwaarden op die uitbesteding van toepassing zijn;

b) de locaties, met name de regio's of landen, waar de contractueel overeengekomen of uitbestede functies en ICT-diensten moeten worden geleverd en waar gegevens moeten worden verwerkt, met inbegrip van de opslaglocatie, en de verplichting voor de derde aanbieder van ICT-diensten om de financiële entiteit vooraf in kennis te stellen indien hij voornemens is van locatie te veranderen;

c) bepalingen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid met betrekking tot de bescherming van gegevens, met inbegrip van persoonsgegevens;

d) bepalingen inzake het waarborgen van de toegang, het herstel en de teruggave in een gemakkelijk toegankelijk formaat van door de financiële entiteit verwerkte persoonsgegevens en niet-persoonsgebonden gegevens in geval van insolventie, afwikkeling of stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten, of in geval van beëindiging van de contractuele overeenkomsten;

e) beschrijvingen van het dienstenniveau, met inbegrip van actualiseringen en herzieningen daarvan;

f) de verplichting van de derde aanbieder van ICT-diensten om de financiële entiteit zonder extra kosten, of tegen een vooraf bepaalde kostprijs, bijstand te verlenen wanneer zich een incident voordoet dat verband houdt met de aan de financiële entiteit geleverde ICT-dienst;

g) de verplichting van de derde aanbieder van ICT-diensten om volledige medewerking te verlenen aan de bevoegde autoriteiten en de afwikkelingsautoriteiten van de financiële entiteit, met inbegrip van de door hen aangestelde personen;

h) beëindigingsrechten en de bijbehorende minimumopzegtermijnen voor de beëindiging van de contractuele overeenkomsten, in overeenstemming met de verwachtingen van de bevoegde autoriteiten en de afwikkelingsautoriteiten;

i) de voorwaarden voor deelname van derde aanbieders van ICT-diensten aan bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid van de financiële entiteiten, overeenkomstig artikel 13, lid 6.

3. De contractuele overeenkomsten inzake het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen, omvatten, bovenop de in lid 2 genoemde elementen, ten minste het volgende:

a) beschrijvingen van het niveau van volledige dienstverlening, met inbegrip van actualiseringen en herzieningen daarvan met nauwkeurige kwantitatieve en kwalitatieve prestatiedoelstellingen binnen de overeengekomen dienstverleningsniveaus, teneinde de financiële entiteit in staat te stellen een doeltreffende monitoring van de ICT-diensten te verrichten en onverwijld passende corrigerende maatregelen te nemen wanneer de overeengekomen dienstverleningsniveaus niet worden gehaald;

b) kennisgevingstermijnen en rapportageverplichtingen van de derde aanbieder van ICT-diensten ten aanzien van de financiële entiteit, met inbegrip van de kennisgeving van ontwikkelingen die materiële gevolgen kunnen hebben voor het vermogen van de derde aanbieder om op doeltreffende wijze de ICT-diensten die kritieke of belangrijke functies ondersteunen te leveren in overeenstemming met de afgesproken dienstverleningsniveaus;

c) verplichtingen voor de derde aanbieder van ICT-diensten om bedrijfsnoodplannen in te voeren en te testen en te beschikken over ICT-beveiligingsmaatregelen, -instrumenten en -beleidslijnen waarmee de financiële entiteit kan zorgen voor een passend niveau van veiligheid bij het verlenen van diensten in overeenstemming met haar regelgevingskader;

d) de verplichting voor de derde aanbieder van ICT-diensten om deel te nemen aan en volledig mee te werken bij de TLPT van de financiële entiteit als bedoeld in de artikelen 26 en 27;

e) het recht om de prestaties van de derde aanbieder van ICT-diensten permanent te monitoren, hetgeen het volgende inhoudt:

i) onbeperkte rechten van toegang, inspectie en audit door de financiële entiteit of een daartoe aangestelde derde partij alsook door de bevoegde autoriteit, en het recht om ter plaatse kopieën van relevante documenten te maken indien deze cruciaal zijn voor de activiteiten van de derde aanbieder van ICT-diensten, waarbij de doeltreffende uitoefening van dit recht niet wordt belemmerd of beperkt door andere contractuele overeenkomsten of ander uitvoeringsbeleid;

ii) het recht om andere garantieniveaus overeen te komen indien de rechten van andere cliënten worden aangetast;

iii) de verplichting van de derde aanbieder van ICT-diensten om tijdens de door de bevoegde autoriteiten, de lead overseer, de financiële entiteit of een aangestelde derde partij ter plaatse uitgevoerde inspecties en audits volledig mee te werken, en

iv) de verplichting om bijzonderheden te verschaffen over het toepassingsgebied, te volgen procedures en de frequentie van dergelijke inspecties en audits;

f) exitstrategieën, met name de invoering van een verplichte passende overgangsperiode:

i) waarin de derde aanbieder van ICT-diensten de levering van de respectieve functies of ICT-diensten zal blijven voortzetten, teneinde het risico op verstoring bij de financiële entiteit te beperken of voor een doeltreffende afwikkeling en herstructurering te zorgen;

ii) waarin de financiële entiteit kan overstappen naar een andere derde aanbieder van ICT-diensten of naar interne oplossingen in overeenstemming met de complexiteit van de geleverde dienst.

In afwijking van punt e) kunnen de derde aanbieder van ICT-diensten en de financiële entiteit die een micro-onderneming is, overeenkomen dat de rechten van toegang, inspectie en audit van de financiële entiteit mogen worden gedelegeerd aan een onafhankelijke derde partij die wordt aangesteld door de derde aanbieder van ICT-diensten, en dat de financiële entiteit de derde partij te allen tijde om informatie en garanties kan verzoeken met betrekking tot de prestaties van de derde aanbieder van ICT-diensten.

4. Bij onderhandelingen over contractuele overeenkomsten houden financiële entiteiten en derde aanbieders van ICT-diensten rekening met het gebruik van modelcontractbepalingen die door overheidsinstanties zijn ontwikkeld voor specifieke diensten.

5. De ETA's stellen via het Gemengd Comité ontwerpen van technische reguleringsnormen op tot nadere bepaling van de in lid 2, punt a), genoemde elementen die een financiële entiteit nodig heeft om te kunnen bepalen en te beoordelen wanneer over te gaan tot uitbesteding van ICT-diensten die kritieke of belangrijke functies ondersteunen.

Bij het opstellen van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang en het algehele risicoprofiel van de financiële entiteit, en met de aard, schaal en complexiteit van de diensten, activiteiten en verrichtingen ervan.

De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 juli 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in de eerste alinea bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Afdeling II

Oversightkader voor kritieke derde aanbieders van ICT-diensten

Artikel 31

Aanwijzing van kritieke derde aanbieders van ICT-diensten

1. De ETA's zorgen via het Gemengd Comité en op aanbeveling van het overeenkomstig artikel 32, lid 1, opgerichte oversightforum voor het volgende:

a) zij wijzen de derde aanbieders van ICT-diensten aan die cruciaal zijn voor financiële entiteiten, na een beoordeling die rekening houdt met de in lid 2 gespecificeerde criteria;

b) zij stellen voor iedere kritieke derde aanbieder van ICT-diensten als lead overseer de ETA aan die overeenkomstig Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 of (EU) nr. 1095/2010 verantwoordelijk is voor de financiële entiteiten die samen over het grootste aandeel van de totale activa beschikken ten opzichte van de waarde van de totale activa van alle financiële entiteiten die gebruikmaken van de diensten van de betrokken kritieke derde aanbieder van ICT-diensten, zoals resulteert uit de som van de individuele balansen van die financiële entiteiten.

2. De in lid 1, punt a), bedoelde aanwijzing is gebaseerd op alle volgende criteria met betrekking tot door de derde aanbieder van ICT-diensten geleverde ICT-diensten:

a) de systemische effecten op de stabiliteit, continuïteit of kwaliteit van de verlening van financiële diensten ingeval de betrokken derde aanbieder van ICT-diensten te maken zou krijgen met een grootschalige operationele verstoring van de dienstverlening, rekening houdend met het aantal financiële entiteiten en de totale waarde van de activa van de financiële entiteiten waaraan de betrokken derde aanbieder ICT-diensten verleent;

b) het systemische karakter of belang van de financiële entiteiten die afhankelijk zijn van de betrokken derde aanbieder van ICT-diensten, dat wordt beoordeeld aan de hand van de volgende criteria:

   i) het aantal mondiaal systeemrelevante instellingen (MSI's) of andere systeemrelevante instellingen (ASI's) die afhankelijk zijn van de respectieve derde aanbieder van ICT-diensten;

   ii) de onderlinge afhankelijkheid tussen de MSI's of ASI's als bedoeld in punt i) en andere financiële entiteiten, met inbegrip van situaties waarin de MSI's of ASI's diensten op het gebied van financiële infrastructuur verlenen aan andere financiële entiteiten;

c) de afhankelijkheid van financiële entiteiten ten aanzien van de diensten die door de betrokken derde aanbieder van ICT-diensten worden verleend met betrekking tot kritieke of belangrijke functies van financiële entiteiten waarbij uiteindelijk dezelfde derde aanbieder van ICT-diensten betrokken is, ongeacht of financiële entiteiten direct of indirect via uitbestedingsregelingen van die diensten afhankelijk zijn;

d) de graad van substitueerbaarheid van de derde aanbieder van ICT-diensten, rekening houdend met de volgende parameters:

   i) het ontbreken van reële, zelfs gedeeltelijke, alternatieven als gevolg van het beperkte aantal derde aanbieders van ICT-diensten die actief zijn op een specifieke markt, of het marktaandeel van de betrokken derde aanbieder van ICT-diensten, of de technische complexiteit of geavanceerdheid die in het geding is, onder meer met betrekking tot eigendomstechnologie, of de specifieke kenmerken van de organisatie of activiteit van de derde aanbieder van ICT-diensten;

   ii) moeilijkheden in verband met het geheel of gedeeltelijk migreren van de relevante gegevens en werklast van de desbetreffende derde aanbieder van ICT-diensten naar een andere derde aanbieder van ICT-diensten, hetzij ten gevolge van hoge financiële kosten, de tijd of andere middelen die het migratieproces kan meebrengen, of een hoger ICT-risico of andere operationele risico's waaraan de financiële entiteit kan worden blootgesteld door een dergelijke migratie.

3. Indien de derde aanbieder van ICT-diensten tot een groep behoort, wordt met de in lid 2 bedoelde criteria rekening gehouden met betrekking tot de ICT-diensten die door de groep als geheel worden verleend.

4. Kritieke derde aanbieders van ICT-diensten die deel uitmaken van een groep wijzen één rechtspersoon als coördinatiepunt aan teneinde passende vertegenwoordiging en communicatie met de lead overseer te waarborgen.

5. De lead overseer stelt de derde aanbieder van ICT-diensten in kennis van het resultaat van de beoordeling die tot de in lid 1, punt a), bedoelde aanwijzing heeft geleid. Binnen zes weken na datum van de kennisgeving kan de derde aanbieder van ICT-diensten bij de lead overseer een met redenen omklede verklaring met relevante informatie ten behoeve van de beoordeling indienen. De lead overseer neemt de met redenen omklede verklaring in overweging en kan binnen 30 kalenderdagen na de ontvangst van dergelijke verklaring om aanvullende informatie verzoeken.

Nadat een derde aanbieder van ICT-diensten als cruciaal is aangewezen, stellen de ETA's de derde aanbieder van ICT-diensten via het Gemengd Comité in kennis van die aanwijzing alsook van de aanvangsdatum vanaf wanneer zij daadwerkelijk aan oversightactiviteiten zullen worden onderworpen. De aanvangsdatum valt niet later dan één maand na de kennisgeving. De derde aanbieder van ICT-diensten stelt de financiële entiteiten waaraan hij diensten verleent in kennis van zijn aanwijzing als cruciaal.

6. De Commissie is bevoegd om overeenkomstig artikel 57 een gedelegeerde handeling in aanvulling op deze verordening vast te stellen waarin de in lid 2 van dit artikel genoemde criteria verder worden gespecificeerd, en dit uiterlijk op 17 juli 2024.

7. De in lid 1, punt a), bedoelde aanwijzing wordt niet gebruikt totdat de Commissie een gedelegeerde handeling overeenkomstig lid 6 heeft vastgesteld.

8. De in lid 1, punt a), bedoelde aanwijzing is niet van toepassing op:

i) financiële entiteiten die ICT-diensten verlenen aan andere financiële entiteiten;

ii) derde aanbieders van ICT-diensten die onderworpen zijn aan oversightkaders die zijn vastgesteld ter ondersteuning van de in artikel 127, lid 2, van het Verdrag betreffende de werking van de Europese Unie bedoelde taken;

iii) aanbieders van ICT-diensten binnen een groep;

iv) derde aanbieders van ICT-diensten die uitsluitend in één lidstaat ICT-diensten verlenen aan financiële entiteiten die alleen in die lidstaat actief zijn.

