Europees Parlement
2019-2024

Zittingsdocument

A9-0341/2021

7.12.2021

***I
VERSLAG

over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht van de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Commissie economische en monetaire zaken

Rapporteur: Billy Kelleher

Verklaring van de gebruikte tekens

*	Raadplegingsprocedure
***	Goedkeuringsprocedure
***I	Gewone wetgevingsprocedure (eerste lezing)
***II	Gewone wetgevingsprocedure (tweede lezing)
***III	Gewone wetgevingsprocedure (derde lezing)

(De aangeduide procedure is gebaseerd op de in de ontwerptekst voorgestelde rechtsgrond.)

Amendementen op een ontwerphandeling

Amendementen van het Parlement in twee kolommen

Geschrapte tekstdelen worden in de linkerkolom in ***vet cursief*** aangegeven. Vervangen tekstdelen worden in beide kolommen in ***vet cursief*** aangegeven. Nieuwe tekst wordt in de rechterkolom in ***vet cursief*** aangegeven.

In de eerste en tweede regel van de koptekst boven elk amendement wordt verwezen naar het tekstdeel in kwestie van de ontwerphandeling. Indien een amendement betrekking heeft op een bestaande handeling, waarop in de ontwerphandeling wijzigingen worden voorgesteld, bevat de koptekst bovendien een derde en vierde regel, die verwijzen naar de bestaande handeling respectievelijk naar de bepaling in kwestie.

Amendementen van het Parlement in de vorm van een geconsolideerde tekst

Nieuwe tekstdelen worden in ***vet cursief*** aangegeven. Geschrapte tekstdelen worden aangegeven met het symbool ▌ of worden doorgestreept. Waar tekstdelen vervangen worden, wordt de nieuwe tekst in ***vet cursief*** aangegeven, terwijl de vervangen tekst wordt geschrapt of doorgestreept. Bij wijze van uitzondering worden zuiver technische wijzigingen die de diensten aanbrengen met het oog op de opstelling van de definitieve tekst, niet gemarkeerd.

INHOUD

Blz.

ONTWERPWETGEVINGSRESOLUTIE VAN HET EUROPEES PARLEMENT

over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht van de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Gewone wetgevingsprocedure: eerste lezing)

Het Europees Parlement,

– gezien het voorstel van de Commissie aan het Europees Parlement en de Raad (COM(2020)0595),

– gezien artikel 294, lid 2, en artikel 114 van het Verdrag betreffende de werking van de Europese Unie, op grond waarvan het voorstel door de Commissie bij het Parlement is ingediend (C9-0304/2020),

– gezien artikel 294, lid 3, van het Verdrag betreffende de werking van de Europese Unie,

– gezien het advies van het Europees Economisch en Sociaal Comité van 24 februari 2021[1],

– gezien artikel 59 van zijn Reglement,

– gezien het verslag van de Commissie economische en monetaire zaken (A9-0341/2021),

1. stelt onderstaand standpunt in eerste lezing vast;

2. verzoekt de Commissie om hernieuwde voorlegging aan het Parlement indien zij haar voorstel vervangt, ingrijpend wijzigt of voornemens is het ingrijpend te wijzigen;

3. verzoekt zijn Voorzitter het standpunt van het Parlement te doen toekomen aan de Raad en aan de Commissie alsmede aan de nationale parlementen.

[1] PB C 155 van 30.4.2021, blz. 38.

Amendement 1

AMENDEMENTEN VAN HET EUROPEES PARLEMENT*

op het voorstel van de Commissie

2020/0266(COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014

(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[2],

Gezien het advies van het Europees Economisch en Sociaal Comité,[3]

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) In het digitale tijdperk ondersteunt informatie- en communicatietechnologie (ICT) complexe systemen die worden gebruikt voor dagelijkse maatschappelijke activiteiten. ICT houdt belangrijke sectoren van onze economie draaiende, waaronder de financiële, en verbetert de werking van de eengemaakte markt. Meer digitalisering en onderlinge verwevenheid vergroten ook de ICT-risico's, 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 alle activiteiten van financiële entiteiten in de Unie,

---

* Amendementen: nieuwe of vervangende tekst staat in vet en cursief, schrappingen worden aangeduid met het symbool ▌.

2 [referentie invoegen] PB C van , blz. .

3 PB C 155 van 30.4.2021, blz. 38.

moet digitale veerkracht nog voldoende in hun operationele kaders worden ingebouwd.

(2) Het gebruik van ICT heeft in de afgelopen decennia een centrale rol gekregen in het geldwezen, zodat ICT nu van cruciaal belang is voor de werking van typische dagelijkse functies van alle financiële entiteiten. Digitalisering betreft bijvoorbeeld betalingen, die steeds minder met op contant geld en papier gebaseerde methoden 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. ***De verzekeringssector is ook getransformeerd door het gebruik van ICT-technologie, van de opkomst van digitale verzekeringstussenpersonen die met InsurTech werken tot digitale afsluiting van verzekeringen en contractdistributie.*** 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[4] 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 kan vormen, aangezien lokale cyberincidenten zich snel van elk van de ongeveer 22 000 financiële entiteiten van de Unie[5] zouden kunnen verspreiden naar het gehele financiële stelsel, niet gehinderd door geografische grenzen. Ernstige ICT-inbreuken die zich in het geldwezen 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, waardoor liquiditeitsruns en een algeheel verlies van vertrouwen in de financiële markten kunnen ontstaan.

(4) De laatste jaren hebben nationale, Europese en internationale beleidsmakers, toezichthouders en normalisatie-instellingen zich beziggehouden met ICT-risico's en is geprobeerd de veerkracht 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 G7 en G20 ernaar de bevoegde autoriteiten en marktdeelnemers in verschillende rechtsgebieden te voorzien

---

4 Verslag over systemisch cyberrisico van het ESRB van februari 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

5 Volgens de effectbeoordeling bij de evaluatie van de Europese toezichthoudende autoriteiten (SWD(2017) 308) zijn er ongeveer 5 665 kredietinstellingen, 5 934 beleggingsondernemingen, 2 666 verzekeringsondernemingen, 1 573 IBPV's, 2 500 beleggingsbeheermaatschappijen, 350 marktinfrastructuren (zoals CTP's, effectenbeurzen, beleggingsondernemingen met systematische interne afhandeling, transactieregisters en MTF's), 45 ratingbureaus en 2 500 vergunninghoudende betalingsinstellingen en instellingen voor elektronisch geld. Bij elkaar zijn dit ongeveer 21 233 entiteiten, waarbij crowdfundingentiteiten, wettelijke auditors en auditkantoren, aanbieders van cryptoactivadiensten en benchmarkbeheerders niet zijn meegeteld.

van instrumenten om de veerkracht van hun financiële stelsels op te vijzelen. ***Bijgevolg moeten ICT-risico's in aanmerking worden genomen in de context van een onderling zeer sterk verbonden mondiaal financieel stelsel waarin wereldwijd prioriteit moet worden gegeven aan de consistentie van de internationale regelgeving en de samenwerking tussen bevoegde autoriteiten.***

(5) Ondanks gerichte nationale en Europese beleids- en wetgevingsinitiatieven blijven ICT-risico's een uitdaging vormen voor de operationele veerkracht, prestaties en stabiliteit van het financiële stelsel van de Unie. De hervorming die volgde op de financiële crisis van 2008, heeft in de eerste plaats de financiële veerkracht van de financiële sector van de Unie versterkt en had als doel het concurrentievermogen en de stabiliteit van de Unie te waarborgen vanuit economisch, prudentieel en marktgedragsoogpunt. Hoewel ICT-beveiliging en digitale veerkracht deel uitmaken van operationeel risico, hebben zij in de regelgevingsagenda na de 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) Het FinTech-actieplan[6] van de Commissie van 2018 benadrukte dat het van het grootste belang is de financiële sector van de Unie weerbaarder te maken, ook 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 Bankautoriteit (EBA), de Europese Autoriteit voor effecten en markten (ESMA) en de Europese Autoriteit voor verzekeringen en bedrijfspensioenen (Eiopa) (samen "Europese toezichthoudende autoriteiten" of "ETA's" genoemd) gezamenlijk twee technische adviezen uitgebracht waarin werd opgeroepen tot een samenhangende aanpak van ICT-risico's in de financiële sector en werd aanbevolen om op evenredige wijze de digitale operationele veerkracht 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 geharmoniseerd gemeenschappelijk rulebook en is onderworpen aan een Europees systeem van financieel toezicht. Niettemin zijn de bepalingen inzake digitale operationele veerkracht en ICT-beveiliging nog niet volledig of consistent geharmoniseerd, hoewel digitale operationele veerkracht 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 deze component worden ontwikkeld, door het mandaat van de financiële toezichthouders ***te versterken*** om ***ICT-risico's in*** de financiële ***sector*** te beheersen en de integriteit ***en de efficiëntie van***

---

[6] Mededeling van de Commissie aan het Europees Parlement, de Raad, de Europese Centrale Bank, het Europees Economisch en Sociaal Comité en het Comité van de Regio's getiteld "FinTech-actieplan: voor een meer concurrerende en innovatieve Europese financiële sector" (COM(2018)0109 final https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52018DC0109&qid=1638981189065

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 ICT-risico leiden tot obstakels voor de eengemaakte markt voor financiële diensten die de vlotte uitoefening van de vrijheid van vestiging en het verlenen van diensten belemmeren voor financiële entiteiten met grensoverschrijdende aanwezigheid. De concurrentie tussen hetzelfde type financiële entiteiten in verschillende lidstaten kan ook worden verstoord. Met name op gebieden waar de harmonisatie op Unieniveau zeer beperkt is gebleven, zoals bij het testen van de digitale operationele veerkracht, of geheel ontbreekt, zoals bij het monitoren van ICT-risico's van derde aanbieders, zouden verschillen als gevolg van geplande ontwikkelingen op nationaal niveau verdere belemmeringen voor de werking van de eengemaakte 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, zijn op belangrijke gebieden – zoals het melden van ICT-gerelateerde incidenten en het testen van digitale operationele veerkracht – lacunes of overlappingen ontstaan, alsook inconsistenties als gevolg van uiteenlopende nationale regels of kostenineffici ënte 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 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 ICT-risico's moeten aanpakken en de negatieve gevolgen van ICT-incidenten moeten beperken.

(10 bis) Het opzetten en in stand houden van adequate infrastructuur voor netwerken en informatiesystemen is ook een fundamentele voorwaarde voor de effectieve samenvoeging van risicogegevens en effectieve risicorapportagepraktijken, die op hun beurt een essentiële voorwaarde vormen voor degelijke en duurzame procedures voor risicobeheer en besluitvorming door kredietinstellingen. Het Bazels Comité voor bankentoezicht (BCBS) heeft in 2013 een reeks beginselen gepubliceerd voor de effectieve aggregatie van risicogegevens en voor effectieve risicorapportage ("BCBS 239"), opgedeeld in twee overkoepelende categorieën: governance en IT-infrastructuur, die begin 2016 moesten zijn uitgevoerd. Overeenkomstig het verslag van de Europese Centrale Bank (ECB) van mei 2018 over de thematische evaluatie van effectieve risicogegevensaggregatie en risicorapportage van mei 2018 en het voortgangsverslag van het BCBS van april 2020 was de door mondiaal systeemrelevante banken geboekte vooruitgang bij de uitvoering onbevredigend en een bron van zorg. Ter bevordering van de naleving van en de afstemming op internationale normen moet de Commissie, in nauwe samenwerking met de ECB en na raadpleging van de EBA en het ESRB, een verslag opstellen met een beoordeling van de wisselwerking tussen de BCBS 239-beginselen en de bepalingen van deze

verordening, en, indien toepasselijk, hoe de BCBS 239-beginselen in het Unierecht moeten worden opgenomen.

(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 veerkracht voor alle financiële entiteiten geboden. De capaciteiten en algehele veerkracht die financiële entiteiten op basis van dergelijke essentiële vereisten zouden ontwikkelen om operationele storingen te weerstaan, zouden helpen 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 eengemaakte markt, moet zij gebaseerd zijn op de bepalingen van artikel 114 VWEU, geïnterpreteerd in overeenstemming met de vaste rechtspraak van het Hof van Justitie van de Europese Unie.

(12) Deze verordening is in de eerste plaats gericht op het consolideren en verbeteren van de vereisten inzake ICT-risico, die tot dusver afzonderlijk zijn behandeld in verschillende verordeningen en richtlijnen. Hoewel de belangrijkste categorieën financiële risico's (bv. kredietrisico, marktrisico, tegenpartijkredietrisico en liquiditeitsrisico, marktgedragrisico) in die rechtshandelingen van de Unie aan bod kwamen, was het ten tijde van de vaststelling ervan niet mogelijk alle componenten van operationele veerkracht te behandelen. In de vereisten inzake operationeel risico die in deze 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 ICT-risico's te dekken); er werden dus geen gerichte kwalitatieve vereisten vastgesteld om capaciteiten te versterken voor bescherming, opsporing, inperking, herstel en reparatie bij ICT-gerelateerde incidenten of voor rapportage en digitale tests. Die richtlijnen en verordeningen waren in de eerste plaats bedoeld om essentiële regels inzake prudentieel toezicht, marktintegriteit of marktgedrag vast te stellen.

Door middel van deze operatie, waarbij de regels inzake ICT-risico's worden geconsolideerd en bijgewerkt, worden alle bepalingen met betrekking tot digitaal risico in de financiële sector voor de eerste keer op consistente wijze in één wetgevingshandeling samengebracht. Dit initiatief moet dus in sommige van die rechtshandelingen leemten opvullen of inconsistenties wegnemen, ook wat betreft de daarin gebruikte terminologie, en expliciet naar ICT-risico verwijzen door middel van gerichte regels inzake ICT-risicobeheercapaciteiten, rapportage en tests en monitoring van het derdenrisico. ***Met dit initiatief wordt ook beoogd het bewustzijn van ICT-risico's te vergroten en wordt erkend dat ICT-incidenten en het gebrek aan operationele veerkracht de financiële gezondheid van financiële entiteiten in gevaar kunnen brengen.***

(13) Financiële entiteiten moeten, ***in overeenstemming met hun omvang, aard, complexiteit en risicoprofiel***, 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) Het gebruik van een verordening helpt de complexiteit van de regelgeving te verminderen, bevordert de convergentie van het toezicht en vergroot de rechtszekerheid, maar 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 veerkracht 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 sectoren van de Unie.

(14 bis) De uitvoering van deze verordening mag echter geen belemmering vormen voor innovatie met betrekking tot de manier waarop financiële entiteiten omgaan met problemen in verband met digitale operationele veerkracht bij de naleving van de bepalingen ervan, noch met betrekking tot de diensten die zij aanbieden, noch met betrekking tot de diensten die door derde ICT-dienstverleners worden aangeboden.

(15) Naast de wetgeving inzake financiële diensten is Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[7] het huidige algemene kader voor cyberbeveiliging op Unieniveau. In de zeven cruciale sectoren is die richtlijn ook van toepassing 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, worden 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.

(16) Aangezien deze verordening het niveau van harmonisatie op onderdelen van digitale veerkracht verhoogt door vereisten inzake ICT-risicobeheer en rapportage van ICT-gerelateerde incidenten in te voeren die strenger zijn dan die welke in de huidige Uniewetgeving inzake financiële diensten zijn opgenomen, is ook in vergelijking met de vereisten van Richtlijn (EU) 2016/1148 sprake van een grotere harmonisatie. Deze verordening is ***voor financiële entiteiten*** dus een lex specialis ten opzichte van Richtlijn (EU) 2016/1148.

Het is van cruciaal belang om een sterke relatie tussen de financiële sector en het horizontale cyberbeveiligingskader van de Unie te handhaven, ***teneinde*** te zorgen voor samenhang met de reeds door de lidstaten ingevoerde cyberbeveiligingsstrategieën, en financiële toezichthouders te kunnen wijzen op cyberincidenten die gevolgen hebben voor andere onder Richtlijn (EU) 2016/1148 vallende sectoren.

(17) Om een sectoroverschrijdend leerproces mogelijk te maken en daadwerkelijk gebruik

---

[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).

te maken van de ervaringen van andere sectoren bij de aanpak van cyberdreigingen, moeten de in Richtlijn (EU) 2016/1148 bedoelde financiële entiteiten deel blijven uitmaken van het "ecosysteem" van die richtlijn (bv. de NIS-samenwerkingsgroep en CSIRT's).

De ETA's en nationale bevoegde autoriteiten moeten in staat zijn deel te nemen aan respectievelijk de strategische beleidsdiscussies en de technische werkzaamheden van de NIS-samenwerkingsgroep, en daarnaast moeten zij in staat zijn informatie uit te wisselen en te blijven samenwerken met de krachtens Richtlijn (EU) 2016/1148 aangewezen centrale contactpunten. ***Het orgaan voor gezamenlijk toezicht, de leidende toezichthouders en de*** bevoegde autoriteiten in de zin van deze verordening moeten ook overleg plegen en samenwerken met de overeenkomstig artikel 9 van Richtlijn (EU) 2016/1148 aangewezen nationale CSIRT's.

Voorts moet met deze verordening worden gewaarborgd dat gedetailleerde informatie over ernstige ICT-gerelateerde incidenten wordt verstrekt aan het CSIRT-netwerk dat uit hoofde van Richtlijn (EU) 2016/1148 is tot stand gebracht.