9. Jaarlijks stellen de ETA's via het Gemengd Comité de lijst op van kritieke derde aanbieders van ICT-diensten op het niveau van de Unie, en publiceren en actualiseren zij deze lijst.

10. Voor de toepassing van lid 1, punt a), zenden de bevoegde autoriteiten de in artikel 28, lid 3, derde alinea, bedoelde verslagen jaarlijks en op geaggregeerde basis toe aan het overeenkomstig artikel 32 opgerichte toezichtforum. Het oversightforum beoordeelt de afhankelijkheden van financiële entiteiten ten aanzien van derde aanbieders van ICT-diensten op basis van de informatie die het van de bevoegde autoriteiten ontvangt.

11. De derde aanbieders van ICT-diensten die niet in de lid 9 bedoelde lijst zijn opgenomen, kunnen verzoeken om als cruciaal te worden aangewezen, overeenkomstig lid 1, punt a).

Voor de toepassing van de eerste alinea dient de derde aanbieder van ICT-diensten een met redenen omkleed verzoek in bij de EBA, de ESMA of de Eiopa, die via het Gemengd Comité besluit die derde aanbieder van ICT-diensten al dan niet als cruciaal aan te wijzen, overeenkomstig lid 1, punt a).

Het in de tweede alinea bedoelde besluit wordt binnen zes maanden na ontvangst van het verzoek vastgesteld en ter kennis gebracht van de derde aanbieder van ICT-diensten.

12. Financiële entiteiten maken alleen gebruik van de diensten van een in een derde land gevestigde derde aanbieder van ICT-diensten die overeenkomstig lid 1, punt a), als cruciaal is aangewezen indien deze laatste binnen de twaalf maanden na de aanwijzing een dochteronderneming in de Unie heeft gevestigd.

13. De in lid 12 bedoelde kritieke derde aanbieder van ICT-diensten stelt de lead overseer in kennis van alle wijzigingen in de beheersstructuur van de in de Unie gevestigde dochteronderneming.

Artikel 32

Structuur van het oversightkader

1. Het Gemengd Comité richt overeenkomstig artikel 57, lid 1, van Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 het oversightforum op als subcomité ter ondersteuning van de werkzaamheden van het Gemengd Comité en van de lead overseer als bedoeld in artikel 31, lid 1, punt b), op het gebied van ICT-risico van derde aanbieders in alle financiële sectoren. Het oversightforum stelt de ontwerpen van gemeenschappelijke standpunten en de ontwerpen van gemeenschappelijke handelingen van het Gemengd Comité op dat gebied op.

Het oversightforum bespreekt regelmatig relevante ontwikkelingen inzake ICT-risico en -kwetsbaarheden en bevordert een consistente aanpak bij de monitoring van het ICT-risico van derde aanbieders op Unieniveau.

2. Het oversightforum verricht jaarlijks een collectieve beoordeling van de resultaten en bevindingen van de oversightactiviteiten voor alle kritieke derde aanbieders van ICT-diensten en bevordert coördinatiemaatregelen om de digitale operationele weerbaarheid van financiële entiteiten te vergroten, beste praktijken voor de aanpak van het ICT-concentratierisico aan te moedigen en limiterende instrumenten voor sectoroverschrijdende risico-overdrachten te onderzoeken.

3. Het oversightforum dient alomvattende benchmarks voor kritieke derde aanbieders van ICT-diensten in die door het Gemengd Comité als gemeenschappelijke standpunten van de ETA's worden vastgesteld in overeenstemming met artikel 56, lid 1, van Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

4. Het oversightforum is samengesteld uit:

a) de voorzitters van de ETA's;

b) één vertegenwoordiger op hoog niveau van het huidige personeel van de in artikel 46 bedoelde bevoegde autoriteit van elke lidstaat;

c) de uitvoerend directeur van elke ETA en één vertegenwoordiger van de Commissie, het ESRB, de ECB en Enisa als waarnemers;

d) waar passend, één extra vertegenwoordiger van een in artikel 46 bedoelde bevoegde autoriteit van elke lidstaat als waarnemer;

e) indien van toepassing, één vertegenwoordiger van de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten die verantwoordelijk zijn voor het toezicht op een essentiële of belangrijke entiteit die onder die richtlijn valt en die is aangewezen als kritieke derde aanbieder van ICT-diensten, als waarnemer.

Het oversightforum kan in voorkomend geval het advies inwinnen van overeenkomstig lid 6 aangestelde onafhankelijke deskundigen.

5. Elke lidstaat wijst de bevoegde autoriteit aan waarvan een personeelslid de in lid 4, eerste alinea, punt b), bedoelde vertegenwoordiger op hoog niveau zal zijn, en stelt de lead overseer daarvan in kennis.

De ETA's publiceren de lijst van door de lidstaten aangewezen vertegenwoordigers op hoog niveau uit het personeel op dat moment van de desbetreffende bevoegde autoriteit op hun website.

6. De in lid 4, tweede alinea, bedoelde onafhankelijke deskundigen worden door het oversightforum aangesteld uit een groep deskundigen die op basis van een openbare en transparante sollicitatieprocedure zijn geselecteerd.

De onafhankelijke deskundigen worden aangesteld op basis van hun deskundigheid op het gebied van financiële stabiliteit, digitale operationele weerbaarheid en ICT-beveiliging. Zij handelen onafhankelijk, objectief en uitsluitend in het belang van de Unie als geheel, en vragen noch aanvaarden instructies van instellingen of organen van de Unie, van de regering van een lidstaat of van andere publieke of particuliere organen.

7. Overeenkomstig artikel 16 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 vaardigen de ETA's voor de toepassing van deze afdeling uiterlijk op 17 juli 2024 richtsnoeren uit betreffende de samenwerking tussen de ETA's en de bevoegde autoriteiten betreffende de nadere procedures en voorwaarden voor de toewijzing en uitvoering van taken tussen de bevoegde autoriteiten en de ETA's alsook de details over de uitwisseling van informatie die de bevoegde autoriteiten nodig hebben om de follow-up van aanbevelingen krachtens artikel 35, lid 1, punt d), aan het adres van de kritieke derde aanbieders van ICT-diensten, te waarborgen.

8. De in deze afdeling gestelde vereisten doen geen afbreuk aan de toepassing van Richtlijn (EU) 2022/2555 en van andere Unieregels inzake toezicht die van toepassing zijn op aanbieders van cloudcomputingdiensten.

9. De ETA's dienen, via het Gemengd Comité en op basis van de voorbereidende werkzaamheden van het oversightforum jaarlijks een verslag in bij het Europees Parlement, de Raad en de Commissie over de toepassing van deze afdeling.

Artikel 33

Taken van de lead overseer

1. De overeenkomstig artikel 31, lid 1, punt b), aangestelde lead overseer oefent het oversight uit over de aangewezen kritieke derde aanbieders van ICT-diensten en is voor alle aan het oversight gerelateerde aangelegenheden het eerste contactpunt voor die kritieke derde aanbieders van ICT-diensten.

2. Voor de toepassing van lid 1, beoordeelt de lead overseer of elke kritieke derde aanbieder van ICT-diensten over uitgebreide, deugdelijke en doeltreffende regels, procedures, mechanismen en regelingen beschikt voor het beheer van het ICT-risico dat hij voor financiële entiteiten kan inhouden.

De in de eerste alinea bedoelde beoordeling is voornamelijk gericht op ICT-diensten verleend door de kritieke derde aanbieder van ICT-diensten die kritieke of belangrijke functies of financiële entiteiten ondersteunt. Waar dat nodig is om alle relevante risico's aan te pakken, wordt de beoordeling uitgebreid tot ICT-diensten die andere functies dan de kritieke of de belangrijke functies ondersteunen.

3. De in lid 2 bedoelde beoordeling heeft betrekking op:

a) ICT-voorschriften om met name de veiligheid, beschikbaarheid, continuïteit, schaalbaarheid en kwaliteit van diensten die de kritieke derde aanbieder van ICT-diensten aan financiële entiteiten verleent, te garanderen alsook het vermogen om te allen tijde hoge normen inzake beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens te handhaven;

b) de fysieke beveiliging die tot de ICT-beveiliging bijdraagt, inclusief de beveiliging van gebouwen, faciliteiten en datacentra;

c) de processen inzake risicobeheer, met inbegrip van het beleid inzake ICT-risicobeheer, het ICT-bedrijfscontinuïteitsbeleid en de ICT-respons- en herstelplannen;

d) de governanceregelingen, met inbegrip van een organisatiestructuur met duidelijke, transparante en consistente regels inzake taakverdeling en verantwoording die doeltreffend ICT-risicobeheer mogelijk maken;

e) de opsporing, monitoring en snelle rapportage van materiële ICT-gerelateerde incidenten aan financiële entiteiten, het beheer en de oplossing van die incidenten, met name cyberaanvallen;

f) de mechanismen voor overdracht van gegevens en applicaties en interoperabiliteit, die een doeltreffende uitoefening van het beëindigingsrecht door de financiële entiteiten verzekeren;

g) het testen van ICT-systemen, -infrastructuur en -controles;

h) de ICT-audits;

i) het gebruik van relevante nationale en internationale normen die van toepassing zijn op het verlenen van ICT-diensten aan de financiële entiteiten.

4. Op basis van de in lid 2 bedoelde beoordeling en in overleg met het in artikel 34, lid 1, bedoelde gezamenlijk oversightnetwerk (JON) stelt de lead overseer een duidelijk, gedetailleerd en met redenen omkleed individueel oversightplan op met de jaarlijkse oversightdoelstellingen en de belangrijkste geplande oversightacties voor elke kritieke derde aanbieder van ICT-diensten. Dat plan wordt jaarlijks aan de kritieke derde aanbieder van ICT-diensten meegedeeld.

Voorafgaand aan de vaststelling van het oversightplan door de lead overseer, wordt het ontwerp van dat oversightplan aan de kritieke derde aanbieder van ICT-diensten meegedeeld.

Na ontvangst van het ontwerp van het oversightplan, kan de kritieke derde aanbieder van ICT-diensten binnen 15 kalenderdagen een met redenen omklede verklaring indienen met de verwachte gevolgen voor klanten die entiteiten zijn die buiten het toepassingsgebied van deze verordening vallen, en waar passend oplossingen formuleren om risico's te mitigeren.

5. Zodra de in lid 4 bedoelde jaarlijkse oversightplannen zijn vastgesteld en aan de kritieke derde aanbieder van ICT-diensten zijn meegedeeld, kunnen de bevoegde autoriteiten maatregelen met betrekking tot deze kritieke derde aanbieders van ICT-diensten alleen nemen in overeenstemming met de lead overseer.

Artikel 34

Operationele coördinatie tussen de lead overseers

1. Teneinde een consistente aanpak van oversightactiviteiten te waarborgen en gecoördineerde algemene oversightstrategieën en samenhangende operationele benaderingen en werkmethoden mogelijk te maken, zetten de drie overeenkomstig artikel 31, lid 1, punt b), aangestelde lead overseers een JON op om onderling te overleggen tijdens de voorbereidende fasen en om de uitvoering te coördineren van oversightactiviteiten ten aanzien van de respectieve kritieke derde aanbieders van ICT-diensten waarop zij toezien, alsook gedurende elke activiteit die overeenkomstig artikel 42 noodzakelijk kan zijn.

2. Voor de toepassing van lid 1 stellen de lead overseers een gemeenschappelijk oversightprotocol op met gedetailleerde procedures voor de dagelijkse coördinatie en waarmee snelle uitwisselingen en reacties gewaarborgd kunnen worden. Het protocol zal op gezette tijden herzien worden om tegemoet te komen aan de operationele behoeften, met name de ontwikkeling van praktische oversightregelingen.

3. De lead overseers kunnen op ad-hocbasis een beroep doen op de ECB en Enisa voor technisch advies, praktijkervaring delen of deelnemen aan specifieke coördinatievergaderingen van het JON.

Artikel 35

Bevoegdheden van de lead overseer

1. Voor de uitvoering van de in deze afdeling omschreven taken beschikt de lead overseer ten aanzien van de kritieke derde aanbieders van ICT-diensten over de bevoegdheid om:

a) alle relevante informatie en documentatie overeenkomstig artikel 37 op te vragen;

b) algemene onderzoeken en inspecties te verrichten overeenkomstig respectievelijk de artikelen 38 en 39;

c) na afloop van de oversightactiviteiten te verzoeken om verslagen met vermelding van de ondernomen acties of de corrigerende maatregelen die door de kritieke derde aanbieders van ICT-diensten zijn genomen met betrekking tot de in punt d) bedoelde aanbevelingen;

d) aanbevelingen uit te vaardigen met betrekking tot de in artikel 33, lid 3, bedoelde gebieden, met name over:

   i) het gebruik van specifieke ICT-beveiligings- en kwaliteitsvereisten of -processen, met name met betrekking tot de uitrol van patches, updates, encryptie en andere beveiligingsmaatregelen die de lead overseer relevant acht om de ICT-beveiliging van diensten voor financiële entiteiten te waarborgen;

   ii) het gebruik van voorwaarden, met inbegrip van de technische uitvoering ervan, voor het verlenen van ICT-diensten aan financiële entiteiten door derde aanbieders van ICT-diensten, die de lead overseer relevant acht om het ontstaan van zwakke punten ("single points of failure"), de uitbreiding daarvan te voorkomen, of om mogelijke systemische effecten in de hele financiële sector van de Unie te beperken in geval van ICT-concentratierisico;

   iii) geplande uitbestedingen waarbij de lead overseer van oordeel is dat verdere uitbesteding — inclusief uitbestedingsregelingen die de kritieke derde aanbieders van ICT-diensten voornemens zijn te treffen met derde aanbieders van ICT-diensten of met in een derde land gevestigde ICT-subcontractanten — risico's voor de levering van diensten door de financiële entiteit of risico's voor de financiële stabiliteit met zich mee kan brengen, op basis van onderzoek van de overeenkomstig de artikelen 37 en 38 verzamelde informatie;

   iv) het stopzetten van verdere uitbestedingsregelingen, wanneer aan de volgende cumulatieve voorwaarden is voldaan:

      — de beoogde subcontractant is een in een derde land gevestigde derde aanbieder van ICT-diensten of een in een derde land gevestigde ICT-subcontractant;

      — de uitbesteding heeft betrekking op kritieke of belangrijke functies van de financiële entiteit, en

— de lead overseer is van oordeel dat dit soort uitbesteding een duidelijk en ernstig risico vormt voor de financiële stabiliteit van de Unie of voor financiële entiteiten, inclusief voor het vermogen van financiële entiteiten om aan toezichtvereisten te voldoen.

Voor de toepassing van punt iv) van dit punt zenden derde aanbieders van ICT-diensten de informatie inzake uitbesteding aan de lead overseer toe, en gebruiken daarbij het in artikel 41, lid 1, punt b), bedoelde model.

2. Wanneer de lead overseer de in dit artikel bedoelde bevoegdheden uitoefent:

a) zorgt hij voor regelmatige coördinatie binnen het JON, en met name consistente benaderingen, voor zover nodig, met betrekking tot het oversight van kritieke derde aanbieders van ICT-diensten;

b) houdt hij terdege rekening met het bij Richtlijn (EU) 2022/2555 vastgestelde kader en raadpleegt indien nodig de relevante bevoegde autoriteiten die overeenkomstig die richtlijn zijn aangewezen of ingesteld, om overlappingen te voorkomen van technische en organisatorische maatregelen die op grond van die richtlijn van toepassing kunnen zijn op kritieke derde aanbieders van ICT-diensten;

c) beperkt hij zo veel mogelijk het risico van verstoring van diensten die kritieke derde aanbieders van ICT-diensten verlenen aan klanten die entiteiten zijn die buiten het toepassingsgebied van deze verordening vallen.

3. De lead overseer overlegt met het oversightforum vooraleer hij de in lid 1 bedoelde bevoegdheden uitoefent.

Alvorens aanbevelingen uit te vaardigen overeenkomstig lid 1, punt d), stelt de lead overseer de derde aanbieder van ICT-diensten in de gelegenheid om binnen 30 kalenderdagen relevante informatie te verstrekken waaruit de verwachte gevolgen blijken voor klanten die entiteiten zijn die buiten het toepassingsgebied van deze verordening vallen en formuleren daarbij, voor zover van toepassing, oplossingen om de risico's te mitigeren.

4. De lead overseer stelt het JON in kennis van het resultaat van de uitoefening van de in lid 1, punten a) en b), bedoelde bevoegdheden. De lead overseer zendt de in lid 1, punt c), bedoelde verslagen onverwijld toe aan het JON en aan de bevoegde autoriteiten van de financiële entiteiten die gebruikmaken van de ICT-diensten van die kritieke derde aanbieder van ICT-diensten.

5. Kritieke derde aanbieders van ICT-diensten werken te goeder trouw samen met de lead overseer en ondersteunen hem bij de uitvoering van zijn taken.

6. In geval van gehele of gedeeltelijke niet-naleving van de krachtens de uitoefening van de bevoegdheden uit hoofde van lid 1, punten a), b) en c), te nemen maatregelen, en na het verstrijken van een termijn van ten minste 30 kalenderdagen vanaf de datum waarop de kritieke derde aanbieder van ICT-diensten een kennisgeving van de respectieve maatregelen heeft ontvangen, neemt de lead overseer een besluit aan waarmee een dwangsom wordt opgelegd om de kritieke derde aanbieder van ICT-diensten tot nakoming van die maatregelen te dwingen.

7. De in lid 6 bedoelde dwangsom wordt dagelijks opgelegd tot aan de verplichtingen is voldaan, gedurende een termijn van ten hoogste zes maanden volgend op de kennisgeving van het besluit een dwangsom op te leggen aan de kritieke derde aanbieder van ICT-diensten.

8. Het bedrag van de dwangsom, berekend vanaf de datum die is vastgesteld in het besluit tot oplegging van de dwangsom, bedraagt maximaal 1 % van de wereldwijde gemiddelde dagomzet van de kritieke derde aanbieder van ICT-diensten in het voorafgaande boekjaar. De lead overseer houdt bij de vaststelling van het bedrag van de dwangsom rekening met de volgende criteria inzake niet-naleving van de in lid 6 bedoelde maatregelen:

a) de ernst en de duur van niet-naleving;

b) de vraag of niet-naleving opzettelijk dan wel uit onachtzaamheid is gepleegd;

c) de mate van medewerking van de derde aanbieder van ICT-diensten met de lead overseer.

Voor de toepassing van de eerste alinea, en met het oog op een consistente benadering, overlegt de lead overseer binnen het JON.

9. Dwangsommen hebben een administratief karakter en zijn afdwingbaar. De tenuitvoerlegging geschiedt volgens de bepalingen van burgerlijk procesrecht die van kracht zijn in de lidstaat op het grondgebied waar de inspecties worden verricht en de toegang wordt gevraagd. Klachten over de regelmatigheid van de tenuitvoerlegging behoren tot de bevoegdheid van de rechterlijke instanties van de betrokken lidstaat. De bedragen van dwangsommen worden toegewezen aan de algemene begroting van de Europese Unie.

10. De lead overseer maakt alle opgelegde dwangsommen openbaar, tenzij die openbaarmaking de financiële markten ernstig in gevaar zou brengen of onevenredige schade zou toebrengen aan de betrokken partijen.

11. Alvorens een dwangsom op grond van lid 6 op te leggen, stelt de lead overseer de vertegenwoordigers van de kritieke derde aanbieder van ICT-diensten die aan de procedure is onderworpen, in de gelegenheid te worden gehoord over de bevindingen, en hij baseert zijn besluiten uitsluitend op bevindingen waarover de aan de procedure onderworpen kritieke derde aanbieder van ICT-diensten opmerkingen heeft kunnen maken.

Het recht van verweer van de aan de procedure onderworpen personen wordt tijdens de procedure ten volle geëerbiedigd. De kritieke derde aanbieder van ICT-diensten die aan de procedure is onderworpen, is gerechtigd toegang te krijgen tot het dossier, onder voorbehoud van het rechtmatige belang van andere personen bij de bescherming van hun zakengeheimen. Het recht van toegang tot het dossier is niet van toepassing op vertrouwelijke informatie of op interne voorbereidende documenten van de lead overseer.

Artikel 36

Uitoefening van de bevoegdheden van de lead overseer buiten de Unie

1. Wanneer de oversightdoelstellingen niet kunnen worden bereikt via interactie met de voor de toepassing van artikel 31, lid 12, opgerichte dochteronderneming, of via oversightactiviteiten in bedrijfsruimten die zich in de Unie bevinden, kan de lead overseer de in de volgende bepalingen bedoelde bevoegdheden uitoefenen in alle bedrijfsruimten in een derde land die eigendom zijn van, of gebruikt worden door een kritieke derde aanbieder van ICT-diensten bij het verlenen van diensten aan financiële entiteiten in de Unie, in verband met de bedrijfsactiviteiten, functies of diensten — inclusief administratieve, commerciële of operationele kantoren, bedrijfsruimten, gronden, gebouwen of andere eigendommen:

a) in artikel 35, lid 1, punt a), en

b) in artikel 35, lid 1, punt b), overeenkomstig artikel 38, lid 2, punten a), b), en d), en in artikel 39, lid 1, en lid 2, punt a).

De uitoefening van de in de eerste alinea bedoelde bevoegdheden is onderworpen aan alle volgende voorwaarden:

i) de lead overseer is van mening dat een inspectie in een derde land noodzakelijk is om hem in staat te stellen zijn taken uit hoofde van deze verordening volledig en doeltreffend uit te voeren;

ii) de inspectie in een derde land houdt rechtstreeks verband met het verlenen van ICT-diensten aan financiële entiteiten in de Unie;

iii) de betrokken kritieke derde aanbieder van ICT-diensten stemt in met het uitvoeren van een inspectie in een derde land, en

iv) de betrokken autoriteit van het derde land is door de lead overseer officieel in kennis gesteld en heeft geen bezwaar gemaakt.

2. Onverminderd de respectieve bevoegdheden van de instellingen van de Unie en van de lidstaten, sluiten de EBA, de ESMA of de Eiopa voor de toepassing van lid 1 regelingen voor administratieve samenwerking met de betrokken autoriteit van het derde land teneinde de inspecties in het betrokken derde land door de lead overseer en zijn voor die missie in dat derde land aangewezen team, vlot te laten verlopen. Deze samenwerkingsregelingen scheppen geen wettelijke verplichtingen voor de Unie en haar lidstaten en beletten de lidstaten en hun bevoegde autoriteiten niet om bilaterale of multilaterale regelingen met die derde landen en hun betrokken autoriteiten te sluiten.

In die samenwerkingsregelingen worden ten minste de volgende elementen gespecificeerd:

a) de procedures voor de coördinatie van uit hoofde van deze verordening uitgevoerde oversightactiviteiten en elke overeenkomstige door de betrokken autoriteit van het derde land in kwestie uitgevoerde monitoring van het ICT-risico van derde aanbieders in de financiële sector, met inbegrip van details over het toezenden door de lead overseer en zijn team, van de toestemming van de betrokken autoriteit van het derde land in kwestie om algemene onderzoeken en inspecties ter plaatse uit te voeren, zoals bedoeld in lid 1, eerste alinea, op het grondgebied dat onder de jurisdictie van de betrokken autoriteit van het derde land valt;

b) het mechanisme voor het doorgeven van relevante informatie tussen de EBA, de ESMA of de Eiopa, en de betrokken autoriteit van het derde land in kwestie, met name in verband met informatie waar de lead overseer uit hoofde van artikel 37 om kan verzoeken;

c) de mechanismen voor snelle kennisgeving door de betrokken autoriteit van het derde land in kwestie aan de EBA, de ESMA of de Eiopa, van gevallen waarbij vermoed wordt dat een in een derde land gevestigde derde aanbieder van ICT-diensten die overeenkomstig artikel 31, lid 1, punt a), als cruciaal is aangewezen, de vereisten heeft overtreden die hij krachtens het toepasselijke recht van het derde land in kwestie moet naleven bij het verlenen van diensten aan financiële instellingen in dat derde land, evenals de toegepaste rechtsmiddelen en sancties;

d) het regelmatig doorgeven van updates over ontwikkelingen op het gebied van regelgeving en toezicht inzake de monitoring van het ICT-risico van derde aanbieders van financiële instellingen in het derde land in kwestie;

e) de details om indien nodig de deelname van een vertegenwoordiger van de betrokken autoriteit van het derde land aan de door de lead overseer en het aangewezen team uitgevoerde inspecties, mogelijk te maken.

3. Wanneer de lead overseer niet in staat is om buiten de Unie oversightactiviteiten zoals bedoeld in de leden 1 en 2, uit te voeren:

a) oefent hij zijn bevoegdheden uit hoofde van artikel 35 uit op basis van alle feiten en documenten waarover hij beschikt;

b) documenteert hij en licht hij de gevolgen toe van zijn onvermogen om de in dit artikel bedoelde beoogde oversightactiviteiten uit te voeren.