(18) Het is ook belangrijk te zorgen voor consistentie met ***zowel*** de richtlijn betreffende Europese kritieke infrastructuur, die momenteel wordt herzien om kritieke infrastructuur beter te beschermen en weerbaarder te maken tegen niet-cybergerelateerde dreigingen, als ***de richtlijn betreffende de veerkracht van kritieke entiteiten***[8], met mogelijke gevolgen voor de financiële sector.

(19) Aanbieders van cloudcomputingdiensten zijn één van de categorieën digitaledienstverleners die onder Richtlijn (EU) 2016/1148 vallen. Als zodanig zijn zij onderworpen aan toezicht achteraf dat wordt verricht door de overeenkomstig die richtlijn aangewezen nationale autoriteiten en dat beperkt is tot de in die handeling vastgestelde vereisten inzake ICT-beveiliging en melding van incidenten. Aangezien het bij deze verordening vastgestelde toezichtkader van toepassing is op alle cruciale derde aanbieders van ICT-diensten, waaronder aanbieders van cloudcomputingdiensten, wanneer zij ICT-diensten aan financiële entiteiten verlenen, moet het als complementair aan het krachtens Richtlijn (EU) 2016/1148 verrichte toezicht worden beschouwd ***en moeten de materiële en procedurele vereisten die krachtens deze verordening op cruciale derde aanbieders van ICT-diensten van toepassing zijn, coherent zijn met en naadloos aansluiten op de vereisten die onder die richtlijn van toepassing zijn***. Bovendien moet het bij deze verordening vastgestelde toezichtkader betrekking hebben op aanbieders van cloudcomputingdiensten, gezien het ontbreken van een horizontaal sectoragnostisch kader van de Unie tot oprichting van een autoriteit voor digitaal toezicht.

(20) Om ICT-risico's volledig onder controle te houden, moeten financiële entiteiten beschikken over alomvattende capaciteiten die een krachtig en doeltreffend ICT-risicobeheer mogelijk maken, naast specifieke mechanismen en beleidsmaatregelen voor het melden van ICT-gerelateerde incidenten, het testen van ICT-systemen en het

[8] Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

beheren van het ICT-risico van derde aanbieders ***en aanbieders binnen de groep***. De lat voor de digitale operationele veerkracht van het financiële stelsel moet hoger worden gelegd, terwijl een evenredige toepassing van de vereisten mogelijk moet zijn, ***waarbij rekening wordt gehouden met hun aard, omvang, complexiteit en algemene risicoprofiel***.

(21) De drempels en taxonomieën voor de rapportage van ICT-gerelateerde incidenten variëren aanzienlijk op nationaal niveau. Hoewel via relevante werkzaamheden van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)[9] en de NIS-samenwerkingsgroep overeenstemming kan worden bereikt voor de onder Richtlijn (EU) 2016/1148 vallende financiële entiteiten, kunnen voor de overige financiële entiteiten verschillende benaderingen inzake drempels en taxonomieën bestaan of ontstaan. Dit brengt vele vereisten mee waaraan financiële entiteiten moeten voldoen, vooral wanneer zij in verschillende rechtsgebieden van de Unie actief zijn en wanneer zij deel uitmaken van een financiële groep. Bovendien kunnen deze 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 ICT-risico's in geval van grootschalige aanvallen met potentieel systemische gevolgen.

(21 bis) Teneinde de administratieve lasten te verminderen en complexiteit en overlappende rapportageverplichtingen voor de betalingsdienstaanbieders die onder deze verordening vallen te voorkomen, moeten de vereisten voor het melden van incidenten krachtens Richtlijn (EU) 2015/2366 niet langer van toepassing zijn. Als zodanig moeten kredietinstellingen, instellingen voor elektronisch geld en betalingsinstellingen uit hoofde van deze verordening alle betalingsgerelateerde en niet-betalingsgerelateerde operationele of beveiligingsincidenten melden die eerder op grond van Richtlijn (EU) 2015/2366 werden gemeld, ongeacht of de incidenten al dan niet ICT-gerelateerd zijn.

(22) Om de bevoegde autoriteiten in staat te stellen hun toezichthoudende rol te vervullen door een volledig overzicht te krijgen 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, moeten regels worden vastgesteld teneinde ***een robuuste*** regeling voor het melden van ICT-gerelateerde incidenten ***te verkrijgen*** met voorschriften waarmee ***tekortkomingen in de sectorale wetgeving*** inzake financiële diensten ***worden aangepakt***, en moeten bestaande overlappingen en doublures worden weggenomen om de kosten te verlichten. Het is daarom essentieel de regeling voor het melden van ICT-gerelateerde incidenten te harmoniseren door voor te schrijven dat alle financiële entiteiten aan hun bevoegde autoriteiten rapporteren ***door middel van één enkel gestroomlijnd kader zoals uiteengezet in deze verordening***. Daarnaast moeten de ETA's de bevoegdheid krijgen elementen van de rapportage van ICT-gerelateerde incidenten verder uit te werken, zoals taxonomie,

[9] ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

tijdschema's, datasets, modellen en toepasselijke drempels.

(23) In sommige financiële subsectoren zijn vereisten voor het testen van de digitale operationele veerkracht ontwikkeld binnen verschillende ***soms*** ongecoördineerde nationale kaders waarin dezelfde kwesties op verschillende manieren worden aangepakt. Dit leidt tot dubbele kosten voor grensoverschrijdende financiële entiteiten en zou de wederzijdse erkenning van resultaten ***kunnen belemmeren***. Ongecoördineerd testen kan de eengemaakte markt dus segmenteren.

(24) Bovendien blijven, wanneer testen niet vereist is, kwetsbaarheden onontdekt, waardoor de financiële entiteit en uiteindelijk de stabiliteit en integriteit van de financiële sector meer risico lopen. Zonder optreden van de Unie zou het testen van de digitale operationele veerkracht fragmentarisch blijven en zou er geen sprake zijn van wederzijdse erkenning van testresultaten tussen verschillende rechtsgebieden. Aangezien het onwaarschijnlijk is dat andere financiële subsectoren dergelijke regelingen op betekenisvolle schaal zouden invoeren, zouden zij ook de potentiële voordelen missen, zoals het onthullen van kwetsbaarheden en risico's, het testen van verdedigingscapaciteiten en bedrijfscontinuïteit en het groeiende vertrouwen van klanten, leveranciers en zakenpartners. Om dergelijke overlappingen, verschillen en leemten te verhelpen, moeten regels worden vastgesteld voor gecoördineerde tests door financiële entiteiten en bevoegde autoriteiten, zodat de wederzijdse erkenning van geavanceerde tests voor significante financiële entiteiten wordt vergemakkelijkt.

(25) Dat financiële entiteiten van ICT-diensten afhankelijk zijn, komt deels doordat zij zich moeten aanpassen aan een opkomende concurrerende digitale mondiale economie, hun bedrijfsefficiëntie moeten verbeteren en aan de vraag van de consument moeten voldoen. De aard en de omvang van die afhankelijkheid ontwikkelen zich de laatste jaren voortdurend, wat heeft geleid tot een daling van de kosten van financiële bemiddeling, en bedrijfsuitbreiding en schaalbaarheid bij de ontplooiing van financiële activiteiten mogelijk heeft gemaakt, terwijl een breed scala aan ICT-instrumenten wordt aangeboden om complexe interne processen te beheren.

(26) Dit grootschalige gebruik van ICT-diensten komt tot uiting in complexe contractuele regelingen, 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, wanneer deze laatste in de overeenkomsten zijn vastgelegd. Bovendien voorzien veel van dergelijke contracten niet in voldoende waarborgen om een volwaardige monitoring van onderaannemingsprocessen mogelijk te maken, zodat de financiële entiteit niet langer in staat is de hiermee gepaard gaande risico's te beoordelen. Aangezien derde aanbieders van ICT-diensten vaak gestandaardiseerde diensten aan verschillende soorten klanten aanbieden, houden dergelijke contracten ook niet altijd voldoende rekening met de individuele of specifieke behoeften van actoren uit de financiële sector.

(27) Hoewel sommige wetgevingshandelingen van de Unie op het gebied van financiële diensten enkele algemene voorschriften inzake uitbesteding bevatten, is de monitoring van de contractuele dimensie niet volledig in de wetgeving van de Unie verankerd. Door het ontbreken van duidelijke en op maat gemaakte Unienormen voor

contractuele regelingen met derde aanbieders van ICT-diensten wordt de externe bron van ICT-risico niet grondig aangepakt. Het is dan ook nodig bepaalde basisbeginselen vast te leggen die als leidraad moeten dienen voor het beheer van het ICT-risico van derde aanbieders door financiële entiteiten, alsook een reeks contractuele basisrechten met betrekking tot verschillende elementen van de uitvoering en beëindiging van contracten, teneinde bepaalde minimumwaarborgen vast te leggen ter ondersteuning van het vermogen van financiële entiteiten om alle risico's die zich voordoen in verband met ICT-diensten van derden, doeltreffend te monitoren.

(28) Er is een gebrek aan homogeniteit en convergentie met betrekking tot ICT-risico van derde aanbieders en afhankelijkheid van derden op ICT-gebied. Ondanks enige inspanningen om het specifieke gebied van uitbesteding aan te pakken, zoals de aanbevelingen van 2017 over uitbesteding aan aanbieders van clouddiensten[10], komt de kwestie van systeemrisico's die kunnen voortvloeien uit de blootstelling van de financiële sector aan een beperkt aantal cruciale aanbieders van ICT-diensten, in de wetgeving van de Unie nauwelijks aan de orde. Dit wordt nog verergerd door het ontbreken van specifieke mandaten en instrumenten die de nationale toezichthouders in staat stellen een goed inzicht te verwerven in afhankelijkheden van derden op ICT-gebied en de uit een concentratie van dergelijke afhankelijkheden voortvloeiende risico's adequaat te monitoren.

(29) Rekening houdend met de potentiële systeemrisico's die de toegenomen uitbesteding en de concentratie van ICT bij derden meebrengen, en met de ontoereikendheid van nationale mechanismen waarmee financiële toezichthouders de gevolgen van ICT-risico's bij cruciale derde aanbieders van ICT-diensten kunnen kwantificeren, kwalificeren en herstellen, moet een passend toezichtkader van de Unie tot stand worden gebracht om de activiteiten van derde aanbieders van ICT-diensten die ***cruciale diensten*** aan financiële entiteiten verlenen, voortdurend te kunnen monitoren. ***Aangezien binnen een groep verleende ICT-diensten niet dezelfde risico's met zich meebrengen, moeten dienstverleners die van dezelfde groep of hetzelfde institutionele protectiestelsel deel uitmaken niet als cruciale derde aanbieders van ICT-diensten worden gedefinieerd.***

(30) Nu ICT-dreigingen steeds complexer en geavanceerder worden, zijn goede opsporings- en preventiemaatregelen in grote mate afhankelijk van regelmatige uitwisseling van informatie over bedreigingen en kwetsbaarheden tussen financiële entiteiten. Informatie-uitwisseling draagt bij tot een groter bewustzijn van cyberdreigingen, wat er op zijn beurt voor zorgt dat financiële entiteiten beter in staat zijn te voorkomen dat dreigingen werkelijkheid worden, en de gevolgen van ICT-gerelateerde incidenten kunnen beperken en efficiënter kunnen herstellen. Bij gebrek aan 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. ***Het is derhalve belangrijk om de samenwerkingsregelingen en rapportage tussen financiële entiteiten en de bevoegde autoriteiten alsook de informatie-uitwisseling met het publiek te versterken, teneinde een open kader voor***

[10] Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), inmiddels ingetrokken bij de EBA-richtsnoeren inzake uitbesteding (EBA/GL/2019/02).

informatie-uitwisseling en een "beveiliging door ontwerp"-aanpak te ontwikkelen, die van essentieel belang zijn om de operationele veerkracht en paraatheid van de financiële sector met betrekking tot ICT-risico's te vergroten. In regelingen voor informatie-uitwisseling moet altijd terdege rekening worden gehouden met mogelijke risico's in verband met cyberveiligheid, gegevensbescherming of bedrijfsgeheimen.

(31) 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 omvang en de kwaliteit van informatie-uitwisseling blijven 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 geïntegreerde financiële sector. ***Daarom is het belangrijk deze communicatiekanalen te versterken en gedurende de gehele toezichtcyclus, indien nodig en relevant, te beschikken over input van niet-toezichthoudende autoriteiten.***

(32) Financiële entiteiten moeten derhalve worden aangemoedigd hun individuele kennis en praktische ervaring op strategisch, tactisch en operationeel niveau collectief te benutten om beter in staat te zijn cyberdreigingen adequaat te beoordelen, te monitoren, af te weren en aan te pakken. Op Unieniveau moeten dus mechanismen voor vrijwillige informatie-uitwisseling mogelijk worden gemaakt die, wanneer zij in vertrouwde omgevingen worden uitgevoerd, de financiële gemeenschap zouden helpen dreigingen te voorkomen en collectief aan te pakken door de verspreiding van ICT-risico's snel te beperken en mogelijke besmetting via de financiële kanalen te verhinderen. Die mechanismen moeten worden uitgevoerd met volledige inachtneming van de toepasselijke mededingingsregels van de Unie[11] en op een wijze die de volledige naleving van de gegevensbeschermingsregels van de Unie garandeert, met name Verordening (EU) 2016/679 van het Europees Parlement en de Raad[12], vooral 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.

(33) Ondanks de brede dekking waarin deze verordening voorziet, moet bij de toepassing van de regels inzake digitale operationele veerkracht, waaronder de voorschriften van het kader voor ICT-risicobeheer, rekening worden gehouden met aanzienlijke verschillen tussen financiële entiteiten qua omvang, ***aard, complexiteit en 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, ***aard, complexiteit, bedrijfsprofiel en relatief risicoprofiel***, terwijl de

---

11 Mededeling van de Commissie "Richtsnoeren inzake de toepasselijkheid van artikel 101 van het Verdrag betreffende de werking van de Europese Unie op horizontale samenwerkingsovereenkomsten" (PB C 11 van 14.1.11, blz. 1).

12 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).

bevoegde autoriteiten de daarbij gehanteerde benadering moeten blijven beoordelen en evalueren.

(34) Aangezien grotere financiële entiteiten doorgaans over meer middelen beschikken en die middelen snel 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 zijn 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 personeelsdocument op te stellen waarin het beleid inzake toegangsrechten uitvoerig wordt toegelicht.

Evenzo moet het alleen voor dergelijke financiële entiteiten verplicht worden diepgaande evaluaties uit te voeren na grote veranderingen in de infrastructuur en processen van het netwerk en het informatiesysteem, regelmatig risicoanalyses met betrekking tot hun bestaande ICT-systemen uit te voeren en in de testplannen voor bedrijfscontinuïteit en respons en herstel scenario's op te nemen voor de omschakeling tussen de primaire ICT-infrastructuur en de reservefaciliteiten.

(35) Aangezien alleen die financiële entiteiten die voor geavanceerde tests op digitale veerkracht als significant worden beschouwd, verplicht moeten zijn om dreigingsgestuurde penetratietests uit te voeren, moeten bovendien de administratieve processen en de financiële kosten die de uitvoering van dergelijke tests meebrengt, worden afgewenteld op een klein percentage van de financiële entiteiten. Tot slot moet, om de regeldruk te verlichten, alleen aan andere financiële entiteiten dan micro-ondernemingen worden gevraagd om regelmatig aan de bevoegde autoriteiten verslag uit te brengen over alle ***geraamde*** kosten en verliezen als gevolg van ***aanzienlijke*** ICT-verstoringen, over ***ernstige ICT-gerelateerde incidenten*** en over de resultaten van post-incidentenevaluaties na ***dergelijke*** ICT-verstoringen.

(36) Om te zorgen voor volledige afstemming en algehele samenhang tussen de bedrijfsstrategieën van financiële entiteiten enerzijds en de uitvoering van ICT-risicobeheer anderzijds, moet het leidinggevend orgaan verplicht zijn 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 veerkracht. De door het leidinggevend orgaan te volgen aanpak moet niet alleen gericht zijn op middelen om de veerkracht van de ICT-systemen te waarborgen, maar ook op personen en processen. Daarvoor dient een reeks beleidsmaatregelen die op elke bedrijfslaag 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.

De uiteindelijke verantwoordelijkheid van het leidinggevend orgaan voor het beheer van de ICT-risico's van een financiële entiteit moet een overkoepelend beginsel van die alomvattende aanpak zijn, dat verder tot uiting komt in een voortdurende betrokkenheid van het leidinggevend orgaan bij de controle van de monitoring van het ICT-risicobeheer.

(37) Volledige verantwoordingsplicht van het leidinggevend orgaan betekent bovendien dat

moet worden gezorgd voor voldoende ICT-investeringen en budget, zodat de financiële entiteit haar basisniveau van digitale operationele veerkracht kan bereiken.

(38) Deze verordening, die geïnspireerd is op relevante internationale, nationale en door de sector vastgestelde normen, richtsnoeren, aanbevelingen en benaderingen ten aanzien van het beheer van cyberrisico's[13], bevordert een reeks functies die de algemene structurering van het ICT-risicobeheer vergemakkelijken. Zolang de belangrijkste door financiële entiteiten gecreëerde capaciteiten voorzien in de behoeften in verband met de doelstellingen van de in deze verordening beschreven functies (identificatie, bescherming en voorkoming, detectie, respons en herstel, scholing en ontwikkeling en communicatie), staat het de financiële entiteiten vrij om anders opgezette of gecategoriseerde modellen voor ICT-risicobeheer te gebruiken.