De in punt b) van dit lid bedoelde mogelijke gevolgen worden in aanmerking genomen in de aanbevelingen die de lead overseer overeenkomstig artikel 35, lid 1, punt d), uitvaardigt.

Artikel 37

Verzoek om informatie

1. De lead overseer kan kritieke derde aanbieders van ICT-diensten verzoeken of bij besluit gelasten alle informatie die hij nodig heeft om zijn taken uit hoofde van deze verordening uit te voeren, te verstrekken, met inbegrip van alle relevante bedrijfs- of operationele documenten, contracten, beleidsdocumentatie, verslagen van ICT-beveiligingsaudits, verslagen van ICT-gerelateerde incidenten, alsmede alle informatie met betrekking tot partijen waaraan de kritieke derde aanbieder van ICT-diensten operationele functies of activiteiten heeft uitbesteed.

2. Bij het toezenden van een verzoek om informatie krachtens lid 1 neemt de lead overseer het volgende in acht:

a) hij vermeldt dit artikel als rechtsgrondslag voor het verzoek;

b) hij geeft het doel van het verzoek aan;

c) hij vermeldt welke informatie wordt verlangd;

d) hij bepaalt binnen welke termijn de informatie moet worden verstrekt;

e) hij deelt de vertegenwoordiger van de voor informatie aangezochte kritieke derde aanbieder van ICT-diensten mee dat deze niet verplicht is de informatie te verstrekken maar dat, in geval vrijwillig op het verzoek wordt ingegaan, de verstrekte informatie niet onjuist en misleidend mag zijn.

3. Wanneer de lead overseer krachtens lid 1 bij besluit informatieverstrekking gelast, neemt hij het volgende in acht:

a) hij vermeldt dit artikel als rechtsgrondslag voor het besluit;

b) hij geeft het doel van het besluit aan;

c) hij vermeldt welke informatie wordt verlangd;

d) hij bepaalt binnen welke termijn de informatie moet worden verstrekt;

e) hij vermeldt welke dwangsom overeenkomstig artikel 35, lid 6, wordt opgelegd indien de gevraagde informatie niet volledig wordt overgelegd of wanneer deze informatie niet binnen de in punt d) van dit lid vermelde termijn wordt verstrekt;

f) hij vermeldt dat tegen het besluit bezwaar kan worden aangetekend bij de bezwaarcommissie van de ETA's en dat bij het Hof van Justitie van de Europese Unie ("Hof van Justitie") tegen het besluit in beroep kan worden gegaan overeenkomstig de artikelen 60 en 61 van Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 of (EU) nr. 1095/2010.

4. De vertegenwoordigers van de kritieke derde aanbieders van ICT-diensten verstrekken de gevraagde informatie. Naar behoren gemachtigde advocaten kunnen namens hun cliënten de gevraagde informatie verstrekken. De kritieke derde aanbieder van ICT-diensten blijft volledig verantwoordelijk indien de verstrekte inlichtingen onvolledig, onjuist of misleidend zijn.

5. De lead overseer zendt onverwijld een afschrift van het besluit inzake informatieverstrekking aan de bevoegde autoriteiten van de financiële entiteiten die gebruikmaken van de diensten van de betrokken kritieke derde aanbieders van ICT-diensten en aan het JON.

Artikel 38

Algemene onderzoeken

1. Voor de uitvoering van zijn taken uit hoofde van deze verordening kan de lead overseer, ondersteund door het in artikel 40, lid 1, bedoelde gezamenlijke onderzoeksteam, zo nodig, bij kritieke derde aanbieders van ICT-diensten onderzoeken verrichten.

2. De lead overseer is bevoegd om:

a) registers, data, procedures en alle overig voor de uitvoering van zijn taken relevant materiaal te onderzoeken, ongeacht de drager waarop dit materiaal opgeslagen;

b) voor eensluidend gewaarmerkte kopieën of uittreksels te maken of te verkrijgen van deze registers, data, gedocumenteerde procedures en enig ander materiaal;

c) vertegenwoordigers van kritieke derde aanbieder van ICT-diensten op te roepen en te verzoeken om mondelinge of schriftelijke toelichting te geven bij feiten of documenten die betrekking hebben op het onderwerp en het doel van het onderzoek, en de antwoorden op te tekenen;

d) alle andere dan onder punt c) genoemde natuurlijke personen of rechtspersonen te horen, voor zover die daarin toestemmen, om informatie over het onderwerp van een onderzoek te verzamelen;

e) overzichten van telefoon- en dataverkeer op te vragen.

3. De functionarissen van de lead overseer en andere door hem voor de uitvoering van de in lid 1 bedoelde onderzoeken gemachtigde personen oefenen hun bevoegdheden uit na overlegging van een schriftelijke machtiging waarin het onderwerp en het doel van het onderzoek zijn vermeld.

In deze machtiging worden eveneens de in artikel 35, lid 6, bedoelde dwangsommen genoemd die kunnen worden opgelegd indien de vereiste registers, data, gedocumenteerde procedures of enig ander materiaal, dan wel de antwoorden op vragen van de onderzoekers aan vertegenwoordigers van derde aanbieders van ICT-diensten, niet of niet volledig worden verstrekt.

4. De vertegenwoordigers van kritieke derde aanbieders van ICT-diensten zijn verplicht zich aan het onderzoek te onderwerpen op basis van een besluit van de lead overseer. Het besluit vermeldt het onderwerp en het doel van het onderzoek, de dwangsommen die overeenkomstig artikel 35, lid 6, kunnen worden opgelegd, de krachtens de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 beschikbare rechtsmiddelen, en het recht om bij het Hof van Justitie in beroep te gaan tegen het besluit.

5. De lead overseer stelt de bevoegde organen van de financiële entiteit die gebruikmaakt van de ICT-diensten van die kritieke derde aanbieder van ICT-diensten, geruime tijd vóór de start van het onderzoek in kennis van het voorgenomen onderzoek en van de identiteit van de gemachtigde personen.

De lead overseer stelt het JON in kennis van alle overeenkomstig de eerste alinea toegestuurde informatie.

Artikel 39

Inspecties

1. De lead overseer kan voor de uitvoering van zijn taken uit hoofde van deze verordening, en ondersteund door de in artikel 40, lid 1, bedoelde gezamenlijke onderzoeksteams, alle nodige inspecties ter plaatse verrichten in alle bedrijfsruimten, op alle terreinen en op of in alle eigendommen van derde aanbieders van ICT-diensten, zoals hoofdkantoren, operationele centra en secundaire locaties. Ook kan hij off-site-inspecties verrichten.

Voor de uitoefening van de in de eerste alinea bedoelde bevoegdheden raadpleegt de lead overseer het JON.

2. De functionarissen en andere personen die door de lead overseer zijn gemachtigd tot het verrichten van een inspectie ter plaatse, beschikken over de bevoegdheid om:

a) zich toegang te verschaffen tot de eerder genoemde bedrijfsruimten, terreinen en eigendommen, en

b) bedrijfsruimten, boeken en bescheiden te verzegelen zolang en voor zover dit nodig is voor de inspectie.

De functionarissen en andere personen die door de lead overseer zijn gemachtigd, oefenen deze bevoegdheden uit na overlegging van een schriftelijke machtiging waarin het onderwerp en het doel van de inspectie worden vermeld, alsmede de dwangsommen als bedoeld in artikel 35, lid 6, indien de vertegenwoordigers van de kritieke derde aanbieders van ICT-diensten zich niet aan de inspectie onderwerpen.

3. De lead overseer stelt de bevoegde autoriteiten van de financiële entiteit die gebruikmaakt van de derde aanbieder van ICT-diensten, geruime tijd vóór de start ervan in kennis van de inspectie.

4. De inspectie heeft betrekking op alle ICT-systemen, -netwerken, -apparatuur, -informatie en -data die worden gebruikt voor of bijdragen tot het verlenen van ICT-diensten aan financiële entiteiten.

5. Vóór een geplande inspectie ter plaatse stelt de lead overseer de kritieke derde aanbieder van ICT-diensten in kennis van de inspectie en neemt hierbij een redelijke termijn in acht, tenzij dit niet mogelijk is vanwege een nood- of crisissituatie of de kennisgeving zou leiden tot een situatie waarin de inspectie of audit niet langer doeltreffend is.

6. De kritieke derde aanbieder van ICT-diensten onderwerpt zich aan de inspecties ter plaatse die bij besluit van de lead overseer zijn gelast. Het besluit vermeldt het onderwerp en het doel van de inspectie, de datum waarop de inspectie zal aanvangen, de dwangsommen als bedoeld in artikel 35, lid 6, de krachtens de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 beschikbare rechtsmiddelen, en het recht om bij het Hof van Justitie tegen het besluit in beroep te gaan.

7. Indien de door de lead overseer gemachtigde functionarissen en andere personen constateren dat een kritieke derde aanbieder van ICT-diensten zich verzet tegen een krachtens dit artikel gelaste inspectie, stelt de lead overseer de kritieke derde aanbieder van ICT-diensten in kennis van de gevolgen van dit verzet, met inbegrip van de mogelijkheid voor de bevoegde autoriteiten van de financiële entiteit om van de financiële entiteit te vereisen dat zij de contractuele overeenkomsten met de kritieke derde aanbieder van ICT-diensten beëindigt.

Artikel 40

Oversight tijdens de uitvoering

1. Bij het uitvoeren van oversightactiviteiten, met name algemene onderzoeken of inspecties, wordt de lead overseer bijgestaan door een gezamenlijk onderzoeksteam dat voor iedere toezichtactiviteit bij een kritieke derde aanbieder van ICT-diensten wordt opgericht.

2. Het in lid 1 bedoelde gezamenlijke onderzoeksteam bestaat uit functionarissen van:

a) de ETA's;

b) de bevoegde autoriteiten die toezicht houden op de financiële entiteiten waaraan de kritieke derde aanbieder van ICT-diensten ICT-diensten verleent;

c) de in artikel 32, lid 4, punt e), bedoelde nationale bevoegde autoriteit (op vrijwillige basis);

d) één nationale bevoegde autoriteit van de lidstaat waar de kritieke derde aanbieder van ICT-diensten is gevestigd (op vrijwillige basis).

De leden van het gezamenlijke onderzoeksteam beschikken over deskundigheid op het terrein van ICT-aangelegenheden en van operationele risico's. Het team wordt gecoördineerd door een functionaris van de lead overseer die hiertoe is aangewezen (de "coördinator van de lead overseer").

3. Binnen drie maanden na de voltooiing van een onderzoek of een inspectie doet de lead overseer, na raadpleging van het oversightforum, aanbevelingen aan de kritieke derde aanbieder van ICT-diensten (overeenkomstig de in artikel 35 bedoelde bevoegdheden).

4. De kritieke derde aanbieder van ICT-diensten en de bevoegde autoriteiten van de financiële entiteit waarvoor de dienstverlener ICT-diensten werkt, worden onverwijld in kennis gesteld van de in lid 3 bedoelde aanbevelingen.

Voor de uitvoering van de oversightactiviteiten kan de lead overseer eventuele certificeringen door derden en interne of externe ICT-auditverslagen in aanmerking nemen die door de kritieke derde aanbieder van ICT-diensten te zijner beschikking zijn gesteld.

Artikel 41

Harmonisatie van de voorwaarden voor de uitoefening van de oversightactiviteiten

1. De ETA's stellen via het Gemengd Comité ontwerpen van technische reguleringsnormen op tot nadere omschrijving van:

a) de door de derde aanbieder van ICT-diensten te verstrekken informatie bij diens vrijwillige verzoek om te worden aangewezen als kritieke ICT-dienstverlener als bedoeld in artikel 31, lid 11;

b) de inhoud, de structuur en het formaat van de informatie die overeenkomstig artikel 35, lid 1, door de kritieke derde aanbieder van ICT-diensten moet worden ingediend, openbaar gemaakt of gerapporteerd, met inbegrip van het model voor het verstrekken van informatie over onderaannemingsovereenkomsten;

c) de criteria voor het bepalen van de samenstelling van het gezamenlijke onderzoeksteam in verband met een evenwichtige participatie van functionarissen van de ETA's en van de bevoegde autoriteiten, alsmede van hun aanwijzing, hun taken en hun werkafspraken.

d) de nadere gegevens van de beoordeling die de bevoegde autoriteiten overeenkomstig artikel 42, lid 3, hebben verricht van de maatregelen die door de kritieke derde aanbieder van ICT-diensten zijn genomen op basis van de aanbevelingen van de lead overseer.