(39) Om gelijke tred te houden met ontwikkelingen in het cyberdreigingslandschap, moeten financiële entiteiten geactualiseerde ICT-systemen in stand houden die betrouwbaar zijn en over voldoende capaciteit beschikken om niet alleen de gegevensverwerking te garanderen die nodig is in het kader van hun dienstverlening, maar om ook te zorgen voor technologische veerkracht, zodat zij adequaat kunnen inspelen op extra verwerkingsbehoeften die door gespannen marktomstandigheden of andere ongunstige situaties kunnen ontstaan. Deze verordening brengt geen normalisatie van specifieke ICT-systemen, -instrumenten of -technologieën mee maar vertrouwt op een passend gebruik door financiële entiteiten van Europese en internationaal erkende technische normen (bv. ISO) of beste praktijken in de sector, voor zover dit gebruik volledig strookt met specifieke instructies van de toezichthouder voor het gebruik en de integratie van internationale normen.

(40) Efficiënte bedrijfscontinuïteits- en herstelplannen zijn nodig om financiële entiteiten in staat te stellen snel een oplossing te vinden voor ICT-gerelateerde incidenten, met name cyberaanvallen, door de schade te beperken en prioriteit te geven aan de hervatting van activiteiten en aan herstelmaatregelen, ***rekening houdend met de vraag of het om een cruciale of belangrijke functie gaat***. Backupsystemen moeten onverwijld starten met de verwerking, maar hierdoor mogen in geen geval de integriteit en de beveiliging van het netwerk en van de informatiesystemen of de vertrouwelijkheid van gegevens in gevaar komen.

(41) Hoewel deze verordening financiële entiteiten toestaat op flexibele wijze hersteltijddoelstellingen vast te stellen en daarbij dus ten volle rekening kan worden gehouden met de aard en het cruciale karakter van de betrokken functie en met eventuele specifieke bedrijfsbehoeften, moet bij het vaststellen van dergelijke doelstellingen toch ook het mogelijke algemene effect op de marktefficiëntie worden geëvalueerd.

(42) De aanzienlijke gevolgen van cyberaanvallen worden versterkt wanneer zij zich voordoen in de financiële sector, die veel meer risico loopt het doelwit te worden van

---

[13] CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf G7 Fundamental Elements of Cybersecurity for the Financial Sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB CIRR toolkit, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

kwaadwilligen die rechtstreeks aan de bron op zoek zijn naar financieel gewin. Om dergelijke risico's te beperken en te voorkomen dat ICT-systemen aan integriteit inboeten of onbeschikbaar worden en dat inbreuk wordt gemaakt op vertrouwelijke gegevens of fysieke ICT-infrastructuur wordt beschadigd, moet de rapportage van ernstige ICT-gerelateerde incidenten door financiële entiteiten aanzienlijk worden verbeterd.

De rapportage van ICT-gerelateerde incidenten moet voor alle financiële entiteiten worden geharmoniseerd door hen te verplichten alleen aan hun bevoegde autoriteiten te rapporteren. Hoewel deze rapportageverplichting voor alle financiële entiteiten zou gelden, zouden deze niet allemaal op dezelfde wijze worden getroffen, aangezien materialiteitsdrempels en termijnen zodanig moeten worden afgestemd dat alleen ernstige ICT-gerelateerde incidenten worden gemeld. Directe rapportage zou financiële toezichthouders toegang geven tot informatie over ICT-gerelateerde incidenten. Niettemin moeten financiële toezichthouders deze informatie doorgeven aan niet-financiële overheidsinstanties (voor NIS bevoegde autoriteiten, nationale gegevensbeschermingsautoriteiten en rechtshandhavingsinstanties voor incidenten van criminele aard). De informatie over ICT-gerelateerde incidenten moet onderling worden gedeeld: de financiële toezichthouders moeten de financiële entiteit alle nodige feedback of richtsnoeren geven, terwijl de ETA's geanonimiseerde gegevens over dreigingen en kwetsbaarheden in verband met een gebeurtenis moeten delen met het oog op een bredere collectieve verdediging.

(43) Er moet verder worden nagedacht over mogelijke centralisatie van rapporten over ICT-gerelateerde incidenten in de vorm van een centrale ICT-hub ***voor de melding van ICT-gerelateerde incidenten***, die ofwel de desbetreffende rapporten rechtstreeks ontvangt en de nationale bevoegde autoriteiten daarvan automatisch in kennis stelt, ofwel slechts de door de nationale bevoegde autoriteiten doorgezonden rapporten centraal bewaart en een coördinerende rol vervult. De ETA's moeten ertoe worden verplicht om uiterlijk op een bepaalde datum in overleg met de ECB en het Enisa een gezamenlijk verslag op te stellen waarin wordt nagegaan of het haalbaar is een dergelijke centrale EU-hub op te richten.

(44) Om een robuuste digitale operationele veerkracht te bereiken, en in overeenstemming met internationale normen (bv. de fundamentele elementen van de G7 voor dreigingsgestuurde penetratietests), moeten financiële entiteiten, ***die geen micro-ondernemingen zijn***, hun ICT-systemen en personeel regelmatig testen met betrekking tot de doeltreffendheid van hun preventie-, detectie-, respons- en herstelcapaciteiten, om potentiële ICT-kwetsbaarheden aan het licht te brengen en aan te pakken. Om in te spelen op verschillen tussen en binnen de financiële subsectoren met betrekking tot de paraatheid van financiële entiteiten op het gebied van cyberbeveiliging, moeten de tests een breed scala aan instrumenten en acties omvatten, variërend van een beoordeling van de basisvereisten (bv. kwetsbaarheidsbeoordelingen en -scans, open-sourceanalyses, netwerkbeveiligingsbeoordelingen, kloofanalyses, fysieke beveiligingsonderzoeken, vragenlijsten en scanningsoftwareoplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests of eind-tot-eindtests) tot geavanceerdere tests (bv. dreigingsgestuurde penetratietests voor financiële entiteiten die vanuit ICT-perspectief

volwassen genoeg zijn om zulke tests uit te voeren). Het testen van de digitale operationele veerkracht moet dus strenger zijn voor belangrijke financiële entiteiten (zoals grote kredietinstellingen, effectenbeurzen, centrale effectenbewaarinstellingen, centrale tegenpartijen, enz.). Tegelijkertijd moet het testen van digitale operationele veerkracht ook relevanter zijn voor sommige subsectoren die een cruciale systemische rol spelen (bv. betalingen, bankwezen, clearing en afwikkeling) en minder relevant voor andere subsectoren (bv. vermogensbeheerders, ratingbureaus enz.). Grensoverschrijdende financiële entiteiten die hun vrijheid van vestiging of dienstverrichting binnen de Unie uitoefenen, moeten in hun lidstaat van herkomst voldoen aan één reeks geavanceerde testvereisten (bv. dreigingsgestuurde penetratietests), en die test moet de ICT-infrastructuur omvatten in alle rechtsgebieden waar de grensoverschrijdende groep binnen de Unie actief is, zodat grensoverschrijdende groepen in slechts één rechtsgebied testkosten hoeven te maken. ***Teneinde de samenwerking met betrouwbare derde landen op het gebied van veerkracht van financiële entiteiten te versterken, moeten de Commissie en de bevoegde autoriteiten trachten een kader voor de wederzijdse erkenning van de resultaten van dreigingsgestuurde penetratietests (TLPT) instellen.***

De lidstaten moeten één enkele overheidsinstantie aanwijzen die op nationaal niveau verantwoordelijk is voor TLPT in de financiële sector. De enkele overheidsinstantie kan onder meer een nationale bevoegde autoriteit zijn, of een overheidsinstantie die is aangewezen overeenkomstig artikel 8 van Richtlijn (EU) 2016/1148 (NIS). De enkele overheidsinstantie moet verantwoordelijk zijn voor het afgeven van attesten dat TLPT in overeenstemming met de voorschriften is uitgevoerd. Dergelijke verklaringen moeten de wederzijdse erkenning van tests door de bevoegde autoriteiten vergemakkelijken.

Sommige financiële entiteiten hebben de capaciteit om interne geavanceerde tests uit te voeren, terwijl andere entiteiten externe testers uit de Unie of uit een derde land zullen contracteren. Daarom is het belangrijk dat alle testers aan dezelfde duidelijke voorschriften worden onderworpen. Om de onafhankelijkheid van interne testers te waarborgen, is voor het gebruik van interne testers de goedkeuring van de bevoegde autoriteit vereist.

De methode voor TLPT moet niet verplicht worden gesteld, maar het gebruik van het bestaande TIBER-EU-kader moet worden geacht in overeenstemming te zijn met de in deze verordening vastgestelde TLPT-voorschriften.

Tot de inwerkingtreding van deze verordening en de aan de ETA's opgedragen ontwikkeling en vaststelling van de technische reguleringsnormen inzake TLPT, moeten de financiële entiteiten de toepasselijke Unierichtsnoeren en -kaders voor op inlichtingen gebaseerde penetratietests volgen, aangezien deze na de inwerkingtreding van de verordening van toepassing blijven.

(44 bis) ***De verantwoordelijkheid voor de uitvoering van TLPT — en voor het beheer van cyberveiligheid in het algemeen en de preventie van cyberaanvallen — moet volledig bij de financiële entiteit blijven berusten, en door de autoriteiten verstrekte attesten mogen uitsluitend dienen voor wederzijdse erkenning en mogen geen beletsel vormen voor eventuele follow-upmaatregelen met betrekking tot de omvang van het ICT-risico waaraan de financiële entiteit is blootgesteld, noch worden gezien***

als een bevestiging van haar vermogen om ICT-risico's te beheren en te beperken.

(45) Om te zorgen voor een degelijke monitoring van het ICT-risico van derde aanbieders, moet een reeks op beginselen gebaseerde regels worden vastgesteld voor de monitoring door financiële entiteiten van risico's die zich voordoen in de context van aan derde aanbieders van ICT-diensten uitbestede taken, ***met name wat betreft de voorziening van cruciale of belangrijke functies door derde aanbieders van ICT-diensten***, en, meer in het algemeen, in de context van ICT-afhankelijkheid van derden.

(46) Een financiële entiteit moet te allen tijde volledig verantwoordelijk blijven voor de naleving van de verplichtingen uit hoofde van deze verordening. Een evenredige monitoring van risico's die zich voordoen op het niveau van de derde aanbieder van ICT-diensten, moet worden georganiseerd door terdege rekening te houden met de ***aard***, de omvang, de complexiteit en het belang van ICT-gerelateerde afhankelijkheden, het cruciale karakter of het belang van de diensten, processen of functies die onder de contractuele regelingen vallen, en moet uiteindelijk gebaseerd zijn op een zorgvuldige beoordeling van de mogelijke impact op de continuïteit en kwaliteit van financiële diensten op individueel en groepsniveau, naargelang het geval, e***n op de vraag of de ICT-diensten worden verleend door een aanbieder van ICT-diensten binnen de groep of een derde aanbieder van diensten***.

(47) De uitvoering van deze monitoring moet een strategische benadering van het ICT-risico van derde aanbieders volgen, die wordt geformaliseerd doordat het leidinggevend orgaan van de financiële entiteit een specifieke strategie goedkeurt die is gebaseerd op een voortdurende screening van alle ICT-afhankelijkheden van derden. Om ervoor te zorgen dat toezichthouders zich beter bewust zijn van ICT-afhankelijkheden van derden, en om het bij deze verordening ingestelde toezichtkader verder te ondersteunen, moeten financiële toezichthouders regelmatig essentiële informatie uit de registers ontvangen en op ad-hocbasis uittreksels daarvan kunnen opvragen.

(48) Aan de formele sluiting van contractuele regelingen moet een grondige precontractuele analyse ten grondslag liggen, terwijl er corrigerende en herstelmaatregelen, zoals de beëindiging van contracten, moeten worden genomen in geval van ten minste een reeks omstandigheden die tekortkomingen bij de derde aanbieder van ICT-diensten aantonen.

(49) Om de systeemeffecten van het risico van concentratie van ICT bij derden aan te pakken, moet de voorkeur worden gegeven aan een evenwichtige oplossing via een flexibele en geleidelijke aanpak, aangezien starre plafonds of strikte beperkingen de bedrijfsvoering en de contractuele vrijheid kunnen belemmeren. Financiële entiteiten moeten contractuele regelingen grondig beoordelen om na te gaan hoe groot de kans is dat een dergelijk risico zich zal voordoen, onder meer door middel van diepgaande analyses van onderaanbestedingsovereenkomsten ▌. Om een billijk evenwicht te vinden tussen het behoud van de contractuele vrijheid en de waarborging van de financiële stabiliteit, wordt het op dit ogenblik niet wenselijk geacht te voorzien in strikte plafonds en beperkingen voor ICT-blootstellingen aan derden. ***Het orgaan voor gezamenlijk toezicht*** dat toezicht houdt op elke cruciale derde aanbieder van ICT-diensten ***en de ETA die is aangewezen voor het dagelijkse toezicht*** ("de leidende toezichthouder"), moeten bij de uitoefening van toezichtstaken bijzondere aandacht

besteden aan het verkrijgen van een volledig inzicht in de omvang van de onderlinge afhankelijkheden en het ontdekken van de specifieke gevallen waarin een hoge mate van concentratie van cruciale 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 zij moeten, wanneer dat risico wordt vastgesteld, voorzien in een dialoog met cruciale derde aanbieders van ICT-diensten[14].

(50) Om het vermogen van de derde aanbieder van ICT-diensten om veilig diensten aan de financiële entiteit te verlenen zonder nadelige gevolgen voor de veerkracht van deze entiteit, regelmatig te kunnen evalueren en monitoren, moet harmonisatie plaatsvinden van de belangrijkste contractuele elementen in de hele uitvoering van contracten met derde aanbieders van ICT-diensten. Die elementen hebben alleen betrekking op contractuele minimumaspecten die cruciaal worden geacht om een volledige monitoring door de financiële entiteit mogelijk te maken met het oog op de waarborging van haar digitale veerkracht die berust op de stabiliteit en veiligheid van de ICT-dienst.

(51) Contractuele regelingen moeten met name voorzien in een specificatie van volledige beschrijvingen van functies en diensten, van locaties waar dergelijke functies worden verstrekt en gegevens worden verwerkt, alsook in een indicatie van beschrijvingen van volledige dienstverlening vergezeld van kwantitatieve en kwalitatieve prestatiedoelen met overeengekomen dienstverleningsniveaus om doeltreffende monitoring door de financiële entiteit mogelijk te maken. In dezelfde geest moeten bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens, alsook garanties voor toegang, herstel en teruggave in geval van insolventie, afwikkeling of stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten ***of beëindiging van de contractuele regelingen*** worden beschouwd als essentiële elementen voor het vermogen van een financiële entiteit om te zorgen voor de monitoring van het derdenrisico.

(52) Om ervoor te zorgen dat financiële entiteiten de volledige controle behouden over alle ontwikkelingen die hun ICT-beveiliging in het gedrang kunnen brengen, moeten kennisgevingstermijnen en rapportageverplichtingen van de derde aanbieder van ICT-diensten worden opgenomen in geval van ontwikkelingen met mogelijke materiële impact op het vermogen van de derde aanbieder van ICT-diensten om cruciale of belangrijke functies doeltreffend uit te voeren, inclusief het verlenen van bijstand door laatstgenoemde in geval van een ICT-gerelateerd incident ***in verband met de diensten die de derde aanbieder van ICT-diensten aan de financiële instelling op overeengekomen dienstverleningsniveaus verleent***, zonder dat extra kosten worden aangerekend, of tegen vooraf vastgestelde kosten. ***ICT-gerelateerde nevendiensten waarvan de financiële entiteiten niet operationeel afhankelijk zijn, vallen niet onder deze verordening.***

Voorts moet de definitie van "cruciale of belangrijke functie" in deze verordening de definitie omvatten van "kritieke functies" als bedoeld in artikel 2, lid 1, punt 35, van

[14] Voorts moeten financiële entiteiten, wanneer zich het risico van misbruik door een als dominant beschouwde derde aanbieder van ICT-diensten voordoet, de mogelijkheid hebben om een formele of informele klacht in te dienen bij de Europese Commissie of de nationale mededingingsautoriteiten.

Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014[15]***. Dienovereenkomstig moeten kritieke functies in de zin van Richtlijn 2014/59/EU worden geacht cruciale of belangrijke functies in de zin van deze verordening te zijn.***

(53) ***In het geval van contractuele regelingen voor cruciale of belangrijke functies***, zijn rechten van toegang, inspectie en audit door de financiële entiteit of een aangewezen derde 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 laatstgenoemde tijdens inspecties. Evenzo moeten het ***orgaan voor gezamenlijk toezicht en de leidende toezichthouder*** van de financiële entiteit die rechten hebben om, na kennisgeving, de derde aanbieder van ICT-diensten te inspecteren en auditen, onder het voorbehoud van vertrouwelijkheid ***en met de nodige voorzichtigheid teneinde de dienstverlening aan andere klanten van de derde aanbieder van ICT-diensten niet te verstoren***. ***De financiële entiteit en de derde aanbieder van ICT-diensten moeten kunnen overeenkomen dat het recht op toegang, inspectie en audit aan een onafhankelijke derde kan worden gedelegeerd.***

(54) Contractuele regelingen moeten voorzien in duidelijke beëindigingsrechten en bijbehorende minimale opzegtermijnen alsook specifieke exitstrategieën die met name verplichte overgangsperioden mogelijk maken waarin de derde aanbieders van ICT-diensten de relevante functies moeten blijven verrichten om het risico op verstoringen op het niveau van de financiële entiteit te beperken of de financiële entiteit in staat te stellen daadwerkelijk over te stappen naar andere derde aanbieders van ICT-diensten, of anders gebruik te maken van interne oplossingen, in overeenstemming met de complexiteit van de verleende dienst. ***Bovendien moeten kredietinstellingen ervoor zorgen dat de relevante ICT-contracten degelijk en volledig afdwingbaar zijn in geval van afwikkeling van de kredietinstelling. In overeenstemming met de verwachtingen van de afwikkelingsautoriteiten moeten kredietinstellingen ervoor zorgen dat de relevante contracten voor ICT-diensten afwikkelingsbestendig zijn. Zo lang er nog cruciale of belangrijke ICT-functies worden uitgevoerd, moeten die financiële entiteiten ervoor zorgen dat de contracten, naast andere vereisten, bedingen bevatten op basis waarvan zij niet kunnen worden beëindigd, opgeschort en gewijzigd op grond van herstructurering of afwikkeling.***

(55) Bovendien kan het vrijwillige gebruik van door de Commissie ontwikkelde modelcontractbepalingen voor cloudcomputingdiensten de financiële entiteiten en hun derde aanbieders van ICT-diensten meer zekerheid bieden door de rechtszekerheid over het gebruik van cloudcomputingdiensten door de financiële sector te vergroten, in volledige overeenstemming met de vereisten en verwachtingen van de regelgeving inzake financiële diensten. Deze werkzaamheden bouwen voort op maatregelen die al

---

15 ***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).***

waren gepland in het FinTech-actieplan van 2018, waarin het voornemen van de Commissie werd 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.

(55 bis) De ETA's moeten worden belast met de opstelling van technische uitvoeringsnormen en regelgevingsnormen waarin de verwachtingen worden gespecificeerd van het beleid inzake het beheer van ICT-risico's van derde aanbieders en inzake contractuele vereisten. Tot de inwerkingtreding van die normen moeten financiële entiteiten de relevante richtsnoeren en andere maatregelen van de ETA's en bevoegde autoriteiten volgen.

(56) Om de convergentie en efficiëntie met betrekking tot toezichtsbenaderingen van het ICT-risico van derde aanbieders voor de financiële sector te bevorderen, de digitale operationele veerkracht te versterken van financiële entiteiten die voor de uitvoering van operationele taken afhankelijk zijn van cruciale derde aanbieders van ICT-diensten, en zo bij te dragen aan het behoud van de stabiliteit van het financiële stelsel van de Unie en de integriteit van de eengemaakte markt voor financiële diensten, moeten cruciale derde aanbieders van ICT-diensten onderworpen zijn aan een toezichtkader van de Unie.

(57) Aangezien een speciale behandeling alleen gerechtvaardigd is voor cruciale derde aanbieders van ICT-diensten, moet een aanwijzingsmechanisme voor de toepassing van het toezichtkader van de Unie worden ingesteld om rekening te houden met de omvang en de aard van de afhankelijkheid van de financiële sector ten aanzien van dergelijke derde aanbieders van ICT-diensten, hetgeen zich vertaalt in een reeks kwantitatieve en kwalitatieve criteria met parameters om het cruciale karakter vast te stellen waarmee rekening wordt gehouden in het toezichtkader. Cruciale derde aanbieders van ICT-diensten die niet automatisch worden aangewezen op grond van de toepassing van bovengenoemde criteria, moeten de mogelijkheid hebben vrijwillig aan het toezichtkader deel te nemen, terwijl derde aanbieders van ICT-diensten die al onderworpen zijn aan toezichtmechanismen ***ter ondersteuning van de uitvoering*** van de in artikel 127, lid 2, van het Verdrag betreffende de werking van de Europese Unie bedoelde taken op Eurosysteemniveau, moeten worden vrijgesteld. ***Evenzo mag het mechanisme om als cruciaal te worden aangewezen niet van toepassing zijn op ondernemingen die deel uitmaken van een financiële groep en die uitsluitend ICT-diensten verlenen aan financiële entiteiten binnen diezelfde financiële groep.***

(58) De vereiste dat als cruciaal aangemerkte derde aanbieders van ICT-diensten juridisch zijn opgericht in de Unie, houdt geen gegevenslokalisatie in, aangezien deze verordening geen verdere vereisten inzake gegevensopslag of -verwerking in de Unie bevat. ***Met het vereiste om een onderneming te hebben, zoals een in de Unie krachtens het recht van een lidstaat opgerichte dochteronderneming, wordt beoogd een contactpunt te verschaffen tussen de derde aanbieder van ICT-diensten enerzijds en de leidende toezichthouder en het orgaan voor gezamenlijk toezicht anderzijds, en ervoor te zorgen dat de leidende toezichthouder en het orgaan voor***

gezamenlijk toezicht hun taken kunnen uitvoeren en hun bevoegdheden op het gebied van toezicht en handhaving kunnen uitoefenen zoals bepaald in deze verordening. De gecontracteerde diensten van de derde aanbieder van ICT-diensten hoeven niet door zijn entiteit in de Unie te worden verricht.

(58 bis) ***Als gevolg van de aanzienlijke impact die de aanwijzing als cruciaal op derde aanbieders van ICT-diensten kan hebben, moeten rechten om vooraf te worden gehoord worden vastgesteld als een verplichting voor de ETA's en het orgaan voor gezamenlijk toezicht om naar behoren rekening te houden met alle aanvullende informatie die in de loop van de aanwijzingsprocedure door derde aanbieders van ICT-diensten wordt verstrekt.***

(59) ***Het toezicht***kader mag geen afbreuk doen aan de bevoegdheid van de lidstaten om eigen toezichttaken uit te voeren met betrekking tot derde aanbieders van ICT-diensten die niet cruciaal zijn in de zin van deze verordening maar op nationaal niveau belangrijk kunnen worden geacht.

(60) Om ten volle gebruik te maken van de huidige meerlagige institutionele architectuur op het gebied van financiële diensten, moet het Gemengd Comité van de ETA's blijven zorgen voor sectoroverschrijdende coördinatie met betrekking tot alle kwesties in verband met ICT-risico, overeenkomstig zijn taken op het gebied van cyberbeveiliging, ***door middel van het nieuw opgerichte orgaan voor gezamenlijk toezicht dat*** individuele besluiten ***neemt*** ten aanzien van cruciale derde aanbieders van ICT-diensten en voor collectieve aanbevelingen, met name inzake het benchmarken van de toezichtprogramma's van cruciale derde aanbieders van ICT-diensten, alsook het identificeren van beste praktijken voor de aanpak van kwesties in verband met het ICT-concentratierisico.

(61) Om ervoor te zorgen dat in de Unie op vergelijkbare wijze toezicht wordt gehouden op derde aanbieders van ICT-diensten die een cruciale rol vervullen voor de werking van de financiële sector, ***moet het orgaan voor gezamenlijk toezicht worden opgericht om rechtstreeks toezicht te houden op derde aanbieders van ICT-diensten***. ***Voorts*** moet een van de ETA's worden aangewezen als leidende toezichthouder voor elke cruciale externe ICT-dienstverlener ***om dagelijks toezicht en onderzoekswerkzaamheden te verrichten en te coördineren, als enig contactpunt op te treden en de continuïteit te waarborgen. Het orgaan voor gezamenlijk toezicht en de leidende toezichthouder moeten naadloos samenwerken om te zorgen voor efficiënt dagelijks toezicht en een holistische benadering van besluitvorming en aanbevelingen.***

(62) Leidende toezichthouders moeten de nodige bevoegdheden hebben om onderzoeken, inspecties ter plaatse met betrekking tot cruciale derde aanbieders van ICT-diensten te verrichten, toegang te krijgen tot alle relevante gebouwen en locaties en volledige en bijgewerkte informatie te verkrijgen, zodat zij in staat zijn daadwerkelijk inzicht te verwerven in het soort, de omvang en de impact van het ICT-risico van derde aanbieders voor financiële entiteiten en uiteindelijk voor het financiële stelsel van de Unie.

(62 bis) Om de systemische dimensie van ICT-risico's in de financiële sector te onderkennen en aan te pakken, is het een voorwaarde dat rechtstreeks toezicht aan het ***orgaan voor gezamenlijk toezicht*** wordt toevertrouwd. De voetafdruk in de Unie van

cruciale derde aanbieders van ICT-diensten en de daaraan verbonden potentiële kwesties in verband met het ICT-concentratierisico vergen een collectieve aanpak op het niveau van de Unie. Wanneer een groot aantal bevoegde autoriteiten los van elkaar, met weinig of geen coördinatie, vele audits verricht en toegangsrechten uitoefent, zou geen volledig overzicht worden verkregen van het ICT-risico van derde aanbieders, maar zouden wel onnodige redundantie, lasten en complexiteit ontstaan voor de cruciale derde aanbieders van ICT-diensten die met al die verzoeken te maken krijgen.

(63) Daarnaast moet ***het orgaan voor gezamenlijk toezicht*** aanbevelingen kunnen doen over kwesties in verband met ICT-risico en voor passende oplossingen, waaronder de afwijzing van bepaalde contractuele regelingen die uiteindelijk van invloed zijn op de stabiliteit van de financiële entiteit of het financiële stelsel. Als onderdeel van hun taak op het gebied van prudentieel toezicht op financiële entiteiten moeten de nationale bevoegde autoriteiten nagaan of deze inhoudelijke aanbevelingen van het ***orgaan voor gezamenlijk toezicht*** in acht worden genomen. ***Voorafgaand aan de afronding van die aanbevelingen moeten cruciale derde aanbieders van ICT-diensten de mogelijkheid krijgen om informatie te verstrekken waarvan zij redelijkerwijs van mening zijn dat die in aanmerking moet worden genomen voordat de aanbeveling wordt afgerond en uitgevaardigd***.

(63 bis) Ter voorkoming van doublures en tegenstrijdigheden met de technische en organisatorische maatregelen die van toepassing zijn op cruciale derde aanbieders van ICT-diensten, moeten de leidende toezichthouders en het orgaan voor gezamenlijk toezicht bij de uitoefening van hun bevoegdheden overeenkomstig het toezichtkader in deze verordening naar behoren rekening houden met het kader dat is ingesteld bij Richtlijn (EU) 2016/1148. Alvorens die bevoegdheden uit te oefenen moeten het orgaan voor gezamenlijk toezicht en de leidende toezichthouders overleg plegen met de betrokken bevoegde autoriteiten die bevoegd zijn krachtens Richtlijn (EU) 2016/1148.

(64) Het toezichtkader komt op generlei wijze, ook niet gedeeltelijk, in de plaats van het beheer door financiële entiteiten van het risico dat het gebruik van derde aanbieders van ICT-diensten meebrengt, inclusief de verplichting om hun contractuele regelingen met cruciale derde aanbieders van ICT-diensten doorlopend te monitoren. Het laat de volledige verantwoordelijkheid van de financiële entiteiten voor de naleving van alle vereisten van deze verordening en de desbetreffende wetgeving inzake financiële diensten onverlet. Om doublures en overlappingen te voorkomen, moeten de bevoegde autoriteiten afzien van individuele maatregelen om de risico's van cruciale derde aanbieders van ICT-diensten te monitoren. Dergelijke maatregelen moeten van tevoren worden gecoördineerd en overeengekomen zijn in de context van het toezichtkader.

(65) Om convergentie op internationaal niveau te bevorderen inzake beste praktijken voor de evaluatie van het digitale risicobeheer van derde aanbieders van ICT-diensten, moeten de ETA's worden aangemoedigd samenwerkingsovereenkomsten te sluiten met de relevante toezichthoudende en regelgevende bevoegde autoriteiten van derde landen om de ontwikkeling van beste praktijken voor het aanpakken van het ICT-risico van derde aanbieders te vergemakkelijken.

(66) Om de technische expertise van deskundigen van de bevoegde autoriteiten op het

gebied van beheer van operationeel en ICT-risico ten volle te benutten, moeten de leidende toezichthouders ***bij het verrichten van algemene onderzoeken of inspecties ter plaatse***, gebruikmaken van nationale toezichtervaring en specifieke onderzoeksteams opzetten voor elke cruciale derde aanbieder van ICT-diensten. Daarbij worden multidisciplinaire teams samengebracht om de voorbereiding en de uitvoering van toezichtactiviteiten, inclusief inspecties ter plaatse bij cruciale derde aanbieders van ICT-diensten, alsook de benodigde follow-up daarvan te ondersteunen.

(67) De bevoegde autoriteiten moeten over alle nodige toezichts-, onderzoeks- en sanctiebevoegdheden beschikken om de toepassing van deze verordening te waarborgen. Administratieve sancties dienen in beginsel te worden bekendgemaakt. Aangezien financiële entiteiten en derde aanbieders van ICT-diensten kunnen zijn gevestigd in verschillende lidstaten en kunnen ressorteren onder het toezicht van verschillende sectorale bevoegde autoriteiten, moet middels wederzijdse uitwisseling van informatie en verlening van bijstand bij het toezicht worden gezorgd voor nauwe samenwerking tussen de relevante bevoegde autoriteiten, met inbegrip van de ECB met betrekking tot de specifieke taken die haar bij Verordening (EU) nr. 1024/2013 van de Raad[16] zijn opgedragen, en voor overleg met de ETA's. ***De Gemeenschappelijke Afwikkelingsraad is weliswaar geen bevoegde autoriteit in de zin van deze verordening, maar moet niettemin worden betrokken bij de mechanismen voor de wederzijdse uitwisseling van informatie voor entiteiten die binnen het toepassingsgebied van Verordening (EU) nr. 806/2014 van het Europees Parlement en de Raad[17] vallen***.

(68) Om de criteria voor de aanwijzing van cruciale derde aanbieders van ICT-diensten verder te kwantificeren en te kwalificeren en de toezichtvergoedingen te harmoniseren, moet de bevoegdheid om handelingen vast te stellen overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie aan de Commissie worden overgedragen met het oog op: verdere specificatie van de systeemeffecten die het falen van een derde aanbieder van ICT-diensten kan hebben voor de financiële entiteiten die hij bedient, de aantallen mondiaal systeemrelevante instellingen (MSI's) of andere systeemrelevante instellingen (ASI's) die afhankelijk zijn van de respectieve derde aanbieder van ICT-diensten, het aantal op een specifieke markt actieve derde aanbieders van ICT-diensten, de kosten voor het migreren naar een andere derde aanbieder van ICT-diensten, het aantal lidstaten waar de betrokken derde aanbieder van ICT-diensten diensten verleent en waar financiële entiteiten actief zijn die de betrokken derde aanbieder van ICT-diensten gebruiken, alsook het bedrag van de toezichtvergoedingen en de wijze waarop zij moeten worden betaald.

---

16 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).

17 ***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)***.

Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven[18]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(69) Aangezien deze verordening, samen met Richtlijn (EU) 20xx/xx van het Europees Parlement en de Raad[19] 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, waaronder de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014, moeten die verordeningen, om te zorgen voor volledige consistentie, worden gewijzigd om te verduidelijken dat de relevante bepalingen inzake ICT-risico in deze verordening zijn opgenomen.

Relevante richtsnoeren betreffende de toepassing van die verordeningen en richtlijnen, die door de ETA's zijn uitgevaardigd of worden voorbereid, moeten in het kader van het consolidatieproces worden geëvalueerd en herzien zodat de rechtsgrondslag voor vereisten inzake ICT-risico in het Unierecht met betrekking tot entiteiten die binnen het toepassingsgebied daarvan vallen, uitsluitend berust op deze verordening, de bijbehorende uitvoeringshandelingen en de daarmee in overeenstemming vastgestelde besluiten en aanbevelingen.

(69 bis) Technische normen moeten zorgen voor een consequente harmonisatie van de in deze verordening neergelegde voorschriften. De ETA's, als organen met hooggespecialiseerde expertise, moeten worden belast met de ontwikkeling van ontwerpen van technische reguleringsnormen die geen beleidskeuzen inhouden, met het oog op de voorlegging ervan aan de Commissie. Er moeten technische reguleringsnormen worden ontwikkeld op het gebied van ICT-risicobeheer, rapportage, tests en essentiële vereisten voor een degelijke monitoring van het ICT-risico van derde aanbieders. ***Bij het ontwikkelen van ontwerpen van technische reguleringsnormen moeten de ETA's naar behoren rekening houden met hun mandaat in verband met evenredigheidsaspecten, en advies inwinnen bij hun respectieve adviescomités inzake evenredigheid, met name in verband met de toepassing van deze verordening op kmo's en ondernemingen met middelgroot kapitaal.***

(70) Het is van bijzonder belang dat de Commissie tijdens haar voorbereidend werk tot passende raadpleging overgaat, ook op deskundigenniveau. De Commissie en de ETA's dienen ervoor te zorgen dat die normen en vereisten door alle financiële entiteiten kunnen worden toegepast op een wijze die in verhouding staat tot de aard, de

---

18 PB L 123 van 12.5.2016, blz. 1.

19 [Gelieve volledige verwijzing in te voegen]

omvang en de complexiteit van die entiteiten en hun activiteiten.