2. De ETA's leggen deze ontwerpen van technische reguleringsnormen uiterlijk op 17 juli 2024 voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in lid 1 bedoelde technische reguleringsnormen vast te stellen overeenkomstig de procedure bedoeld in de artikelen 10 tot en met 14 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

Artikel 42

Vervolgmaatregelen van de bevoegde autoriteiten

1. Binnen 60 kalenderdagen na ontvangst van de aanbevelingen die de lead overseer overeenkomstig artikel 35, lid 1, punt d), heeft gedaan, stelt de kritieke derde aanbieder van ICT-diensten de lead overseer in kennis van zijn voornemen om de aanbevelingen op te volgen of geeft hij een gemotiveerde verklaring, waarom hij geen gevolg geeft aan de aanbevelingen. De lead overseer stelt de bevoegde autoriteiten van de betrokken financiële entiteit onverwijld in kennis van deze informatie.

2. Indien een kritieke derde aanbieder van ICT-diensten verzuimt de lead overseer overeenkomstig lid 1 in kennis te stellen van zijn voornemens met betrekking tot de aanbeveling of indien de in lid 1 bedoelde verklaring niet toereikend wordt geacht, maakt de lead overseer dit verzuim of deze ontoereikendheid openbaar. Deze openbare informatie omvat de identiteit van de kritieke derde aanbieder van ICT-diensten en informatie over het type en de aard van de niet-naleving. Deze informatie is beperkt tot hetgeen relevant en voldoende is om het publiek op de hoogte te brengen, tenzij de bekendmaking de betrokken partijen onevenredige schade zou berokkenen of de ordelijke werking en de integriteit van de financiële markten of de stabiliteit van het gehele financiële stelsel van de Unie of een deel daarvan ernstig in gevaar zou kunnen brengen.

De lead overseer stelt de kritieke derde aanbieder van ICT-diensten in kennis van die openbaarmaking.

3. De bevoegde autoriteiten stellen de relevante financiële entiteit in kennis van de risico's die zijn geconstateerd in de aanbevelingen aan de kritieke derde aanbieder van ICT-diensten overeenkomstig artikel 35, lid 1, punt d).

Bij het beheer van ICT-risico's van derden houdt een financiële entiteit rekening met de in de eerste alinea bedoelde risico's.

4. Indien een bevoegde autoriteit van oordeel is dat een financiële entiteit bij het beheer van derde ICT-risico's de in de aanbevelingen geconstateerde risico's niet of niet voldoende in aanmerking neemt of onvoldoende in het werk stelt om deze te verhelpen, stelt de autoriteit de financiële entiteit in kennis van de mogelijkheid dat binnen 60 kalenderdagen na de ontvangst van deze kennisgeving een besluit als bedoeld in lid 6 kan worden genomen indien er geen passende contractuele overeenkomsten zijn om deze risico's te verhelpen.

5. Na ontvangst van de in artikel 35, lid 1, punt c), bedoelde meldingen en voordat een besluit als bedoeld in lid 6 van dit artikel wordt genomen, kunnen de bevoegde autoriteiten op vrijwillige basis de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten raadplegen die verantwoordelijk zijn voor het toezicht op een essentiële of belangrijke entiteit die onder die richtlijn valt en die is aangewezen als een kritieke derde aanbieder van ICT-diensten.

6. De bevoegde autoriteiten kunnen bij wijze van laatste redmiddel, na de kennisgeving en, in voorkomend geval, de raadpleging als bedoeld in de leden 4 en 5 van dit artikel, overeenkomstig artikel 50 een besluit nemen waarbij een financiële entiteit wordt verplicht het gebruik of de inzet van een door een kritieke derde aanbieder van ICT-diensten verleende dienst geheel of gedeeltelijk tijdelijk te staken, en wel totdat de in de aanbevelingen aan de kritieke derde aanbieder van ICT-diensten geconstateerde risico's zijn verholpen. Indien nodig kunnen de autoriteiten een financiële entiteit ertoe verplichten de contractuele overeenkomsten met de kritieke derde aanbieder van ICT-diensten geheel of gedeeltelijk te beëindigen.

7. Indien een kritieke derde aanbieder van ICT-diensten weigert de aanbevelingen op te volgen door voor een andere aanpak te kiezen dan die welke door de lead overseer wordt aanbevolen, en indien deze afwijkende keus negatieve gevolgen kan hebben voor een groot aantal financiële entiteiten of voor een aanzienlijk deel van de financiële sector, en indien afzonderlijke waarschuwingen van bevoegde autoriteiten niet hebben geleid tot een consistente aanpak om het potentiële risico voor de financiële stabiliteit te beperken, kan de lead overseer, na raadpleging van het oversightforum, niet-bindende en niet-openbare adviezen aan de bevoegde autoriteiten uitbrengen om consistente en convergente vervolgmaatregelen voor het toezicht te bevorderen, naargelang het geval.

8. De bevoegde autoriteiten nemen na het ontvangen van de in artikel 35, lid 1, punt c), bedoelde meldingen bij het nemen van het in lid 6 van dit artikel bedoelde besluit het soort en de omvang van het risico dat of de risico's die de kritieke derde aanbieder van ICT-diensten niet heeft verholpen, in aanmerking, alsook de ernst van de niet-naleving, en wel op basis van de volgende criteria:

a) de ernst en de duur van de niet-naleving;

b) de vraag of de niet-naleving ernstige zwakheden aan het licht heeft gebracht in de procedures, de beheersystemen, het risicobeheer en de interne controles van de kritieke derde aanbieder van ICT-diensten;

c) de vraag of door de niet-naleving een financieel delict is vergemakkelijkt of veroorzaakt of op andere wijze aan de niet-naleving kan worden toegeschreven;

d) de vraag of de niet-naleving opzettelijk is geweest of aan nalatigheid moet worden toegeschreven;

e) de vraag of het tijdelijk staken of beëindigen van de contractuele overeenkomsten een risico voor de continuïteit van de bedrijfsactiviteiten van de financiële entiteit betekent, niettegenstaande de inspanningen van de financiële entiteit om verstoring van haar dienstverlening te voorkomen;

f) indien van toepassing, het advies, indien hierom overeenkomstig lid 5 van dit artikel op vrijwillige basis is verzocht, van de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten die verantwoordelijk zijn voor het toezicht op een essentiële of belangrijke entiteit die onder die richtlijn valt en die is aangewezen als kritieke derde aanbieder van ICT-diensten.

De bevoegde autoriteiten geven een financiële entiteit de nodige tijd om de contractuele overeenkomsten met de kritieke derde aanbieder van ICT-diensten aan te passen teneinde nadelige gevolgen voor de digitale operationele weerbaarheid van de entiteit te voorkomen en deze in staat te stellen exitstrategieën en transitieplannen als bedoeld in artikel 28 in te zetten.

9. De in artikel 32, lid 4, punten a), b) en c), bedoelde leden van het oversightforum en het JON worden in kennis gesteld van het in lid 6 van dit artikel bedoelde besluit.

De kritieke derde aanbieder van ICT-diensten die gevolgen ondervindt van een in lid 6 bedoeld besluit, werkt volledig samen met de getroffen financiële entiteit, met name bij het tijdelijk staken of beëindigen van hun contractuele overeenkomsten.

10. De bevoegde autoriteiten stellen de lead overseer regelmatig in kennis van de aanpak en de maatregelen die zij in het kader van hun toezichttaken ten aanzien van financiële entiteiten hebben gehanteerd, alsmede van de contractuele overeenkomsten die deze entiteiten hebben gesloten met kritieke derde aanbieders van ICT-diensten die niet of slechts gedeeltelijk zijn ingegaan op de aan hen gerichte aanbevelingen van de lead overseer.

11. De lead overseer kan op verzoek nadere toelichtingen geven op de gedane aanbevelingen om zo de bevoegde autoriteiten te helpen bij vervolgmaatregelen.

Artikel 43

Oversightvergoedingen

1. De lead overseer brengt overeenkomstig de in lid 2 van dit artikel bedoelde gedelegeerde handeling kritieke derde aanbieders van ICT-diensten vergoedingen in rekening die de noodzakelijke uitgaven van de lead overseer in verband met de uitvoering van de oversighttaken uit hoofde van deze verordening volledig dekken. Deze uitgaven bestrijken ook de vergoeding van eventuele kosten van de werkzaamheden van het in artikel 40 bedoelde gezamenlijke onderzoeksteam, alsmede de kosten van het advies van de onafhankelijke deskundigen als bedoeld in artikel 32, lid 4, tweede alinea, met betrekking tot aangelegenheden die deel uitmaken van directe oversightactiviteiten.

Het bedrag van de vergoeding die de kritieke derde aanbieder van ICT-diensten in rekening wordt gebracht, dekt alle kosten die voortvloeien uit de uitvoering van de in deze afdeling opgenomen taken, en staat in verhouding tot diens omzet.

2. De Commissie is bevoegd om overeenkomstig artikel 57 en in aanvulling op deze verordening een gedelegeerde handeling vast te stellen waarin het bedrag van de vergoedingen en de wijze waarop deze uiterlijk op 17 juli 2024 moeten worden betaald, worden bepaald.

Artikel 44

Internationale samenwerking

1. Onverminderd artikel 36, kunnen de EBA, de ESMA en de Eiopa overeenkomstig artikel 33 van respectievelijk Verordeningen (EU) nr. 1093/2010, (EU) nr. 1095/2010 en (EU) nr. 1094/2010 administratieve overeenkomsten sluiten met regelgevende en toezichthoudende autoriteiten van derde landen om de internationale samenwerking op het gebied van ICT-risico's van derde dienstverleners in verschillende financiële sectoren te bevorderen, in het bijzonder door de ontwikkeling van beste praktijken voor de evaluatie van praktijken voor beheer van en controles op ICT-risico's, risicobeperkende maatregelen en responsen op incidenten.

2. De ETA's dienen via het Gemengd Comité om de vijf jaar een gezamenlijk vertrouwelijk verslag in bij het Parlement, de Raad en de Commissie waarin de bevindingen van de besprekingen met de in lid 1 bedoelde autoriteiten van derde landen worden samengevat en waarin bijzondere aandacht wordt geschonken aan de evolutie van de ICT-risico's van derde aanbieders van ICT-diensten en de gevolgen voor de financiële stabiliteit, de integriteit van de markt, de bescherming van beleggers en de werking van de interne markt.

HOOFDSTUK VI

Regelingen voor de uitwisseling van informatie

Artikel 45

Regelingen voor uitwisseling van informatie en inlichtingen over cyberdreiging

1. Financiële entiteiten kunnen onderling informatie en inlichtingen over cyberdreiging uitwisselen, zoals indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten, voor zover dit:

a) bedoeld is om de digitale operationele weerbaarheid van de financiële entiteiten te versterken, met name via bewustmaking van cyberdreigingen, beperking of belemmering van de mogelijkheid tot verdere verspreiding van cyberdreigingen, ondersteuning van defensiecapaciteiten, technieken voor dreigingsdetectie, risicobeperkende strategieën en respons- en herstelfasen;

b) gebeurt binnen vertrouwensgemeenschappen van financiële entiteiten;

c) gedaan wordt via regelingen voor informatie-uitwisseling die de potentieel gevoelige aard van de gedeelde informatie beschermen en waarvoor gedragsregels gelden waarin de vertrouwelijkheid van bedrijfsinformatie, de bescherming van persoonsgegevens overeenkomstig Verordening (EU) 2016/679 en de richtsnoeren inzake mededingingsbeleid volledig worden gerespecteerd.

2. Voor de toepassing van lid 1, punt c), worden in de regelingen voor informatie-uitwisseling de voorwaarden voor deelname bepaald en, in voorkomend geval, nadere bepalingen voor de betrokkenheid van overheidsinstanties en de hoedanigheid waarin deze instanties bij bedoelde regelingen kunnen worden betrokken. Ook kunnen nadere bepalingen worden vastgelegd voor de betrokkenheid van derde aanbieders van ICT-diensten en voor operationele aspecten, waaronder het gebruik van specifieke ICT-platforms.

3. Een financiële entiteit stelt de bevoegde autoriteiten, na goedkeuring van haar deelname in de vertrouwensgemeenschap, in kennis van haar deelname aan de in lid 1 bedoelde regelingen voor informatie-uitwisseling, en, in voorkomend geval, van de beëindiging van haar deelname zodra deze beëindiging van kracht wordt.

HOOFDSTUK III

Bevoegde autoriteiten

Artikel 46

Bevoegde autoriteiten

Onverminderd de bepalingen voor het oversightkader voor kritieke derde aanbieders van ICT-diensten als bedoeld in hoofdstuk V, afdeling II, van deze verordening, wordt de naleving van deze verordening verzekerd door de volgende bevoegde autoriteiten, die handelen in overeenstemming met de bevoegdheden die hen bij de desbetreffende rechtshandelingen zijn verleend:

a) voor kredietinstellingen en voor instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld: de overeenkomstig artikel 4 van die richtlijn aangewezen bevoegde autoriteit, en voor kredietinstellingen die overeenkomstig artikel 6, lid 4, van Verordening (EU) nr. 1024/2013 als belangrijk zijn geclassificeerd: de ECB overeenkomstig de bij die verordening aan de ECB verleende bevoegdheden en taken;

b) voor betalingsinstellingen (waaronder betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld), instellingen voor elektronisch geld (waaronder zij die zijn vrijgesteld krachtens Richtlijn 2009/110/EG), en aanbieders van rekeninginformatiediensten als bedoeld in artikel 33, lid 1, van Richtlijn (EU) 2015/2366: de bevoegde autoriteit als aangewezen overeenkomstig artikel 22 van Richtlijn (EU) 2015/2366;

c) voor beleggingsondernemingen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 4 van Richtlijn (EU) 2019/2034 van het Europees Parlement en de Raad ([38]);

d) voor aanbieders van cryptoactivadiensten met een vergunning op grond van de verordening betreffende markten in cryptoactiva en emittenten van *asset-referenced tokens*: de overeenkomstig de relevante bepaling van die verordening aangewezen bevoegde autoriteit;

e) voor centrale effectenbewaarinstellingen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 11 van Verordening (EU) nr. 909/2014;

f) voor centrale tegenpartijen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 22 van Verordening (EU) nr. 648/2012;

g) voor handelsplatformen en aanbieders van datarapporteringsdiensten: de bevoegde autoriteit als aangewezen overeenkomstig artikel 67 van Richtlijn 2014/65/EU, en de bevoegde autoriteit als gedefinieerd in artikel 2, lid 1, punt 18), van Verordening (EU) nr. 600/2014;

h) voor transactieregisters: de bevoegde autoriteit als aangewezen overeenkomstig artikel 22 van Verordening (EU) nr. 648/2012;

i) voor beheerders van alternatieve beleggingsinstellingen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 44 van Richtlijn 2011/61/EU;

j) voor beheermaatschappijen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 97 van Richtlijn 2009/65/EG;

k) voor verzekerings- en herverzekeringsmaatschappijen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 30 van Richtlijn 2009/138/EG;

l) voor verzekerings-, herverzekerings- en nevenverzekeringstussenpersonen: de bevoegde autoriteit als aangewezen overeenkomstig artikel 12 van Richtlijn (EU) 2016/97;

m) voor instellingen voor bedrijfspensioenvoorziening: de bevoegde autoriteit als aangewezen overeenkomstig artikel 47 van Richtlijn (EU) 2016/2341;

n) voor kredietbeoordelingsbureaus: de bevoegde autoriteit als aangewezen overeenkomstig artikel 21 van Verordening (EG) nr. 1060/2009;

o) voor beheerders van kritieke benchmarks: de bevoegde autoriteit als aangewezen overeenkomstig de artikelen 40 en 41 van Verordening (EU) 2016/1011;

([38]) Richtlijn (EU) 2019/2034 van het Europees Parlement en de Raad van 27 november 2019 betreffende het prudentiële toezicht op beleggingsondernemingen en tot wijziging van Richtlijnen 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU en 2014/65/EU (PB L 314 van 5.12.2019, blz. 64).

p) voor aanbieders van crowdfundingdiensten: de bevoegde autoriteit als aangewezen overeenkomstig artikel 29 van Verordening (EU) 2020/1503;

q) voor securitisatieregisters: de bevoegde autoriteit als aangewezen overeenkomstig artikel 10 en artikel 14, lid 1, van Verordening (EU) 2017/2402.

Artikel 47

Samenwerking met structuren en autoriteiten die zijn opgericht bij Richtlijn (EU) 2022/2555

1. Om de samenwerking te bevorderen en uitwisselingen tussen de krachtens deze verordening aangewezen bevoegde autoriteiten en de bij artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep mogelijk te maken, kunnen de ETA's en de bevoegde autoriteiten deelnemen aan de activiteiten van de samenwerkingsgroep voor aangelegenheden die hun toezicht op de financiële entiteiten betreffen. De ETA's en de bevoegde autoriteiten kunnen verzoeken te worden uitgenodigd om deel te nemen aan de activiteiten van de samenwerkingsgroep voor aangelegenheden met betrekking tot de essentiële of belangrijke entiteiten die onder Richtlijn (EU) 2022/2555 vallen en die overeenkomstig artikel 31 van deze verordening ook zijn aangewezen als kritieke derde aanbieders van ICT-diensten.

2. In voorkomend geval kunnen de bevoegde autoriteiten de centrale contactpunten en de CSIRT's die zijn aangewezen of ingesteld overeenkomstig Richtlijn (EU) 2022/2555 raadplegen en informatie met hen uitwisselen.

3. In voorkomend geval kunnen de bevoegde autoriteiten alle relevante technische adviezen en bijstand inwinnen bij de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten, en kunnen zij samenwerkingsregelingen treffen voor een effectieve coördinatie van een snelle respons.

4. In de in lid 3 van dit artikel bedoelde regelingen kunnen onder meer de procedures worden bepaald voor de coördinatie van de oversightactiviteiten met betrekking tot essentiële of belangrijke entiteiten die onder Richtlijn (EU) 2022/2555 vallen en die overeenkomstig artikel 31 van deze verordening zijn aangewezen als kritieke derde aanbieders van ICT-diensten; ook de procedures voor de uitvoering, overeenkomstig nationaal recht, van onderzoeken en inspecties ter plaatse, alsmede de procedures voor regelingen voor de uitwisseling van informatie tussen de bevoegde autoriteiten uit hoofde van deze verordening en de bevoegde autoriteiten die zijn aangewezen of ingesteld overeenkomstig die richtlijn, kunnen in de in lid 3 van dit artikel bedoelde regelingen worden bepaald, met inbegrip van de toegang tot door die laatste autoriteiten gevraagde informatie.

Artikel 48

Samenwerking tussen autoriteiten

1. De bevoegde autoriteiten werken nauw samen met elkaar en, indien van toepassing, met de lead overseer.

2. De bevoegde autoriteiten en de lead overseer wisselen tijdig alle relevante informatie over kritieke derde aanbieders van ICT-diensten uit die zij nodig hebben om hun taken uit hoofde van deze verordening te verrichten, met name met betrekking tot geconstateerde risico's en benaderingen die worden gehanteerd en maatregelen die worden genomen in het kader van de oversighttaken van de lead overseer.

Artikel 49

Sectoroverschrijdende financiële oefeningen, communicatie en samenwerking

1. De ETA's kunnen via het Gemengd Comité en in samenwerking met de bevoegde autoriteiten de nationale afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU, de ECB, de Gemeenschappelijke Afwikkelingsraad als het om informatie gaat met betrekking tot entiteiten die onder het toepassingsgebied van Verordening (EU) nr. 806/2014 vallen, het ESRB en Enisa — alle voor zover van toepassing — regelingen invoeren voor de uitwisseling tussen financiële sectoren van doeltreffende praktijken, zulks met de bedoeling de situatiekennis en de opsporing van gemeenschappelijke cyberkwetsbaarheden en sectoroverschrijdende risico's te verbeteren.

Zij kunnen oefeningen ontwikkelen voor crisisbeheer en noodsituaties met cyberaanvalsscenario's en zo communicatiekanalen opzetten en geleidelijk een doeltreffende gecoördineerde respons op Unieniveau mogelijk maken bij een ernstig grensoverschrijdend ICT-incident of een daarmee verband houdende dreiging die mogelijk een systemisch effect zal hebben op de financiële sector van de Unie in zijn geheel.

Bij die oefeningen kan indien noodzakelijk ook worden getest in welke mate de financiële sector afhankelijk is van andere economische sectoren.

2. De bevoegde autoriteiten, de ETA's en de ECB werken onderling nauw samen en wisselen informatie uit om hun taken overeenkomstig de artikelen 47 tot en met 54 te verrichten. Zij coördineren ten nauwste hun toezicht teneinde inbreuken op deze verordening op te sporen en te corrigeren, goede praktijken te ontwikkelen en te stimuleren, samenwerking te vergemakkelijken, een consistente interpretatie van ter zake geldende bepalingen te bevorderen, en in geval van meningsverschil rechtsgebiedoverschrijdende beoordelingen te geven.

Artikel 50

Administratieve strafmaatregelen en corrigerende maatregelen

1. De bevoegde autoriteiten hebben alle bevoegdheden inzake toezicht, onderzoek en oplegging van strafmaatregelen die noodzakelijk zijn om hun taken uit hoofde van deze verordening te verrichten.

2. De in lid 1 bedoelde bevoegdheden omvatten ten minste de bevoegdheid om:

a) toegang te verkrijgen tot documenten en gegevens, in enigerlei vorm, die de bevoegde autoriteit relevant acht voor het verrichten van haar taken, en een kopie hiervan te ontvangen of te maken;

b) inspecties of onderzoeken ter plaatse uit te voeren, met inbegrip van, maar niet beperkt tot:

   i) het oproepen van vertegenwoordigers van de financiële entiteit en hen verzoeken om mondelinge of schriftelijke toelichting te geven bij feiten of documenten met betrekking tot het onderwerp en het doel van het onderzoek, en de antwoorden op te tekenen;

   ii) het horen van alle andere natuurlijke personen of rechtspersonen die daarin toestemmen, teneinde informatie over het onderwerp van een onderzoek te verzamelen;

c) corrigerende maatregelen te eisen voor inbreuken op de voorschriften van deze verordening.

3. Onverminderd het recht om overeenkomstig artikel 52 strafrechtelijke maatregelen te nemen, stellen de lidstaten regels vast voor de invoering van passende administratieve strafmaatregelen en corrigerende maatregelen voor inbreuken op deze verordening, en waarborgen zij de daadwerkelijke uitvoering van deze maatregelen.

Deze straf- en andere maatregelen moeten doeltreffend zijn, in verhouding staan tot de inbreuk, en een afschrikkende werking hebben.

4. De lidstaten verlenen de bevoegde autoriteiten de bevoegdheid om bij inbreuk op deze verordening ten minste de volgende administratieve strafmaatregelen of corrigerende maatregelen te nemen:

a) natuurlijke of rechtspersoon bij officieel besluit gelasten de gedraging die inbreuk maakt op deze verordening, te staken en deze gedraging niet te herhalen;

b) eisen dat praktijken of gedragingen die de bevoegde autoriteit strijdig acht met de bepalingen van deze verordening, tijdelijk of definitief worden gestaakt, en dat herhaling van deze praktijk of gedraging wordt voorkomen;

c) het nemen van iedere soort maatregel, onder meer van geldelijke aard, om ervoor te zorgen dat de financiële entiteit aan de wettelijke vereisten blijft voldoen;

d) eisen — voor zover dit bij nationaal recht is toegestaan — dat bestaande overzichten van dataverkeer die in het bezit zijn van een telecommunicatie-exploitant, worden overgelegd, indien er een redelijk vermoeden van inbreuk op deze verordening bestaat, en indien deze overzichten van belang kunnen zijn voor een onderzoek naar inbreuken op deze verordening, en

e) het doen uitgaan van openbare mededelingen, met inbegrip van openbare verklaringen, waarbij de identiteit van de natuurlijke of rechtspersoon die de inbreuk heeft begaan, en de aard van de inbreuk worden bekendgemaakt.

5. Indien lid 2, punt c), en lid 4 van toepassing zijn op rechtspersonen, verlenen de lidstaten de bevoegde autoriteiten de bevoegdheid om administratieve strafmaatregelen of corrigerende maatregelen te nemen ten aanzien van leden van het leidinggevend orgaan van de financiële entiteit en andere personen die krachtens nationaal recht verantwoordelijk zijn voor de inbreuk. Hierbij dienen de voorwaarden van het nationale recht in acht te worden genomen.

6. De lidstaten zien erop toe dat een besluit waarbij de in lid 2, punt c), genoemde administratieve strafmaatregelen of corrigerende maatregelen worden genomen, naar behoren gemotiveerd is en vatbaar is voor beroep.

Artikel 51

Uitoefening van de bevoegdheid tot het nemen van administratieve strafmaatregelen en corrigerende maatregelen

1. De bevoegde autoriteiten oefenen de bevoegdheid tot het nemen van administratieve strafmaatregelen en corrigerende maatregelen als bedoeld in artikel 50 uit conform het nationaal recht, en wel naargelang van het geval:

a) rechtstreeks;

b) in samenwerking met andere autoriteiten;

c) door middel van delegatie aan andere autoriteiten maar onder eigen verantwoordelijkheid, of

d) door middel van een verzoek tot de bevoegde rechterlijke instanties.