(71) Om de vergelijkbaarheid van meldingen van ernstige ICT-gerelateerde incidenten te vergemakkelijken en te zorgen voor transparantie over contractuele regelingen voor het gebruik van ICT-diensten van derde aanbieders, moeten de ETA's de opdracht krijgen ontwerpen van technische uitvoeringsnormen te ontwikkelen waarin gestandaardiseerde templates, formulieren en procedures voor het melden van ernstige ICT-gerelateerde incidenten door financiële entiteiten worden vastgesteld, alsook gestandaardiseerde templates voor het informatieregister. Bij het uitwerken van die normen moeten de ETA's rekening houden met de ***aard***, de omvang, de complexiteit ***en het bedrijfsprofiel*** van financiële entiteiten, alsook met de aard en risicograad van hun activiteiten. De Commissie dient bevoegd te zijn die technische uitvoeringsnormen vast te stellen door middel van gedelegeerde handelingen krachtens artikel 291 VWEU en in overeenstemming met artikel 15 van respectievelijk de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010. Aangezien al verdere vereisten zijn vastgesteld door middel van gedelegeerde en uitvoeringshandelingen op basis van technische regulerings- en uitvoeringsnormen in respectievelijk de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014, is het passend de ETA's, afzonderlijk of gezamenlijk via het Gemengd Comité, opdracht te geven bij de Commissie technische regulerings- en 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.

(72) Deze operatie zal leiden tot latere wijziging van bestaande gedelegeerde en uitvoeringshandelingen op verschillende gebieden van de wetgeving inzake financiële diensten. Het toepassingsgebied van de artikelen over operationeel risico op grond waarvan bevoegdheidsdelegaties in die handelingen noodzakelijkerwijs tot de vaststelling van gedelegeerde en uitvoeringshandelingen hebben geleid, moet worden gewijzigd om alle bepalingen met betrekking tot de digitale operationele veerkracht die momenteel deel uitmaken van die verordeningen, in deze verordening over te nemen.

(73) Aangezien de doelstellingen van deze verordening, namelijk het bereiken van een hoog niveau van digitale operationele veerkracht voor alle financiële entiteiten, niet voldoende door de lidstaten kunnen worden verwezenlijkt omdat zulks de harmonisatie vereist van een veelheid van verschillende voorschriften die thans in sommige handelingen van de Unie of in de rechtsstelsels van de diverse lidstaten bestaan, maar, vanwege de omvang en de gevolgen ervan, beter door de Unie kunnen 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 deze doelstelling te verwezenlijken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

1. Deze verordening stelt met betrekking tot de beveiliging van netwerk- en informatiesystemen ter ondersteuning van bedrijfsprocessen van financiële entiteiten de volgende uniforme vereisten vast die nodig zijn om een hoog gemeenschappelijk niveau van digitale operationele veerkracht te bereiken:

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

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

– de melding van ernstige ICT-gerelateerde incidenten aan de bevoegde autoriteiten;

– ***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 c);***

– het testen van de digitale operationele veerkracht;

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

– maatregelen voor ***het goede*** beheer van het risico inzake derde ICT-aanbieders door financiële entiteiten;

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

c) het toezichtkader voor cruciale 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 5 van Richtlijn (EU) 2016/1148 als aanbieders van essentiële diensten zijn aangewezen, wordt deze verordening voor de toepassing van artikel 1, lid 7, van die richtlijn beschouwd als een sectorspecifieke rechtshandeling van de Unie.

2 bis. Deze verordening laat de bevoegdheden van de lidstaten inzake de handhaving van de openbare veiligheid, defensie en nationale veiligheid onverlet.

Artikel 2

Personele werkingssfeer

1. Deze verordening is van toepassing op de volgende entiteiten:

a) kredietinstellingen,

b) betalingsinstellingen,

c) instellingen voor elektronisch geld,

d) beleggingsondernemingen,

e) aanbieders van cryptoactivadiensten, emittenten ***en aanbieders*** van ***cryptoactiva***, emittenten ***en aanbieders*** van asset-referenced tokens en emittenten van significante asset-referenced tokens,

f) centrale effectenbewaarinstellingen ***en exploitanten van effectenafwikkelingssystemen***,

g) centrale tegenpartijen,

h) handelsplatformen,

i) transactieregisters,

j) beheerders van alternatieve beleggingsinstellingen,

k) beheermaatschappijen,

l) aanbieders van datarapporteringsdiensten,

m) verzekerings- en herverzekeringsondernemingen,

n) verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen ***die geen micro-, kleine of middelgrote ondernemingen zijn, tenzij die micro-, kleine of middelgrote ondernemingen uitsluitend afhankelijk zijn van georganiseerde geautomatiseerde verkoopsystemen***,

o) instellingen voor ***bedrijfspensioenvoorzieningen (IBPV's) die geen pensioenregelingen uitvoeren die samen minder dan 15 leden hebben***,

p) ratingbureaus,

q) wettelijke auditors en auditkantoren ***die geen micro-, kleine of middelgrote ondernemingen zijn, tenzij die micro-, kleine of middelgrote ondernemingen auditdiensten verlenen aan de in dit artikel vermelde entiteiten, met uitzondering van micro-, kleine of middelgrote ondernemingen die controle-entiteiten zonder winstoogmerk zijn in de zin van artikel 2, lid 3, van Verordening (EU) nr. 537/2014, tenzij de bevoegde autoriteit besluit dat de uitzondering niet geldig is***,

r) beheerders van cruciale benchmarks,

s) aanbieders van crowdfundingdiensten,

t) securitisatieregisters,

u) derde aanbieders van ICT-diensten.

1 bis. Deze verordening, met uitzondering van hoofdstuk V, afdeling II, is ook van

toepassing op aanbieders van ICT-diensten binnen een groep.

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

2 bis. Voor de toepassing van deze verordening, met uitzondering van hoofdstuk V, afdeling II, worden derde aanbieders van ICT-diensten en aanbieders van ICT-diensten binnen een groep gezamenlijk aangeduid als "derde aanbieders van ICT-diensten".

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "digitale operationele veerkracht": het vermogen van een financiële entiteit om haar operationele integriteit ▌ op te bouwen, te waarborgen en te evalueren, door ***in geval van operationele storingen die de ICT-capaciteiten van de financiële entiteit beïnvloeden,*** direct of indirect via gebruik van diensten van derde ICT-aanbieders te voorzien in ▌ de permanente verlening van financiële diensten en de kwaliteit ervan ▌ ;

(2) "netwerk- en informatiesysteem": een netwerk- en informatiesysteem in de zin van artikel 4, punt 1), van Richtlijn (EU) 2016/1148;

(3) "beveiliging van netwerk- en informatiesystemen": beveiliging van netwerk- en informatiesystemen in de zin van artikel 4, punt 2), van Richtlijn (EU) 2016/1148;

(4) "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 ***door ICT*** geregelde instrumenten of processen, van de exploitatie en het procesverloop, of van de levering van de diensten in gevaar kan brengen ▌ ;

(5) "informatiebestanddeel": een reeks, al dan niet tastbare, gegevens die beschermenswaardig zijn;

(6) "ICT-gerelateerd incident": een onvoorzien geïdentificeerd ***incident dat, of een reeks gekoppelde incidenten die*** de beveiliging ▌ van netwerk- en informatiesystemen ***in gevaar brengt*** of nadelige gevolgen heeft voor de beschikbaarheid, vertrouwelijkheid, continuïteit***, integriteit*** of authenticiteit van de door de financiële entiteit verleende financiële diensten;

(6 bis) "betalingsgerelateerd operationeel of beveiligingsincident": een niet door de in artikel 2, lid 1, punten a) tot en met c), bedoelde financiële entiteiten voorziene gebeurtenis of reeks gekoppelde gebeurtenissen die nadelige gevolgen heeft of kan hebben voor de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit of continuïteit van betalingsgerelateerde diensten;

(7) "ernstig ICT-gerelateerd incident": een ICT-gerelateerd incident ***dat*** grote nadelige gevolgen ***heeft of kan hebben*** voor de netwerk- en informatiesystemen die cruciale functies van de financiële entiteit ondersteunen;

(7 bis) "ernstig betalingsgerelateerd operationeel of beveiligingsincident": een betalingsgerelateerd operationeel of beveiligingsincident dat aan de in artikel 16

genoemde criteria voldoet;

(8) "cyberdreiging": cyberdreiging in de zin van artikel 2, punt 8), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad[20];

(8 bis) "significante cyberdreiging": een cyberdreiging waarvan de kenmerken duidelijk aangeven dat de kans groot is dat die bedreiging zal resulteren in een ernstig ICT-gerelateerd incident;

(9) "cyberaanval": een kwaadwillig ICT-gerelateerd incident door middel 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;

(10) "inlichtingen over dreigingen": informatie die is geaggregeerd, getransformeerd, geanalyseerd, geïnterpreteerd of verrijkt om de noodzakelijke achtergrond voor besluitvorming te bieden en waarmee relevant en toereikend inzicht wordt verschaft 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;

(11) "verdediging in de diepte": een ICT-gerelateerde strategie waarin personen, processen en technologie worden geïntegreerd om uiteenlopende begrenzingen tussen verschillende lagen en dimensies van de entiteit in te stellen;

(12) "kwetsbaarheid": een zwakte, gevoeligheid of tekortkoming in een actief, systeem, proces of controle die door een ***cyberdreiging*** kan worden misbruikt;

(13) "dreigingsgestuurde penetratietest" (threat led penetration testing): een kader waarin de tactiek, de 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 cruciale reëel bestaande productiesystemen van de entiteit wordt voorgebracht;

(14) "ICT-risico van derde aanbieder": een 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 verdere onderaannemers daarvan worden geleverd;

(15) "derde aanbieder van ICT-diensten": een onderneming die ***ICT-diensten*** aanbiedt, met inbegrip van ***een ICT-diensten verlenende financiële entiteit die deel uitmaakt van een onderneming die een breder scala aan producten of diensten aanbiedt***, maar met uitsluiting van aanbieders van hardwarecomponenten en ondernemingen waaraan krachtens het Unierecht vergunning is verleend om elektronischecommunicatiediensten te verlenen in de zin van artikel 2, punt 4), van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad[21];

---

[20] 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 (cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

[21] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (PB L 321 van 17.12.2018, blz. 36).

(15 bis) "aanbieder van ICT-diensten binnen een groep": een onderneming die deel uitmaakt van een financiële groep en uitsluitend 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;

(16) "ICT-diensten": digitale en gegevensdiensten die via de ICT-systemen ***doorlopend*** aan een of meer interne of externe gebruikers worden verleend, met ***uitzondering*** van ***telecommunicatiecontracten***;

(17) "cruciale of belangrijke functie": een ***activiteit of dienst die essentieel is voor de werking van een financiële entiteit en waarvan de verstoring wezenlijk afbreuk zou doen aan de soliditeit of de continuïteit van de diensten en activiteiten van de financiële entiteit, of*** waarvan de beëindiging of de 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 de toepasselijke wetgeving inzake financiële diensten, ***met inbegrip van "kritieke functies" in de zin van artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU***;

(18) "cruciale derde aanbieder van ICT-diensten": een derde aanbieder van ICT-diensten die overeenkomstig artikel ***28*** is aangewezen en onderworpen is aan het toezichtkader bedoeld in de artikelen ***29*** tot en met 37;

(19) "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 een contractuele overeenkomst met een financiële entiteit heeft gesloten voor de levering van ICT-diensten;

(20) "in een derde land gevestigde ICT-subcontractant": een ICT-subcontractant die een in een derde land gevestigde rechtspersoon is ▌ en 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;

(21) "ICT-concentratierisico": een blootstelling aan individuele of aan meerdere onderling verbonden cruciale 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 laatste ***de financiële stabiliteit van de Unie in haar geheel of*** het vermogen van een financiële entiteit ▌ om cruciale ***of belangrijke*** functies te vervullen of om andere soorten nadelige effecten, waaronder grote verliezen, op te vangen, in gevaar kan brengen;

(22) "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, artikel 2, lid 1, punt 45), van Verordening (EU) nr. 909/2014, artikel 3, lid 1, punt 20), van Verordening (EU) 2016/1011 van het Europees Parlement en de Raad[22], of artikel 3, lid 1, punt ***18***), van

[22] 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

Verordening (EU) 20xx/xx van het Europees Parlement en de Raad[23] [MICA] of de gelijkwaardige personen die de entiteit daadwerkelijk besturen of sleutelfuncties vervullen overeenkomstig de toepasselijke Unie- of nationale wetgeving;

(23) "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[24];

(23 bis) "bij Richtlijn 2013/36/EU vrijgestelde kredietinstelling": een instelling die een vrijstelling geniet op grond van artikel 2, lid 5, punten 4 tot en met 23, van Richtlijn 2013/36/EU;

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

(24 bis) "kleine en niet-verweven beleggingsonderneming": een beleggingsonderneming die voldoet aan de voorwaarden in artikel 12, lid 1, van Verordening (EU) 2019/2033;

(25) "betalingsinstelling": een betalingsinstelling in de zin van artikel 1, lid 1, punt d), van Richtlijn (EU) 2015/2366;

(25 bis) "bij Richtlijn (EU) 2015/2366 vrijgestelde betalingsinstelling": een betalingsinstelling die een vrijstelling geniet op grond van artikel 32, lid 1, van Richtlijn (EU) 2015/2366;

(26) "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[25];

(26 bis) "bij Richtlijn (EU) 2009/110/EG vrijgestelde instelling voor elektronisch geld": een instelling voor elektronisch geld die vrijgesteld is krachtens artikel 9 van Richtlijn 2009/110/EG;

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

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

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

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

---

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).

23 [*please insert full title and OJ details*]

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

25 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).

(31) “beheerder van alternatieve beleggingsinstellingen”: een beheerder van alternatieve beleggingsinstellingen in de zin van artikel 4, lid 1, punt b), van Richtlijn 2011/61/EU;

(32) “beheermaatschappij”: een beheermaatschappij in de zin van artikel 2, lid 1, punt b), van Richtlijn 2009/65/EG;

(33) “aanbieder van datarapporteringsdiensten”: een aanbieder van datarapporteringsdiensten in de zin van artikel 4, lid 1, punt 63), van Richtlijn 2014/65/EU;

(34) “verzekeringsonderneming”: een verzekeringsonderneming in de zin van artikel 13, punt 1), van Richtlijn 2009/138/EG;

(35) “herverzekeringsonderneming”: een herverzekeringsonderneming in de zin van artikel 13, punt 4), van Richtlijn 2009/138/EG;

(36) “verzekeringstussenpersoon”: een verzekeringstussenpersoon in de zin van artikel 2, ***lid 1,*** punt 3), van Richtlijn (EU) 2016/97;

(37) “nevenverzekeringstussenpersoon”: een nevenverzekeringstussenpersoon in de zin van artikel 2, ***lid 1,*** punt 4), van Richtlijn (EU) 2016/97;

(38) “herverzekeringstussenpersoon”: een herverzekeringstussenpersoon in de zin van artikel 2, ***lid 1,*** punt 5), van Richtlijn (EU) 2016/97;

(39) “instelling voor bedrijfspensioenvoorziening”: een instelling voor bedrijfspensioenvoorziening in de zin van artikel 6, punt 1), van Richtlijn 2016/2341;

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

(41) “wettelijke auditor”: een wettelijke auditor in de zin van artikel 2, punt 2), van Richtlijn 2006/43/EG;

(42) “auditkantoor”: een auditkantoor in de zin van artikel 2, punt 3), van Richtlijn 2006/43/EG;

(43) “aanbieder van cryptoactivadiensten”: een aanbieder van cryptoactivadiensten in de zin van artikel 3, lid 1, punt ***8***), van Verordening (EU) 202x/xx [*PO: insert reference to MiCA Regulation*];

(44) “emittent van cryptoactiva”: een emittent van cryptoactiva in de zin van artikel 3, lid 1, punt ***6***), van [*OJ: insert reference to MICA Regulation*];

(44 bis) “aanbieder”: een aanbieder in de zin van artikel 3, lid 1, [punt XX)] van [OJ: insert reference to MICA Regulation];

(44 ter) “aanbieder van cryptoactiva”: een aanbieder van “cryptoactiva” in de zin van artikel 3, lid 1, [punt XX)] van [OJ: insert reference to MICA Regulation];

(45) “emittent van asset-referenced tokens”: een emittent van asset-referenced tokens in de zin van artikel 3, lid 1, punt i), van [*OJ: insert reference to MICA Regulation*];

(45 bis) “aanbieder van asset-referenced tokens”: een aanbieder van asset-referenced tokens in de zin van artikel 3, lid 1, [punt XX)] van [OJ: insert reference to MICA Regulation];

(46) "emittent van significante asset-referenced tokens": een emittent van significante asset-referenced tokens in de zin van artikel 3, lid 1, punt ***XX***), van [*OJ: insert reference to MICA Regulation*];

(47) "beheerder van cruciale benchmarks": een beheerder van "cruciale benchmarks" in de zin van artikel ***3***, punt ***25***), van Verordening ***(EU) 2016/1011*** [*OJ: insert reference to Benchmark Regulation*];

(48) "aanbieder van crowdfundingdiensten": een aanbieder van crowdfundingdiensten in de zin van artikel ***2, lid 1***, punt ***e***), van Verordening ***(EU) 2020/1503*** [*OJ: insert reference to Crowdfunding Regulation*];

(49) "securitisatieregister": een securitisatieregister in de zin van artikel 2, punt 23), van Verordening (EU) 2017/2402;

(50) "micro-***, kleine en middelgrote*** onderneming": een ***financiële entiteit*** in de zin van artikel 2 ▌ van de bijlage bij Aanbeveling 2003/361/EG***;***

(50 bis) "afwikkelingsautoriteit": de door een lidstaat overeenkomstig artikel 3 van Richtlijn 2014/59/EU aangewezen autoriteit of de bij artikel 42 van Verordening (EU) nr. 806/2014 opgerichte Gemeenschappelijke Afwikkelingsraad.

Artikel 3 bis

Evenredigheidsbeginsel

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

2. Overeenkomstig het evenredigheidsbeginsel zijn de artikelen 4 tot en met 14 van deze verordening niet van toepassing op:

a) kleine en niet-verweven beleggingsondernemingen of betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld;

b) kredietinstellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld;

c) instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld; of

d) kleine instellingen voor bedrijfspensioenvoorziening.

3. Op basis van het jaarverslag over de evaluatie van het kader voor ICT-risicobeheer als bedoeld in artikel 5, lid 6, en artikel 14 bis, lid 2, toetsen en evalueren de relevante bevoegde autoriteiten de toepassing van de evenredigheid door een financiële entiteit en bepalen zij of het kader voor ICT-risicobeheer van de financiële entiteit een degelijk beheer, digitale operationele veerkracht en dekking van ICT-risico's waarborgt. Daarbij houden de bevoegde autoriteiten rekening met de omvang van de financiële entiteit, de aard, schaal en complexiteit van haar diensten, activiteiten en verrichtingen, en haar algemene risicoprofiel.

4. Indien de relevante bevoegde autoriteit het kader voor ICT-risicobeheer van de financiële entiteit ontoereikend en onevenredig acht, voert zij een dialoog met de financiële entiteit om de tekortkomingen te verhelpen en te zorgen voor volledige naleving van hoofdstuk II.

5. De ETA's stellen ontwerpen van technische reguleringsnormen op ter bepaling van:

a) de mate waarin verplichtingen inzake ICT-risicobeheer van toepassing zijn op elke van de in lid 1 genoemde financiële entiteiten;

b) de inhoud en de vorm van het in lid 3 bedoelde jaarverslag over de evaluatie van het kader voor ICT-risicobeheer;

c) de regels en procedures die de bevoegde autoriteiten en financiële entiteiten moeten volgen in het kader van de in lid 4 bedoelde dialoog.

6. De ETA's leggen de in lid 5 bedoelde ontwerpen van technische reguleringsnormen uiterlijk op [OJ: insert date 1 year after the date of entry into force] voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om de in lid 5 bedoelde technische reguleringsnormen vast te stellen overeenkomstig de artikelen 10 tot en met 14 van respectievelijk de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010.

HOOFDSTUK II

ICT-RISICOBEHEER

AFDELING I

Artikel 4

Governance en organisatie

1. Financiële entiteiten beschikken over ***een*** intern governance- en ***controlekader dat*** een doeltreffend en prudent beheer van alle ICT-risico's ***waarborgt, teneinde een hoog niveau van digitale operationele veerkracht te verkrijgen***.

2. Het leidinggevend orgaan van een financiële entiteit bepaalt alle regelingen met betrekking tot het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer, keurt deze goed, houdt toezicht op de tenuitvoerlegging ervan en legt ervoor verantwoording af.

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

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

a bis) de invoering van procedures en beleidsmaatregelen die erop gericht zijn de handhaving van hoge normen inzake beveiliging, vertrouwelijkheid en integriteit van gegevens te waarborgen;

b) de vaststelling van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies;

c) de bepaling van het passende risicotolerantieniveau voor het ICT-risico van de financiële entiteit, als bedoeld in artikel 5, lid 9, punt b);

d) de goedkeuring van, het toezicht op en de periodieke evaluatie van de uitvoering van het beleid inzake ICT-bedrijfscontinuïteit en van het ICT-noodherstelplan van de financiële entiteit, als bedoeld in artikel 10, respectievelijk leden 1 en 3***, die kunnen worden aangenomen als een specifiek afzonderlijk beleid en als integrerend onderdeel van het ruimere bedrijfsbrede continuïteitsbeleid en noodherstelplan van de financiële entiteit***;

e) de goedkeuring en de periodieke evaluatie van de ICT-auditplannen, ICT-audits en materiële wijzigingen daarvan;

f) de toewijzing en de periodieke evaluatie van het passende budget om te voldoen aan de behoeften inzake digitale operationele veerkracht van de financiële entiteit met betrekking tot alle soorten middelen, waaronder ***relevante*** opleiding inzake ICT-risico's en -vaardigheden voor ***al*** het ▌

personeel;

g) de goedkeuring en de periodieke evaluatie van het beleid van de financiële entiteit inzake regelingen betreffende het gebruik van door derde aanbieders verleende ICT-diensten;

h) het inwinnen van informatie over de regelingen met derde aanbieders van ICT-diensten inzake het gebruik van deze diensten, over elke relevante geplande materiële wijziging betreffende de derde aanbieders van ICT-diensten en over de potentiële effecten van deze veranderingen voor de cruciale of belangrijke functies die onder die regelingen vallen, inclusief door middel van een samenvatting van de risicoanalyse om het effect van deze wijzigingen te beoordelen;

i) het ***regelmatig*** inwinnen van informatie over ***op zijn minst ernstige*** ICT-gerelateerde incidenten en de gevolgen daarvan en de respons daarop, het herstel en de corrigerende maatregelen.

3. Andere financiële entiteiten dan micro-ondernemingen stellen een taak vast om de regelingen ***binnen de financiële entiteit voor het gebruik van ICT-diensten, met name die*** met derde aanbieders van ICT-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's en de gevolgen daarvan voor de activiteiten van de financiële entiteit te begrijpen en te beoordelen***, onder meer door regelmatig specifieke opleidingen te volgen die in verhouding staan tot de beheerde ICT-risico's***.

AFDELING II

Artikel 5

Kader voor ICT-risicobeheer

1. Financiële entiteiten beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer, dat hen in staat stelt ICT-risico's snel, efficiënt en zo volledig mogelijk aan te pakken en een hoog niveau van digitale operationele veerkracht te waarborgen ▌.

2. Het in lid 1 bedoelde kader voor ICT-risicobeheer omvat strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle relevante fysieke componenten en infrastructuren, met inbegrip van computerhardware, servers en alle relevante gebouwen, datacentra en als gevoelig aangewezen gebieden behoorlijk en doeltreffend te beschermen, teneinde te waarborgen dat al deze fysieke elementen adequaat worden beschermd tegen risico's, met inbegrip van schade, ongeoorloofde toegang en ongeoorloofd gebruik.

3. Financiële entiteiten beperken de effecten van ICT-risico's door passende strategieën, beleidslijnen, procedures, protocollen en instrumenten in te voeren zoals bepaald in het kader voor ICT-risicobeheer. Zij verstrekken volledige en geactualiseerde informatie over ICT-risico's ***en over hun kader voor ICT-risicobeheer wanneer*** de bevoegde autoriteiten ***daarom verzoeken***.

4. In het kader van het in lid 1 bedoelde kader voor ICT-risicobeheer voeren andere financiële entiteiten dan micro-ondernemingen een systeem voor beheer van informatiebeveiliging in dat gebaseerd is op erkende internationale normen en in overeenstemming is met de richtsnoeren voor toezicht, ***indien reeds beschikbaar en waar passend, met inbegrip van de richtsnoeren die zijn uiteengezet in de desbetreffende leidraden van de ETA's,*** en zij herzien dit regelmatig.

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

6. Het in lid 1 bedoelde kader voor ICT-risicobeheer wordt ten minste eenmaal per jaar gedocumenteerd en geëvalueerd, alsook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en om de toezichtinstructies of -conclusies van relevante tests of auditprocessen op het gebied van digitale operationele veerkracht te monitoren. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen.

Jaarlijks wordt bij de bevoegde autoriteit een verslag over de evaluatie van het kader voor ICT-risicobeheer ingediend.

7. ***Wat andere financiële entiteiten dan micro-ondernemingen betreft, wordt*** het in lid 1 bedoelde kader voor ICT-risicobeheer ▌regelmatig gecontroleerd door ICT-auditors die over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico's beschikken. De frequentie en de focus van de ICT-audits moeten in verhouding staan tot de ICT-risico's van de financiële entiteit.

8. Er wordt een formeel follow-upproces vastgesteld met regels voor de tijdige verificatie en remediëring van cruciale ICT-auditbevindingen, waarbij rekening wordt gehouden met de conclusies van de audit. ▌

9. Het in lid 1 bedoelde kader voor ICT-risicobeheer omvat een strategie voor digitale ***operationele*** veerkracht waarin de wijze van tenuitvoerlegging van het kader wordt vastgesteld. Met dat doel worden hierin de methoden omschreven om ICT-risico's aan te pakken en specifieke ICT-doelstellingen te bereiken, 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's 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 doelstellingen te bepalen met betrekking tot informatiebeveiliging;

d) de ***ICT-architectuur*** 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 effecten van ICT-gerelateerde incidenten op te sporen, te beveiligen en te voorkomen;

f) nadere gegevens te verschaffen over het aantal gemelde ernstige ICT-gerelateerde incidenten en de doeltreffendheid van preventieve maatregelen;

g) ▌de voornaamste afhankelijkheden ten aanzien van derde aanbieders van ICT-diensten ***in kaart te brengen en exitstrategieën te specificeren met betrekking tot dergelijke belangrijke afhankelijkheden***;

h) tests te verrichten van de digitale operationele veerkracht***, overeenkomstig hoofdstuk IV van deze verordening***;

i) een communicatiestrategie uit te stippelen in het geval van ICT-gerelateerde incidenten ***die overeenkomstig artikel 13 openbaar moeten worden gemaakt***.

10. Na goedkeuring door de bevoegde autoriteiten kunnen financiële entiteiten de verificatietaken inzake naleving van de vereisten op het gebied van ICT-risicobeheer ***uitbesteden*** aan ▌externe ondernemingen.

Na kennisgeving aan de bevoegde autoriteiten kunnen financiële entiteiten de verificatietaak inzake naleving van de vereisten op het gebied van ICT-risicobeheer delegeren aan intragroepsondernemingen.

Wanneer de in de tweede alinea bedoelde delegatie plaatsvindt, blijft de financiële entiteit volledig verantwoordelijk voor de controle van de naleving van de vereisten op het gebied van ICT-risicobeheer.

Artikel 6

ICT-systemen, -protocollen en -instrumenten

1. ***Om ICT-risico's aan te pakken en te beheren*** gebruiken en onderhouden ***financiële entiteiten*** geactualiseerde ICT-systemen, -protocollen en -instrumenten die aan de volgende voorwaarden voldoen:

a) de systemen en instrumenten zijn afgestemd op ▌de omvang van de verrichtingen ter ondersteuning van hun activiteiten;

b) zij zijn betrouwbaar;

c) zij hebben voldoende capaciteit 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) zij zijn technologisch gezien voldoende veerkrachtig om indien nodig in gespannen marktomstandigheden of andere ongunstige situaties naar behoren te voorzien in bijkomende gegevensverwerking.

2. Wanneer financiële entiteiten gebruikmaken van internationaal erkende technische normen en in de sector geldende toonaangevende praktijken inzake informatiebeveiliging en interne ICT-controles, worden deze normen en praktijken gebruikt in overeenstemming met de toepasselijke aanbevelingen over de invoering daarvan.

Artikel 7

Identificatie

1. In het kader van het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer identificeren, classificeren en documenteren financiële entiteiten naar behoren alle ***cruciale of belangrijke*** ICT-gerelateerde bedrijfsfuncties, de informatieactiva die deze functies ondersteunen, en de configuraties en interconnecties van het ICT-systeem met interne en externe ICT-systemen. Financiële entiteiten evalueren indien nodig en ten minste eenmaal per jaar of ***ICT-gerelateerde bedrijfsfuncties cruciaal of belangrijk zijn en of*** de classificatie van de informatieactiva en van alle relevante documentatie adequaat is.

2. Financiële entiteiten identificeren permanent alle bronnen van ICT-risico's, met name de wederzijdse risicoblootstelling ten aanzien van andere financiële entiteiten, en beoordelen de cyberdreigingen en ICT-kwetsbaarheden die relevant zijn voor hun ***cruciale of belangrijke*** ICT-gerelateerde bedrijfsfuncties en informatieactiva. 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 ***indien nodig*** een risicobeoordeling bij elke belangrijke wijziging in de netwerk- en informatiesysteeminfrastructuur en in de processen of procedures die van invloed zijn op hun functies, ondersteunende processen of informatieactiva.

4. Financiële entiteiten identificeren alle ICT-systeemrekeningen, met inbegrip van die welke zich op afgelegen locaties bevinden, de netwerkmiddelen en de hardware-uitrusting en inventariseren de fysieke uitrusting die zij cruciaal achten. Zij inventariseren de configuratie van de ***cruciale of belangrijke*** ICT-activa***, rekening houdend met hun doel en met*** de verbanden en onderlinge afhankelijkheden tussen ***die*** verschillende ICT-activa.

5. Financiële entiteiten identificeren en documenteren alle ***cruciale of belangrijke*** processen die afhankelijk zijn van derde aanbieders van ICT-diensten en identificeren interconnecties met derde aanbieders van ICT-diensten ***die cruciale of belangrijke***

functies ondersteunen.

6. Voor de toepassing van de leden 1, 4 en 5 houden financiële entiteiten de desbetreffende inventarissen bij en actualiseren zij deze regelmatig.

7. Andere financiële entiteiten dan micro-ondernemingen verrichten regelmatig en ten minste eenmaal per jaar een specifieke ICT-risicobeoordeling op alle bestaande ICT-systemen, ***met inbegrip van systemen die nog in gebruik zijn en hun functie vervullen maar die:***

a) oud of aan het eind van hun levensduur zijn, in het geval van hardware;

b) geen ondersteuning of onderhoud van hun leverancier meer kunnen krijgen; of

c) niet meer bijgewerkt kunnen worden of waarvoor dat economisch niet verantwoord zou zijn. Er worden jaarlijkse ICT-risicobeoordelingen op oude ICT-systemen verricht, in het bijzonder voor en na de aansluiting van ▌technologieën, toepassingen of systemen.

Artikel 8

Bescherming en voorkoming

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

2. Financiële entiteiten zorgen voor het ontwerp, de aanbesteding en de uitvoering van ICT-beveiligingsstrategieën, -beleidslijnen, -procedures, -protocollen en -instrumenten die er met name op gericht zijn de veerkracht, continuïteit en beschikbaarheid van ICT-systemen ***die cruciale of belangrijke functies ondersteunen*** te waarborgen alsmede hoge normen inzake beveiliging, vertrouwelijkheid en integriteit 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:

a) ▌de middelen voor overdracht van informatie ***maximaal beveiligen***;

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

c) het lekken van informatie voorkomen;

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

4. In het kader van het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer zorgen financiële entiteiten ***overeenkomstig hun risicoprofiel*** voor het volgende:

a) zij ontwikkelen en documenteren een beleid inzake informatiebeveiliging waarin regels worden vastgesteld om de vertrouwelijkheid, integriteit en beschikbaarheid van hun eigen ICT-middelen, -gegevens en -informatieactiva ▌te beschermen ***en tegelijkertijd waarborgen zij de volledige bescherming van de ICT-middelen, -gegevens en -informatieactiva van hun klanten indien die deel uitmaken van de ICT-systemen van de financiële entiteiten***;

b) zij voeren op grond van een op risico's gebaseerde aanpak een degelijk netwerk- en infrastructuurbeheer in met gebruik van passende technieken, methoden en protocollen, ***in voorkomend geval*** met inbegrip van de toepassing van ▌ mechanismen om in geval van cyberaanvallen de getroffen informatieactiva te isoleren;

c) zij voeren een beleid***, procedures en controles in*** waarbij de fysieke en virtuele toegang tot ICT-systemen en -gegevens wordt beperkt tot hetgeen alleen voor legitieme en goedgekeurde functies en activiteiten noodzakelijk is ▌;

d) zij voeren beleidslijnen en protocollen in voor strenge authenticatiemechanismen***, en de bescherming van cryptografische sleutels,*** die gebaseerd zijn op relevante normen en specifieke controlesystemen ▌;

e) zij voeren beleidslijnen, procedures en controles in voor het beheer van veranderingen in ICT, met inbegrip van veranderingen in software, hardware, firmwarecomponenten, veranderingen in systemen of beveiliging, die gebaseerd zijn op een aanpak inzake risicobeoordeling en integrerend deel uitmaken van het algemene beheerproces met betrekking tot verandering in 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 beleid voor patches en updates.

Voor de toepassing van punt b) ontwerpen financiële entiteiten de netwerkaansluitinfrastructuur op zodanige wijze dat deze ***zo snel mogelijk*** kan worden afgekoppeld en dat compartimentering en segmentering daarmee worden verzekerd, teneinde besmetting te beperken en te voorkomen, met name voor onderling gekoppelde financiële processen.

Voor de toepassing van punt e) wordt het beheerproces inzake ICT-veranderingen goedgekeurd door passende beheerlijnen en worden specifieke protocollen ingesteld voor spoedveranderingen.

Artikel 9

Detectie

1. Financiële entiteiten beschikken over mechanismen om overeenkomstig artikel 15 afwijkende activiteiten zo spoedig mogelijk te detecteren, met inbegrip van kwesties op het gebied van ICT-netwerkprestaties en ICT-gerelateerde incidenten, en om***,***

wanneer zulks technisch mogelijk is, alle potentiële zwakke fysieke punten ("single points of failure") te identificeren ***en te monitoren***.