2. De bevoegde autoriteiten houden bij het bepalen van het type en de omvang van een op grond van artikel 50 te nemen administratieve strafmaatregel of corrigerende maatregel rekening met de vraag, in hoeverre de inbreuk opzettelijk is, dan wel het resultaat is van nalatigheid, en met andere relevante omstandigheden, waaronder, in voorkomend geval:

a) het relatieve belang, de ernst en de duur van de inbreuk;

b) de mate van verantwoordelijkheid van de natuurlijke of rechtspersoon die de inbreuk heeft gepleegd;

c) de financiële draagkracht van de verantwoordelijke natuurlijke of rechtspersoon;

d) de omvang van winsten die de verantwoordelijke natuurlijke of rechtspersoon heeft gemaakt of de verliezen die deze heeft vermeden, voor zover deze winsten of verliezen kunnen worden bepaald;

e) de verliezen voor derde partijen ten gevolge van de inbreuk, voor zover deze kunnen worden bepaald;

f) de mate van medewerking van de verantwoordelijke natuurlijke of rechtspersoon met de bevoegde autoriteit, onverminderd de noodzaak om de terugbetaling van de door deze natuurlijke of rechtspersoon behaalde winsten of vermeden verliezen zeker te stellen;

g) eventuele eerdere inbreuken van de verantwoordelijke natuurlijke of rechtspersoon.

Artikel 52

Strafrechtelijke maatregelen

1. De lidstaten kunnen ertoe besluiten, geen regels voor administratieve strafmaatregelen of corrigerende maatregelen vast te stellen voor inbreuken waarop krachtens hun nationale recht strafrechtelijke maatregelen staan.

2. Indien de lidstaten ervoor hebben gekozen strafrechtelijke maatregelen vast te stellen voor inbreuken op deze verordening, zorgen zij voor passende maatregelen waardoor de bevoegde autoriteiten over alle noodzakelijke bevoegdheden beschikken om met de gerechtelijke, de met vervolging belaste of de strafrechtelijke autoriteiten in hun rechtsgebied in contact te treden ter verkrijging van specifieke informatie met betrekking tot strafrechtelijke onderzoeken of procedures ten aanzien van mogelijke inbreuken op deze verordening. Ook kunnen de bevoegde autoriteiten deze informatie verstrekken aan andere bevoegde autoriteiten en aan de EBA, de ESMA of de Eiopa, opdat zij zo voldoen aan hun verplichting tot samenwerking bij de toepassing van deze verordening.

Artikel 53

Kennisgevingsverplichting

De lidstaten stellen uiterlijk op 17 januari 2025 de Commissie, de ESMA, de EBA en de Eiopa in kennis van de wettelijke en bestuursrechtelijke bepalingen ter uitvoering van dit hoofdstuk, met inbegrip van eventuele strafrechtelijke bepalingen die van toepassing zijn. De lidstaten stellen de Commissie, de ESMA, de EBA en de Eiopa onverwijld in kennis van latere wijzigingen van deze bepalingen.

Artikel 54

Bekendmaking van administratieve strafmaatregelen

1. De bevoegde autoriteiten maken op hun officiële website onverwijld alle niet voor beroep vatbare besluiten tot het nemen van administratieve strafmaatregelen bekend, nadat de natuurlijke of rechtspersoon op wie een dergelijke maatregel van toepassing is, van deze maatregel in kennis is gesteld.

2. De in lid 1 bedoelde bekendmaking bevat informatie over het type en de aard van de inbreuk, de identiteit van de verantwoordelijke natuurlijke of rechtspersoon en de getroffen strafmaatregelen.

3. Indien de bevoegde autoriteit na de beoordeling van een geval van oordeel is dat de bekendmaking van de identiteit in het geval van rechtspersonen of van de identiteit en persoonsgegevens in het geval van natuurlijke personen onevenredige effecten kan hebben — waaronder risico's voor de bescherming van persoonsgegevens — de stabiliteit van de financiële markten of het verloop van een lopend onderzoek in gevaar kan brengen, of, voor zover dit kan worden bepaald, de betrokken natuurlijke of rechtspersonen onevenredige schade zou kunnen berokkenen, kiest zij een van de volgende oplossingen voor het besluit waarbij een administratieve strafmaatregel wordt genomen:

a) zij stelt de bekendmaking van het besluit uit totdat alle redenen voor niet-bekendmaking zijn vervallen;

b) zij maakt het besluit bekend met inachtneming van anonimiteit, in overeenstemming met het nationaal recht, of

c) zij onthoudt zich van de bekendmaking indien de in punten a) en b) genoemde keuzemogelijkheden ontoereikend worden geacht om te garanderen dat er geen gevaar bestaat voor de stabiliteit van de financiële markten of indien de effecten van de bekendmaking niet in verhouding staan tot de clementie van de genomen strafmaatregel.

4. Bij een besluit tot bekendmaking van een administratieve strafmaatregel met inachtneming van anonimiteit als bedoeld in lid 3, punt b), kan de bekendmaking van de betrokken gegevens worden uitgesteld.

5. Indien een bevoegde autoriteit een besluit tot het nemen van een administratieve strafmaatregel bekendmaakt dat vatbaar is voor beroep bij gerechtelijke autoriteiten, maakt de bevoegde autoriteit deze informatie en, in een later stadium, verdere informatie over het resultaat van een eventueel beroep onverwijld bekend op haar officiële website. Rechterlijke beslissingen tot nietigverklaring van een besluit waarbij een administratieve strafmaatregel is genomen, worden eveneens bekendgemaakt.

6. De bevoegde autoriteiten zorgen ervoor dat een bekendmaking als bedoeld in de leden 1 tot en met 4 slechts op hun officiële website blijft staan gedurende de periode die nodig is voor de inwerkingtreding van dit artikel. Deze periode duurt niet langer dan vijf jaar vanaf de bekendmaking ervan.

Artikel 55

Beroepsgeheim

1. Alle uit hoofde van deze verordening ontvangen, uitgewisselde of doorgegeven vertrouwelijke informatie valt onder de in lid 2 neergelegde voorwaarden inzake het beroepsgeheim.

2. Het beroepsgeheim geldt voor alle personen die werkzaam zijn of zijn geweest bij de krachtens deze verordening bevoegde autoriteiten, of voor elke autoriteit of onderneming op de markt, of natuurlijke of rechtspersoon aan wie de bevoegde autoriteit haar bevoegdheden heeft gedelegeerd, met inbegrip van de door deze autoriteiten aangestelde accountants en deskundigen.

3. Onder het beroepsgeheim vallende informatie, waaronder de uitwisseling van informatie tussen de bevoegde autoriteiten uit hoofde van deze verordening en de overeenkomstig Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten, wordt aan geen enkele andere persoon of autoriteit verstrekt, tenzij op grond van Unierechtelijke of nationaalrechtelijke bepalingen;

4. Alle uitwisseling van informatie tussen de bevoegde autoriteiten krachtens deze verordening die betrekking heeft op exploitatie- of bedrijfsomstandigheden en andere economische of persoonlijke zaken, wordt als vertrouwelijk beschouwd en valt onder de vereisten van het beroepsgeheim, tenzij de bevoegde autoriteit op het moment van de mededeling verklaart dat deze informatie kan worden bekendgemaakt of de bekendmaking ervan noodzakelijk is voor gerechtelijke procedures.

Artikel 56

Gegevensbescherming

1. De ETA's en de bevoegde autoriteiten mogen persoonsgegevens alleen verwerken wanneer dat nodig is voor het vervullen van hun respectieve verplichtingen en taken krachtens deze verordening, met name voor onderzoek, inspectie, verzoek om informatie, communicatie, bekendmaking, evaluatie, verificatie, beoordeling en opstelling van oversightplannen. De persoonsgegevens worden verwerkt overeenkomstig Verordening (EU) 2016/679 of Verordening (EU) 2018/1725, naargelang toepasselijk.

2. Tenzij in andere sectorale besluiten anders is bepaald, worden de in lid 1 bedoelde persoonsgegevens bewaard tot de vervulling van de toepasselijke toezichthoudende taken en in elk geval voor een periode van maximaal 15 jaar, behalve in het geval van lopende gerechtelijke procedures die verdere bewaring van dergelijke gegevens vereisen.

HOOFDSTUK VIII

Gedelegeerde handelingen

Artikel 57

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De bevoegdheid om de in artikel 31, lid 6, en artikel 43, lid 2, bedoelde gedelegeerde handelingen vast te stellen wordt aan de Commissie verleend voor een termijn van vijf jaar met ingang van 17 januari 2024. De Commissie stelt uiterlijk negen maanden voor het einde van de termijn van vijf jaar een verslag op over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie wordt stilzwijgend met termijnen van dezelfde duur verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen deze verlenging verzet.

3. Het Europees Parlement of de Raad kan de in artikel 31, lid 6, en artikel 43, lid 2, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een overeenkomstig artikel 31, lid 6, en artikel 43, lid 2, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van drie maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Deze termijn wordt op initiatief van het Europees Parlement of de Raad met drie maanden verlengd.

HOOFDSTUK IX

Overgangs- en slotbepalingen

Afdeling I

Artikel 58

Evaluatieclausule

1. Vanaf 17 januari 2028 voert de Commissie, na raadpleging van de ETA's en het ESRB, naargelang van het geval, een evaluatie uit en dient zij bij het Europees Parlement en de Raad een verslag in, in voorkomend geval vergezeld van een wetgevingsvoorstel. De evaluatie bevat ten minste het volgende:

a) de criteria voor de aanwijzing van kritieke derde aanbieders van ICT-diensten overeenkomstig artikel 31, lid 2;

b) het vrijwillige karakter van het melden van significante cyberdreigingen als bedoeld in artikel 19;

c) de in artikel 31, lid 12, bedoelde regeling en de bevoegdheden van de lead overseer als bedoeld in artikel 35, lid 1, punt d), iv), eerste streepje, met het oog op de evaluatie van de doeltreffendheid van die bepalingen met betrekking tot het waarborgen van doeltreffend oversight van kritieke derde aanbieders van ICT-diensten die in een derde land zijn gevestigd, en van de noodzaak om een dochteronderneming in de Unie op te richten.

   Voor de toepassing van de eerste alinea van dit punt omvat de evaluatie een analyse van de in artikel 31, lid 12, bedoelde regeling, met inbegrip van wat betreft de toegang van financiële entiteiten uit de Unie tot diensten uit derde landen en de beschikbaarheid van diensten op de markt van de Unie, en houdt zij rekening met verdere ontwikkelingen op de markten voor de onder deze verordening vallende diensten, de praktische ervaring van financiële entiteiten en financiële toezichthouders met betrekking tot de toepassing van en het toezicht op die regeling, en alle relevante ontwikkelingen op het gebied van regelgeving en toezicht die op internationaal niveau plaatsvinden.

d) de wenselijkheid om financiële entiteiten als bedoeld in artikel 2, lid 3, punt e), die gebruikmaken van geautomatiseerde verkoopsystemen, in het toepassingsgebied van deze verordening op te nemen in het licht van toekomstige marktontwikkelingen met betrekking tot het gebruik van dergelijke systemen;

e) de werking en doeltreffendheid van het JON bij het ondersteunen van de consistentie van het oversight en de efficiëntie van de uitwisseling van informatie binnen het toezichtkader.

2. In het kader van de herziening van Richtlijn (EU) 2015/2366 beoordeelt de Commissie of het nodig is de cyberweerbaarheid van betalingssystemen en betalingsverwerkingsactiviteiten te vergroten en of het passend is het toepassingsgebied van deze verordening uit te breiden tot exploitanten van betalingssystemen en entiteiten die betrokken zijn bij betalingsverwerkingsactiviteiten. In het licht van deze beoordeling legt de Commissie, bij de herziening van Richtlijn (EU) 2015/2366, uiterlijk op 17 juli 2023 een verslag voor aan het Europees Parlement en aan de Raad.

Op basis van dat evaluatieverslag en na raadpleging van de ETA's, de ECB en het ESRB kan de Commissie, in voorkomend geval en als onderdeel van het wetgevingsvoorstel dat zij krachtens artikel 108, tweede alinea, van Richtlijn (EU) 2015/2366 kan vaststellen, een voorstel indienen om ervoor te zorgen dat alle exploitanten van betalingssystemen en entiteiten die betrokken zijn bij betalingsverwerkingsactiviteiten aan passend oversight zijn onderworpen, rekening houdend met het bestaande oversight door de centrale banken.