Alle in de eerste alinea bedoelde detectiemechanismen worden regelmatig getest overeenkomstig artikel 22.

2. De in lid 1 bedoelde detectiemechanismen ***stellen*** processen voor detectie van en respons op ICT-gerelateerde incidenten in werking***, 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 alsmede het optreden van ICT-anomalieën en ICT-gerelateerde incidenten, met name cyberaanvallen.

3 bis. Financiële entiteiten registreren alle ICT-gerelateerde incidenten die gevolgen hebben voor de stabiliteit, continuïteit of kwaliteit van financiële diensten, onder meer indien het incident gevolgen heeft of dreigt te hebben voor die diensten.

4. De in artikel 2, lid 1, punt l), bedoelde financiële entiteiten beschikken daarnaast over systemen die transactiemeldingen doeltreffend op volledigheid kunnen controleren, omissies en aperte fouten kunnen opsporen en om hernieuwde transmissie van eventuele foutmeldingen kunnen verzoeken.

Artikel 10

Respons en herstel

1. In het raam van het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer en op basis van de in artikel 7 gestelde identificatievereisten voeren financiële entiteiten een ▌alomvattend beleid inzake ICT-bedrijfscontinuïteit ***dat kan worden aangenomen als een specifiek afzonderlijk beleid en*** als integrerend onderdeel van het ***ruimere bedrijfsbrede*** beleid inzake operationele bedrijfscontinuïteit van de financiële entiteit.

Het beleid inzake ICT-bedrijfscontinuïteit is erop gericht risico's die een schadelijk effect op de ICT-systemen en -diensten van financiële entiteiten kunnen hebben, te beheren en te beperken en, indien nodig, het snelle herstel ervan te vergemakkelijken. Bij het opstellen van het beleid inzake ICT-bedrijfscontinuïteit gaan financiële entiteiten specifiek in op risico's die schadelijke gevolgen kunnen hebben voor ICT-diensten en ICT-systemen.

2. Financiële entiteiten voeren het in lid 1 bedoelde beleid inzake ICT-bedrijfscontinuïteit uit via specifieke, aangepaste en gedocumenteerde regelingen, plannen, procedures en mechanismen die erop gericht zijn:

b) de continuïteit van de cruciale functies van de financiële entiteit te verzekeren;

c) op een snelle, passende en doeltreffende wijze een respons en een oplossing te bieden voor alle ICT-gerelateerde incidenten, in het bijzonder maar niet beperkt tot cyberaanvallen, zodanig dat de schade wordt beperkt en prioriteit wordt verleend aan de hervatting van de activiteiten en aan herstelmaatregelen;

d) 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 11;

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

f) 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 13 en aan de bevoegde autoriteiten wordt gemeld overeenkomstig artikel 17.

3. In het raam van het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer voeren financiële entiteiten een bijbehorend ICT-noodherstelplan in dat in het geval van andere financiële entiteiten dan micro-ondernemingen aan onafhankelijke audits wordt onderworpen.

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

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

a) ten minste jaarlijks en na substantiële wijzigingen in de ***cruciale of belangrijke*** ICT-systemen het beleid inzake ICT-bedrijfscontinuïteit en het ICT-noodherstelplan;

b) de overeenkomstig artikel 13 opgestelde crisiscommunicatieplannen.

Voor de toepassing van 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, back-ups en reservefaciliteiten die noodzakelijk zijn om te voldoen aan de in artikel 11 bedoelde verplichtingen.

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

6. Andere financiële entiteiten dan micro-ondernemingen beschikken over een functie voor crisisbeheer***, hetzij als een specifieke functie, hetzij als een onderdeel van de functies die verantwoordelijk zijn voor respons op en beheer van incidenten. De functie voor crisisbeheer bepaalt*** in geval van activering van het beleid inzake ICT-bedrijfscontinuïteit of van het ICT-noodherstelplan in overeenstemming met artikel 13 duidelijke procedures voor het beheer van interne en externe crisiscommunicatie ▌.

7. Financiële entiteiten houden registers bij van hun ***relevante*** activiteiten vóór en tijdens storingen wanneer hun ICT-bedrijfscontinuïteitsbeleid of ICT-noodherstelplan wordt geactiveerd. Deze registers worden op eenvoudige wijze beschikbaar gesteld.

8. De in artikel 2, lid 1, punt f), bedoelde financiële entiteiten verstrekken de bevoegde autoriteiten afschriften van de resultaten van de ICT-bedrijfscontinuïteitstests of soortgelijke oefeningen die plaatsvinden tijdens de verslagperiode.

9. Andere financiële entiteiten dan micro-ondernemingen melden aan de bevoegde autoriteiten alle ***geraamde financiële*** kosten en verliezen als gevolg van ***zware*** ICT-verstoringen en ***ernstige*** ICT-gerelateerde incidenten.

9 bis. De ETA's stellen via het Gemengd Comité gemeenschappelijke richtsnoeren op inzake de methode voor het berekenen van de kosten en het kwantificeren van de verliezen als bedoeld in lid 9.

Artikel 11

Back-upbeleid en herstelmethoden

1. Teneinde het herstel van ICT-systemen te verzekeren met een minimale uitval en een beperkte verstoring, ontwikkelen financiële entiteiten als onderdeel van hun ICT-risicobeheerkader:

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

   b) herstelmethoden.

2. ***In overeenstemming met het in lid 1, punt a), bedoelde back-upbeleid starten*** back-upsystemen ▌onverwijld met de verwerking, tenzij de start van de verwerking de beveiliging van het netwerk en van de informatiesystemen of de integriteit of de vertrouwelijkheid van gegevens in gevaar zou brengen.

3. Wanneer financiële entiteiten back-upgegevens herstellen met behulp van eigen systemen, maken zij gebruik van ICT-systemen ***die fysiek of logisch van hun centrale ICT-systeem zijn gescheiden*** en die tegen ongeoorloofde toegang of beschadiging van ICT zijn beveiligd.

   Voor de in artikel 2, lid 1, punt g), bedoelde financiële entiteiten maken de herstelplannen het herstel van alle transacties mogelijk 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.

4. Financiële entiteiten ***evalueren de noodzaak om*** ICT-capaciteiten in reserve ***te houden*** met middelen, capaciteiten en functionaliteiten die toereikend en adequaat zijn om te voorzien in de zakelijke behoeften ***en te voldoen aan de vereisten inzake digitale operationele veerkracht zoals uiteengezet in deze verordening***.

5. De in artikel 2, lid 1, punt f), bedoelde financiële entiteiten handhaven ten minste één locatie voor secundaire verwerking, en zorgen ervoor dat hun derde aanbieders van ICT-diensten ten minste één locatie voor secundaire verwerking handhaven, met middelen, capaciteiten, functionaliteiten en personeelsvoorziening die toereikend en adequaat zijn 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 cruciale diensten 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 cruciale activiteiten verricht binnen het kader van de hersteldoelstellingen;

c) ▌toegankelijk voor het personeel van de financiële entiteit om de continuïteit van cruciale ***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 cruciale 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 ***zorgen*** financiële entiteiten ▌ervoor ▌dat het hoogste niveau van gegevensintegriteit wordt bereikt***, bijvoorbeeld door meerdere controles, waaronder afstemmingen, te verrichten***. 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 12

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 mogelijke gevolgen ervan voor hun digitale operationele veerkracht te analyseren.

2. Financiële entiteiten verrichten ***evaluaties van ernstige*** ICT-gerelateerde ***incidenten*** na zware ICT-verstoringen van hun kernactiviteiten, 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 10.

Bij het invoeren van veranderingen ***met betrekking tot de aanpak van ICT-risico's die aan het licht zijn gekomen bij evaluaties van ernstige ICT-gerelateerde incidenten,*** delen andere financiële entiteiten dan micro-ondernemingen ***alle belangrijke veranderingen*** mee aan de bevoegde autoriteiten***, waarbij zij gedetailleerd aangeven welke verbeteringen vereist zijn en hoe die verbeteringen verstoringen in de toekomst beogen te voorkomen of te beperken***. ***De kennisgeving van veranderingen aan de bevoegde autoriteiten kan plaatsvinden vóór of na de uitvoering van de veranderingen.***

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 forensische analyses;

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 23 en 24 uitgevoerde tests op de operationele digitale veerkracht 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 bedrijfscontinuïteits- of herstelplannen, samen met relevante informatie die met tegenpartijen wordt uitgewisseld en tijdens toetsingen in het toezicht wordt beoordeeld. Deze bevindingen geven aanleiding tot passende herzieningen van relevante onderdelen van het kader voor ICT-risicobeheer als bedoeld in artikel 5, lid 1.

4. Financiële entiteiten zien toe erop toe dat hun strategie voor digitale veerkracht als bedoeld in artikel 5, lid 9, op doeltreffende wijze wordt uitgevoerd. Zij inventariseren de ontwikkeling van ICT-risico's in de tijd, ***met inbegrip van de afstand van deze risico's tot cruciale of belangrijke functies,*** 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 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 veerkracht als verplichte modules in de opleidingsprogramma's voor het personeel. ***De bewustmakingsprogramma's op het gebied van ICT-beveiliging zijn van toepassing op al het personeel. De opleidingen inzake digitale operationele veerkracht*** zijn ***minstens*** van toepassing op alle werknemers ***met rechtstreekse toegang tot de ICT-systemen*** en op het hoger leidinggevend personeel. ***De complexiteit van de opleidingsmodules staat in verhouding tot het niveau van rechtstreekse toegang van de personeelsleden tot de ICT-systemen en houdt met name rekening met hun toegang tot cruciale of belangrijke functies.***

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 veerkracht. 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 13

Communicatie

1. Als onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 5, lid 1, beschikken financiële entiteiten over communicatieplannen die het mogelijk maken ***ten minste ernstige*** ICT-gerelateerde incidenten of ernstige kwetsbaarheden op verantwoordelijke wijze bekend te maken aan cliënten en tegenpartijen en, in voorkomend geval, aan het publiek.

   De in de eerste alinea bedoelde communicatieplannen zorgen er ook voor dat aan cliënten en tegenpartijen jaarlijks een samenvatting van alle ICT-gerelateerde incidenten wordt verstrekt. Bij een dergelijke openbaarmaking wordt het bedrijfsgeheim van de financiële entiteit en van haar cliënten en tegenpartijen volledig in acht genomen en wordt het in artikel 5, lid 1, bedoelde kader voor ICT-risicobeheer niet in gevaar gebracht.

2. Als onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 5, lid 1, voeren financiële entiteiten een communicatiebeleid in voor het 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 respons en herstel, en personeel dat moet worden geïnformeerd.

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

Artikel 14

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

De Europese Bankautoriteit (EBA), de Europese Autoriteit voor effecten en markten (ESMA) en de Europese Autoriteit voor verzekeringen en bedrijfspensioenen (Eiopa) stellen, in overleg met het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), 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 8, lid 2, teneinde de veiligheid van netwerken te garanderen, passende waarborgen tegen inbreuken en misbruik van gegevens mogelijk te maken, de authenticiteit en de integriteit 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;

d) verdere onderdelen van de controle van rechten voor toegangsbeheer als bedoeld in artikel 8, 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 ICT-risico's via passende indicatoren, onder meer voor patronen en uren van netwerkgebruik, IT-activiteit en onbekende toestellen;

e) de elementen als bedoeld in artikel 9, lid 1, om een snelle detectie van afwijkende activiteiten mogelijk te maken, verder te ontwikkelen alsmede de criteria als bedoeld in artikel 9, lid 2, om processen voor detectie van ICT-gerelateerde incidenten en respons daarop in werking te stellen;

f) de onderdelen van het ICT-bedrijfscontinuïteitsbeleid als bedoeld in artikel 10, lid 1, verder te specificeren;

g) het testen van de ICT-bedrijfscontinuïteitsplannen als bedoeld in artikel 10, lid 5, verder te specificeren om ervoor te zorgen dat naar behoren rekening wordt gehouden met scenario's waarin de kwaliteit van voorziening van een cruciale 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;

h) de onderdelen van het ICT-noodherstelplan als bedoeld in artikel 10, lid 3, verder te specificeren.

De EBA, de ESMA en de Eiopa leggen deze ontwerpen van technische reguleringsnormen uiterlijk op [*OJ: insert date 1 year after the date of entry into force*] voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om 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 14 bis

Kader voor ICT-risicobeheer voor kleine, niet-verweven en vrijgestelde entiteiten

1. Overeenkomstig artikel 3 bis ontwerpen en onderhouden kleine en niet-verweven beleggingsondernemingen, betalingsinstellingen die vrijgesteld zijn krachtens Richtlijn (EU) 2015/2366, kredietinstellingen die vrijgesteld zijn krachtens Richtlijn 2013/36/EU, instellingen voor elektronisch geld die vrijgesteld zijn krachtens Richtlijn 2009/110/EG, en kleine instellingen voor bedrijfspensioenvoorziening een solide en gedocumenteerd kader voor ICT-risicobeheer:

a) waarin de mechanismen en maatregelen gericht op een snel, efficiënt en alomvattend beheer van alle ICT-risico's nauwkeurig worden beschreven, met inbegrip van de bescherming van relevante fysieke componenten en infrastructuur;

b) waarmee voortdurend toezicht wordt gehouden op de beveiliging en werking van alle ICT-systemen;

c) waarmee de gevolgen van ICT-risico's tot een minimum worden beperkt door solide, veerkrachtige en geactualiseerde ICT-systemen, -protocollen en -instrumenten te gebruiken die geschikt zijn voor het ondersteunen van de prestaties van hun activiteiten en de levering van diensten;

d) waarmee de vertrouwelijkheid, integriteit en beschikbaarheid van gegevensnetwerk- en informatiesystemen naar behoren worden beschermd;

e) waarmee bronnen van risico en anomalieën in de netwerk- en informatiesystemen zo spoedig mogelijk kunnen worden geïdentificeerd en gedetecteerd en ICT-incidenten snel kunnen worden afgehandeld.

2. Het in lid 1 bedoelde kader voor ICT-risicobeheer wordt ten minste eenmaal per jaar gedocumenteerd en geëvalueerd, alsook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en om de toezichtinstructies of -conclusies van relevante tests of auditprocessen op het gebied van digitale operationele veerkracht te monitoren. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen.

Jaarlijks wordt bij de bevoegde autoriteit een verslag over de evaluatie van het kader voor ICT-risicobeheer ingediend.

HOOFDSTUK III

ICT-GERELATEERDE INCIDENTEN

BEHEER, CLASSIFICATIE EN RAPPORTAGE

Artikel 15

Beheerproces voor ICT-gerelateerde incidenten

1. Financiële entiteiten stellen een beheerproces voor ICT-gerelateerde incidenten vast en leggen dit ten uitvoer om ICT-gerelateerde incidenten te detecteren, te beheren en te melden, en voeren indicatoren voor vroegtijdige waarschuwing in als alarmmelding.

2. 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 ***en aangepakt*** teneinde dergelijke incidenten te voorkomen.

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

   a) procedures vast te stellen om ICT-gerelateerde incidenten te identificeren, te detecteren, te categoriseren en te klasseren op basis van hun prioriteit en de ernst en het cruciale karakter van de getroffen diensten in overeenstemming met de in artikel 16, lid 1, bedoelde criteria;

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

   c) plannen op te stellen voor communicatie met personeel, externe belanghebbenden en media in overeenstemming met artikel 13, en voor mededeling aan cliënten, interne escalatieprocedures, met inbegrip van ICT-gerelateerde klachten van cliënten, alsmede voor verstrekking van informatie, indien noodzakelijk, aan financiële entiteiten die optreden als tegenpartijen;

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

   e) 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 16

Classificatie van ICT-gerelateerde incidenten

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

   a) het aantal gebruikers of financiële tegenpartijen die door de verstoring ten gevolge van het ICT-gerelateerde incident zijn getroffen ▌ ;

   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, zoals verlies aan integriteit, vertrouwelijkheid of beschikbaarheid;

   e) de ernst van de effecten van het ICT-gerelateerde incident op de ICT-systemen van de financiële entiteit;

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

   g) de economische effecten van het ICT-gerelateerde incident in absolute en relatieve termen.

2. De ETA's stellen via het Gemengd Comité van de ETA's ("Gemengd Comité") en ***in coördinatie*** met de Europese Centrale Bank (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 waarvoor de rapportageverplichting van artikel 17, lid 1, geldt;

   b) de door de bevoegde autoriteiten toe te passen criteria voor de beoordeling van de relevantie van ernstige ICT-gerelateerde incidenten voor de rechtsgebieden van andere lidstaten, en de nadere informatie van verslagen over ***ernstige*** ICT-gerelateerde incidenten die overeenkomstig artikel 17, punten 5) en 6), aan andere bevoegde autoriteiten moeten worden meegedeeld.

3. Bij het opstellen van de in lid 2 bedoelde gemeenschappelijke ontwerpen van technische reguleringsnormen houden de ETA's rekening met internationale normen en specificaties die door Enisa zijn ontwikkeld en gepubliceerd, met inbegrip van, in voorkomend geval, specificaties voor andere economische sectoren. ***De ETA's houden er verder rekening mee dat het tijdige en efficiënte beheer van een incident door kleine ondernemingen en micro-ondernemingen niet wordt beperkt doordat aan de classificatievereisten van dit artikel moet worden voldaan. De ETA's houden ook rekening met de omvang van financiële entiteiten, de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen, en hun algemene risicoprofiel.***

   De ETA's leggen die gemeenschappelijke ontwerpen van technische reguleringsnormen uiterlijk op [PO: insert date ***2 years*** after the date of entry into force] voor aan de Commissie.