3. Uiterlijk op 17 januari 2026, voert de Commissie, na raadpleging van de ETA's en het Comité van Europese auditorstoezichthouders, een evaluatie uit en dient zij een verslag in bij het Europees Parlement en de Raad dat, waar van toepassing, vergezeld gaat van een wetgevingsvoorstel over de geschiktheid van aangescherpte vereisten voor wettelijke auditors en auditkantoren wat betreft digitale operationele weerbaarheid, door wettelijke auditors en auditkantoren op te nemen in het toepassingsgebied van deze verordening, of door middel van wijzigingen van Richtlijn 2006/43/EG van het Europees Parlement en de Raad ([39]).

Afdeling II

Wijzigingen

Artikel 59

Wijzigingen van Verordening (EG) nr. 1060/2009

Verordening (EG) nr. 1060/2009 wordt als volgt gewijzigd:

1) in bijlage I, afdeling A, punt 4, wordt de eerste alinea vervangen door:

"Een ratingbureau beschikt over een goede administratieve en boekhoudkundige organisatie, adequate interne controleprocedures, effectieve risicobeoordelingsprocedures en effectieve controle- en beveiligingsvoorzieningen voor het beheer van ICT-systemen in overeenstemming met Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*) .

(*) 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 (PB L 333 van 27.12.2022, blz. 1).";

2) in bijlage III wordt punt 12 vervangen door:

"12. Het ratingbureau schendt artikel 6, lid 2, in samenhang met punt 4 van afdeling A van bijlage I, wanneer het niet beschikt over een goede administratieve of boekhoudkundige organisatie, interne controleprocedures, effectieve risicobeoordelingsprocedures of effectieve controle- of beveiligingsvoorzieningen voor het beheer van ICT-systemen in overeenstemming met Verordening (EU) 2022/2554 , of door niet de in dat punt vereiste besluitvormingsprocedures of organisatiestructuren te volgen en te handhaven.".

Artikel 60

Wijzigingen van Verordening (EU) nr. 648/2012

Verordening (EU) nr. 648/2012 wordt als volgt gewijzigd:

1) Artikel 26 wordt als volgt gewijzigd:

a) lid 3 wordt vervangen door:

"3. Een CTP beschikt over en werkt in het kader van een organisatiestructuur die de continuïteit en ordelijke werking bij het verrichten van haar diensten en activiteiten garandeert. Zij maakt gebruik van passende en evenredige systemen, middelen en procedures, met inbegrip van ICT-systemen die worden beheerd overeenkomstig Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*) .

(*) 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 (PB L 333 van 27.12.2022, blz. 1).";

([39]) Richtlijn 2006/43/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen, tot wijziging van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad en houdende intrekking van Richtlijn 84/253/EEG van de Raad (PB L 157 van 9.6.2006, blz. 87).

b) lid 6 wordt geschrapt;

2) artikel 34 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Een CTP zorgt voor de vaststelling, toepassing en instandhouding van een passend bedrijfscontinuïteitsbeleid en een noodherstelplan, dat ICT-bedrijfscontinuïteitsbeleid en ICT-respons- en herstelplannen omvat die zijn opgezet en worden uitgevoerd in overeenstemming met Verordening (EU) 2022/2554 , met als doel de functies van de CTP in stand te houden, de activiteiten tijdig te hervatten en de verplichtingen van de CTP na te komen.";

b) lid 3, eerste alinea, wordt vervangen door:

"3. Om een consistente toepassing van dit artikel te garanderen, stelt ESMA na overleg met de leden van het ESCB ontwerpen van technische reguleringsnormen op waarin de minimale inhoud en vereisten van het bedrijfscontinuïteitsbeleid en van het noodherstelplan worden gespecificeerd, met uitsluiting van ICT-bedrijfscontinuïteitsbeleid en noodherstelplannen.";

3) in artikel 56, lid 3, wordt de eerste alinea vervangen door:

"3. Om een consistente toepassing van dit artikel te garanderen, stelt ESMA ontwerpen van technische reguleringsnormen op tot bepaling van andere regels voor de in lid 1 vermelde registratieaanvraag dan die welke betrekking hebben op de vereisten inzake ICT-risicobeheer.";

4) in artikel 79 worden de leden 1 en 2 vervangen door:

"1. In een transactieregister worden bronnen van operationele risico's vastgesteld en tot een minimum beperkt via de ontwikkeling van passende systemen, controles en procedures, met inbegrip van ICT-systemen die worden beheerd in overeenstemming met Verordening (EU) 2022/2554.

2. Een transactieregister zorgt voor de opstelling, uitvoering en instandhouding van een passend bedrijfscontinuïteitsbeleid en noodherstelplan, met inbegrip van ICT-bedrijfscontinuïteitsbeleid en ICT-respons- en noodherstelplannen die zijn opgezet in overeenstemming met Verordening (EU) 2022/2554, met als doel de functies van het transactieregister in stand te houden, de activiteiten tijdig te hervatten en de verplichtingen van het transactieregister na te komen.";

5) in artikel 80 wordt lid 1 geschrapt;

6) bijlage I, afdeling II, wordt als volgt gewijzigd:

a) de punten a) en b) worden vervangen door:

"a) een transactieregister maakt inbreuk op artikel 79, lid 1, wanneer het bronnen van operationele risico's niet vaststelt of deze risico's niet tot een minimum beperkt door passende systemen, controles en procedures te ontwikkelen, met inbegrip van ICT-systemen die worden beheerd in overeenstemming met Verordening (EU) 2022/2554 ;

b) een transactieregister maakt inbreuk op artikel 79, lid 2, wanneer het niet zorgt voor de opstelling, uitvoering en instandhouding van een passend bedrijfscontinuïteitsbeleid en een noodherstelplan die zijn opgezet in overeenstemming met Verordening (EU) 2022/2554, met als doel de functies van het transactieregister in stand te houden, de activiteiten tijdig te hervatten en de verplichtingen van het transactieregister na te komen;";

b) punt c) wordt geschrapt;

7) bijlage III wordt als volgt gewijzigd:

a) afdeling II wordt als volgt gewijzigd:

i) punt c) wordt vervangen door:

"c) een tier 2-CTP maakt inbreuk op artikel 26, lid 3, als zij geen organisatiestructuur in stand houdt of exploiteert die de continuïteit en ordelijke werking bij de uitvoering van haar diensten en activiteiten waarborgt, of als zij geen gebruik maakt van passende en evenredige systemen, middelen of procedures, met inbegrip van ICT-systemen die worden beheerd overeenkomstig Verordening (EU) 2022/2554 ";

ii) punt f) wordt geschrapt;

b) in afdeling III wordt punt a) vervangen door:

"a) een tier 2-CTP maakt inbreuk op artikel 34, lid 1, wanneer zij niet zorgt voor de vaststelling, toepassing of handhaving van een passend bedrijfscontinuïteitsbeleid en respons- en herstelplan, die zijn opgezet overeenkomstig Verordening (EU) 2022/2554, die tot doel hebben de functies van de CTP in stand te houden, de activiteiten tijdig te hervatten, en de verplichtingen van de CTP na te komen, dat het ten minste mogelijk maakt dat alle transacties op het ogenblik van de verstoring worden hersteld, zodat de CTP haar bedrijfsactiviteiten met zekerheid kan voortzetten en de afwikkeling op de geplande datum kan voltooien;".

Artikel 61

Wijzigingen van Verordening (EU) nr. 909/2014

Artikel 45 van Verordening (EU) nr. 909/2014 wordt als volgt gewijzigd:

1) lid 1 wordt vervangen door:

"1. Een CSD identificeert bronnen van zowel intern als extern operationeel risico en beperkt de impact daarvan tot een minimum door het gebruik van passende IT-instrumenten, -controles en -procedures die worden opgezet en beheerd in overeenstemming met Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*) , alsmede via andere relevante passende instrumenten, controles en procedures voor andere soorten operationele risico's, inclusief voor alle effectenafwikkelingssystemen die zij exploiteert.

(*) 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 (PB L 333 van 27.12.2022, blz. 1).";

2) lid 2 wordt geschrapt;

3) de leden 3 en 4 worden vervangen door:

"3. Voor diensten die zij verricht en voor elk effectenafwikkelingssysteem dat zij exploiteert, draagt een CSD zorg voor het vaststellen, implementeren en aanhouden van een adequaat bedrijfscontinuïteitsbeleid en noodherstelplan, met inbegrip van ICT-bedrijfscontinuïteitsbeleid en ICT-respons en -herstelplannen die zijn opgezet overeenkomstig Verordening (EU) 2022/2554 , om te zorgen voor het behoud van haar diensten, het tijdig herstel van de bedrijfsactiviteiten en de vervulling van de verplichtingen van de CSD bij gebeurtenissen die een significant risico op verstoring van transacties inhouden.

4. Het in lid 3 bedoelde plan maakt het mogelijk alle transacties en posities van deelnemers op het ogenblik van de verstoring te herstellen, zodat de deelnemers aan een CSD hun bedrijvigheid met zekerheid kunnen voortzetten en de afwikkeling op de geplande datum kunnen uitvoeren, onder meer door ervoor te zorgen dat kritieke IT-systemen na de verstoring weer operationeel worden, zoals bepaald in artikel 12, leden 5 en 7, van Verordening (EU) 2022/2554.";

4) lid 6 wordt vervangen door:

"6. Een CSD is belast met het identificeren, monitoren en beheersen van de risico's die belangrijke deelnemers aan het effectenafwikkelingssysteem dat zij exploiteert alsook dienstverrichters en aanbieders van hulpprogramma's en andere CSD's of andere marktinfrastructuren voor haar bedrijfsactiviteiten kunnen inhouden. Zij verstrekt desgevraagd de bevoegde en de relevante autoriteiten informatie over eventuele geïdentificeerde risico's. Zij stelt de bevoegde autoriteit en de relevante autoriteiten ook onverwijld in kennis van andere operationele incidenten ten gevolge van deze risico's dan die welke betrekking hebben op ICT-risico's.";

5) lid 7, eerste alinea, wordt vervangen door:

"7. De ESMA ontwikkelt, in nauwe samenwerking met de leden van het ESCB, ontwerpen van technische reguleringsnormen tot nadere bepaling van de in de leden 1 en 6 bedoelde operationele risico's die geen ICT-risico zijn, en de methoden om die risico's te testen, aan te pakken of te beperken, met inbegrip van het bedrijfscontinuïteitsbeleid en de noodherstelplannen bedoeld in de leden 3 en 4 en de methoden om die te beoordelen.".

Artikel 62

Wijzigingen van Verordening (EU) nr. 600/2014

Verordening (EU) nr. 600/2014 wordt als volgt gewijzigd:

1) artikel 27 octies wordt als volgt gewijzigd:

a) lid 4 wordt vervangen door:

"4. Een APA voldoet aan de vereisten inzake de beveiliging van netwerk- en informatiesystemen van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*).

(*) 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 (PB L 333 van 27.12.2022, blz. 1).";

b) in lid 8 wordt punt c) vervangen door:

"c) de concrete organisatorische vereisten die zijn vastgelegd in de leden 3 en 5.";

2) artikel 27 novies wordt als volgt gewijzigd:

a) lid 5 wordt vervangen door:

"5. Een CTP voldoet aan de vereisten inzake de beveiliging van netwerk- en informatiesystemen van Verordening (EU) 2022/2554.";

b) in lid 8 wordt punt e) vervangen door:

"e) de concrete organisatorische vereisten die zijn vastgelegd in lid 4.";

3) artikel 27 decies wordt als volgt gewijzigd:

a) lid 3 wordt vervangen door:

"3. Een ARM voldoet aan de vereisten inzake de beveiliging van netwerk- en informatiesystemen van Verordening (EU) 2022/2554 .";

b) in lid 5 wordt punt b) vervangen door:

"b) de concrete organisatorische vereisten die zijn vastgelegd in de leden 2 en 4.".

Artikel 63

Wijziging van Verordening (EU) 2016/1011

Aan artikel 6 van Verordening (EU) 2016/1011 wordt het volgende lid toegevoegd:

"6. Een beheerder beschikt voor kritieke benchmarks over een goede administratieve en boekhoudkundige organisatie, adequate interne controleprocedures, effectieve risicobeoordelingsprocedures en effectieve controle- en beveiligingsvoorzieningen voor het beheer van ICT-systemen in overeenstemming met Verordening (EU) 2022/2554 van het Europees Parlement en de Raad (*).

(*) 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 (PB L 333 van 27.12.2022, blz. 1).".

Artikel 64

Inwerkingtreding en toepassing

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

Zij is van toepassing met ingang van 17 januari 2025.

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

Gedaan te Straatsburg, 14 december 2022.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
R. METSOLA	M. BEK