Aan de Commissie wordt de bevoegdheid gedelegeerd om deze verordening aan te vullen door de in lid 2 bedoelde technische reguleringsnormen overeenkomstig de artikelen 10 tot en met 14 van respectievelijk Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 vast te stellen.

Artikel 17

Rapportage van ernstige ICT-gerelateerde incidenten

1. Financiële entiteiten melden ernstige ICT-gerelateerde incidenten binnen de in lid 3 vastgestelde termijnen aan de relevante bevoegde autoriteit als bedoeld in artikel 41.

   Voor de toepassing van de eerste alinea stellen financiële entiteiten, na het verzamelen en analyseren van alle relevante informatie, een incidentverslag op met gebruikmaking van het model als bedoeld in artikel 18, en dienen zij dit in bij de bevoegde autoriteit.

   Het verslag bevat 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.

1 bis. 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, gebruikers van diensten of cliënten. De relevante bevoegde autoriteit kan dergelijke informatie overeenkomstig lid 5 aan andere relevante autoriteiten verstrekken.

2. Wanneer een ernstig ICT-gerelateerd incident ***optreedt en materiële*** gevolgen heeft ▌voor de financiële belangen van gebruikers van diensten en van cliënten, stellen financiële entiteiten hun gebruikers van diensten en hun cliënten onverwijld ***nadat zij het hebben vastgesteld,*** in kennis van het ernstige ICT-gerelateerde incident en melden zij hun ***de pertinente*** maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk incident te beperken. ***Indien er dankzij de tegenmaatregelen die de financiële entiteit heeft genomen geen schade voor gebruikers van diensten en cliënten ontstaat, is de vereiste om gebruikers van diensten en cliënten in kennis te stellen niet van toepassing.***

3. Financiële entiteiten verstrekken de bevoegde autoriteit als bedoeld in artikel 41:

   a) een eerste kennisgeving van ***het ernstige ICT-gerelateerde*** incident***, met informatie waarover de kennisgevende entiteit naar best vermogen beschikt, en wel als volgt:***

      i) met betrekking tot incidenten die de beschikbaarheid van de door de financiële entiteit verleende diensten aanzienlijk verstoren, wordt de bevoegde autoriteit onverwijld en in elk geval binnen 24 uur na de vaststelling van het incident in kennis gesteld;

      ii) met betrekking tot incidenten die aanzienlijke gevolgen hebben voor de financiële entiteit, maar niet voor de beschikbaarheid van de door die entiteit verleende diensten, wordt de bevoegde autoriteit onverwijld en in elk geval binnen 72 uur na de vaststelling van het incident in kennis gesteld;

iii) met betrekking tot incidenten die gevolgen hebben voor de integriteit, vertrouwelijkheid of beveiliging van door die financiële entiteit bewaarde persoonsgegevens, wordt de bevoegde autoriteit onverwijld en in elk geval binnen 24 uur na de vaststelling van het incident in kennis gesteld;

b) een tussentijds verslag, ***zodra de status van het oorspronkelijke incident ingrijpend is gewijzigd of nieuwe informatie aan het licht is gekomen die van grote invloed kan zijn op de wijze waarop het ICT-gerelateerde incident door de bevoegde autoriteit wordt aangepakt,*** na de eerste kennisgeving als bedoeld in punt a), 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 ten uitvoer zijn gelegd, en wanneer de werkelijke impactcijfers beschikbaar zijn in plaats van ramingen, maar niet later dan één maand na de ***datum van*** verzending van het eerste verslag.

c bis) in het geval van een incident dat nog loopt op het moment dat het in punt c) bedoelde eindverslag wordt ingediend, uiterlijk één maand nadat het incident is opgelost een eindverslag.

De in artikel 41 bedoelde relevante bevoegde autoriteit bepaalt dat het een financiële entiteit in naar behoren gemotiveerde gevallen is toegestaan af te wijken van de in de punten a), b), c) en c bis) van dit lid vastgestelde termijnen, waarbij zij rekening houdt met het vermogen van financiële entiteiten om correcte en zinvolle informatie te verstrekken over ernstige ICT-gerelateerde incidenten.

4. Financiële entiteiten mogen de rapportageverplichtingen uit hoofde van dit artikel alleen aan een derde aanbieder van diensten delegeren na goedkeuring van de delegatie door de relevante bevoegde autoriteit als bedoeld in artikel 41. ***In het geval van een dergelijke delegatie blijft de financiële entiteit volledig verantwoordelijk voor het naleven van de vereisten inzake incidentrapportage.***

5. Na ontvangst van het in lid 1 bedoelde verslag verstrekt de bevoegde autoriteit onverwijld nadere bijzonderheden over het ***ernstige ICT-gerelateerde*** incident aan:

a) de EBA, de ESMA of de Eiopa, naargelang van het geval;

b) de ECB, indien nodig, in het geval van financiële entiteiten als bedoeld in artikel 2, lid 1, punten a), b) en c); en

c) het krachtens artikel 8 van Richtlijn (EU) 2016/1148 aangewezen centraal contactpunt ***of krachtens artikel 9 van Richtlijn (EU) 2016/1149 aangewezen CSIRT's;***

c bis) de afwikkelingsautoriteit die verantwoordelijk is voor de betrokken financiële entiteit, de Gemeenschappelijke Afwikkelingsraad (GAR) met betrekking tot

entiteiten als bedoeld in artikel 7, lid 2, van Verordening (EU) nr. 806/2014 en wat betreft entiteiten en groepen als bedoeld in artikel 7, lid 4, punt b), en lid 5, van Verordening (EU) nr. 806/2014, indien aan de voorwaarden voor de toepassing van die leden is voldaan;

c ter) de nationale afwikkelingsautoriteiten met betrekking tot entiteiten en groepen als bedoeld in artikel 7, lid 3, van Verordening (EU) nr. 806/2014. De nationale afwikkelingsautoriteiten verstrekken de GAR elk kwartaal een samenvatting van de verslagen die zij uit hoofde van dit punt hebben ontvangen met betrekking tot entiteiten als bedoeld in artikel 7, lid 3, van Verordening (EU) nr. 806/2014;

c quater) andere relevante overheidsinstanties, waaronder die in andere lidstaten.

6. De EBA, de ESMA of de Eiopa en de ECB***, in samenwerking met Enisa,*** beoordelen de relevantie van het ernstige ICT-gerelateerde incident voor andere betrokken overheidsinstanties en stellen hen 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.

Artikel 18

Harmonisatie van inhoud en modellen van rapportage

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

a) gemeenschappelijke ontwerpen van technische reguleringsnormen om:

(1) de inhoud van de rapportage voor ernstige ICT-gerelateerde incidenten vast te stellen;

(2) verder te specificeren onder welke voorwaarden financiële entiteiten, na voorafgaande goedkeuring door de bevoegde autoriteit, de in dit hoofdstuk vastgestelde rapportageverplichtingen aan een derde aanbieder van diensten mogen delegeren;

(3) de criteria voor het bepalen van de gevolgen van een ernstig ICT-gerelateerd incident voor een financiële entiteit verder te specificeren voor de toepassing van artikel 17, lid 3, punt a).

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

De ETA's leggen de gemeenschappelijke ontwerpen van technische reguleringsnormen bedoeld in ▌ punt a) ***van de eerste alinea*** en de gemeenschappelijke ontwerpen van technische uitvoeringsnormen bedoeld in ▌ punt b) ***van de eerste alinea*** uiterlijk op xx 202x [PO: insert date ***2*** years after the date of entry into force] voor aan de Commissie.

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

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

2. In afwachting van het resultaat van het in artikel 19 bedoelde haalbaarheidsverslag over de verdere centralisatie van de incidentrapportage ontwikkelen de ETA's, via het Gemengd Comité en in samenwerking met de bevoegde autoriteiten, de ECB, de GAR en Enisa, richtsnoeren voor de uitwisseling van informatie over meldingen van belangrijke ICT-gerelateerde incidenten overeenkomstig artikel 17, lid 5.

In de in de eerste alinea bedoelde richtsnoeren wordt ten minste het volgende in overweging genomen:

a) de meest efficiënte communicatielijnen;

b) het behoud van de beveiliging, vertrouwelijkheid en integriteit van de uitgewisselde gegevens;

c) het mogelijk betrekken van financiële entiteiten om de in artikel 40 bedoelde uitwisseling van informatie aan te vullen.

Artikel 19

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 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 verslag bevat ten minste het volgende:

a) de vereisten voor de oprichting van ***één*** EU-hub;

b) de voordelen, beperkingen en mogelijke risico's;

b bis) het vermogen om de interoperabiliteit te bewerkstelligen en de meerwaarde ervan ten opzichte van andere relevante rapportageregelingen, waaronder Richtlijn (EU) 2016/1148, te beoordelen;

c) elementen van operationeel beheer;

d) de voorwaarden voor het lidmaatschap;

e) regels voor financiële entiteiten en nationale bevoegde autoriteiten om toegang tot ***de ene*** EU-hub te verkrijgen;

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

3. De ETA's leggen het verslag bedoeld in lid 1 uiterlijk op xx 202x [OJ: insert date 3 years after the date of entry into force] voor aan de Commissie, het Europees Parlement en de Raad.

Artikel 20

Feedback van toezichthouders

1. Na ontvangst van een verslag als bedoeld in artikel 17, lid 1, bevestigt de bevoegde autoriteit de ontvangst van de melding en verstrekt zij zo spoedig mogelijk alle nodige feedback of richtsnoeren aan de financiële entiteit, met name om maatregelen op het niveau van de entiteit te bespreken of te onderzoeken hoe de nadelige effecten in alle sectoren zoveel mogelijk kunnen worden beperkt ***en verstrekt zij ook naar behoren geanonimiseerde feedback, inzicht en inlichtingen aan de relevante financiële entiteiten waar dat bevorderlijk kan zijn, gebaseerd op de meldingen van ernstige ICT-gerelateerde incidenten die zij ontvangt***.

2. De ETA's brengen jaarlijks via het Gemengd Comité een geanonimiseerd en geaggregeerd verslag uit over de meldingen van ***ernstige*** ICT-gerelateerde incidenten die zij van de bevoegde autoriteiten hebben ontvangen, met vermelding van ten minste het aantal ***ernstige*** ICT-gerelateerde incidenten, de aard ervan, de gevolgen voor de werking van financiële entiteiten of cliënten, de ***geraamde*** kosten en de genomen corrigerende maatregelen.

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

Artikel 20 bis

Betalingsgerelateerde operationele of beveiligingsincidenten met betrekking tot bepaalde financiële entiteiten

De in dit hoofdstuk III vastgestelde vereisten zijn van toepassing op betalingsgerelateerde operationele of beveiligingsincidenten en op ernstige betalingsgerelateerde operationele of beveiligingsincidenten wanneer zij financiële entiteiten als bedoeld in artikel 2, lid 1, punten a), b) en c), betreffen.

HOOFDSTUK IV

TESTEN VAN DIGITALE OPERATIONELE VEERKRACHT

Artikel 21

Algemene vereisten voor uitvoering van tests van digitale operationele veerkracht

1. Voor de beoordeling van de paraatheid ten aanzien van ICT-gerelateerde incidenten, de omschrijving van zwakheden, gebreken of lacunes in de digitale operationele veerkracht en de snelle tenuitvoerlegging van corrigerende maatregelen zorgen ***andere*** financiële entiteiten ***dan micro-ondernemingen*** voor het vaststellen, handhaven en evalueren van een degelijk en alomvattend programma voor het testen van de digitale operationele veerkracht als integrerend onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 5.

2. Het testprogramma voor digitale operationele veerkracht omvat een reeks beoordelingen, tests, methodologieën, praktijken en instrumenten die overeenkomstig de bepalingen van de artikelen 22 en 23 moeten worden toegepast.

3. Financiële entiteiten volgen bij de uitvoering van het in lid 1 bedoelde testprogramma voor digitale operationele veerkracht een risicogebaseerde benadering, waarbij rekening wordt gehouden met het veranderende landschap van ICT-risico's, eventuele specifieke risico's waaraan de financiële entiteit wordt of kan worden blootgesteld, de cruciale aard van informatieactiva en verleende diensten, alsmede alle andere factoren die de financiële entiteit passend acht.

4. Financiële entiteiten 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. Financiële entiteiten stellen procedures en beleidslijnen vast om alle problemen die tijdens de uitvoering van de tests zijn erkend, te prioriteren, te classificeren en aan te pakken, en stellen interne valideringsmethoden vast om na te gaan of alle vastgestelde zwakheden, gebreken of lacunes volledig worden aangepakt.

6. Financiële entiteiten ***zorgen ervoor dat*** ten minste eenmaal per jaar ***passende tests worden uitgevoerd op*** alle cruciale ICT-systemen en -toepassingen.

Artikel 22

Testen van ICT-instrumenten en -systemen

1. Het testprogramma voor digitale operationele veerkracht bedoeld in artikel 21 voorziet in de uitvoering van een volledige reeks passende tests***.***

Die tests kunnen kwetsbaarheidsbeoordelingen en -scans, opensourceanalyses, netwerkbeveiligingsbeoordelingen, kloofanalyses, beoordelingen van fysieke beveiliging, vragenlijsten en scanningsoftwareoplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests, eind-tot-eindtests of penetratietests ***omvatten***.

2. De in artikel 2, lid 1, punten f) en g), bedoelde financiële entiteiten verrichten kwetsbaarheidsbeoordelingen voordat nieuwe of bestaande diensten ter ondersteuning van cruciale functies, toepassingen en infrastructuurcomponenten van de financiële entiteit worden ingezet of opnieuw worden ingezet.

Artikel 23

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

1. Overeenkomstig ***de tweede alinea van*** lid ***3*** aangewezen financiële entiteiten verrichten ten minste om de drie jaar geavanceerde tests door middel van dreigingsgestuurde penetratietests.

2. Dreigingsgestuurde penetratietests hebben ten minste betrekking op de cruciale ***of belangrijke*** functies en diensten van een financiële entiteit en worden***, indien dat mogelijk is,*** uitgevoerd op systemen die prestaties in het reële leven verrichten ter ondersteuning van deze functies ***of op preproductiesystemen met dezelfde beveiligingsconfiguratie***. De precieze omvang van dreigingsgestuurde penetratietests, op basis van de beoordeling van cruciale ***of belangrijke*** functies en diensten, wordt door financiële entiteiten vastgesteld en wordt door de bevoegde autoriteiten gevalideerd. ***Het is niet vereist dat één enkele*** dreigingsgestuurde penetratietest ***alle cruciale of belangrijke functies bestrijkt.***

   Voor de toepassing van de eerste alinea bepalen financiële entiteiten alle relevante onderliggende ICT-processen, -systemen en technologieën ter ondersteuning van cruciale ***of belangrijke*** functies en diensten, met inbegrip van uitbestede of met derde aanbieders van ICT-diensten contractueel overeengekomen ***cruciale of belangrijke*** functies en diensten.

   Wanneer ***cruciale*** derde aanbieders van ICT-diensten ***en, indien nodig, niet-cruciale derde aanbieders van ICT-diensten*** binnen het toepassingsgebied van de dreigingsgestuurde penetratietests vallen, neemt de financiële entiteit de nodige maatregelen om de deelname van deze aanbieders te waarborgen. ***Deze derde aanbieders van ICT-diensten zijn niet verplicht informatie mee te delen of details te verstrekken over kwesties die niet relevant zijn voor de risicobeheerscontroles van de relevante cruciale of belangrijke functies van de betreffende financiële entiteiten. Dergelijke tests mogen geen nadelige gevolgen hebben voor andere gebruikers van de derde aanbieders van ICT-diensten.***

   In gevallen waarin de betrokkenheid van een derde aanbieder van ICT-diensten bij de dreigingsgestuurde penetratietests potentieel gevolgen kan hebben voor de kwaliteit, vertrouwelijkheid of beveiliging van de diensten die de derde aanbieder van ICT-diensten levert aan andere cliënten die niet binnen het toepassingsgebied van deze verordening vallen, of voor algemene integriteit van de activiteiten van de derde aanbieder van ICT-diensten, kunnen de financiële entiteit en de derde aanbieder van ICT-diensten contractueel overeenkomen dat het de derde aanbieder van ICT-diensten is toegestaan rechtstreeks contractuele regelingen te treffen met een externe tester. Derde aanbieders van ICT-diensten mogen dergelijke regelingen

treffen namens alle financiële entiteiten die hun diensten gebruiken, teneinde gecombineerde tests uit te voeren.

Financiële entiteiten passen doeltreffende risicobeheercontroles toe om de risico's van potentiële effecten op gegevens, schade aan activa en verstoring van cruciale ***of belangrijke functies*** of activiteiten bij de financiële entiteit zelf, bij haar tegenpartijen of in de financiële sector te ***mitigeren***.

Na afloop van de test, nadat overeenstemming is bereikt over verslagen en correctieplannen, verstrekken de financiële entiteit en de externe testers aan ***de overeenkomstig lid 3 bis aangewezen ene overheidsinstantie of, in het geval van derde aanbieders van ICT-diensten die rechtstreeks contractuele regelingen met externe testers treffen, aan Enisa een vertrouwelijke samenvatting van de testresultaten en*** de documenten waarmee wordt bevestigd dat de dreigingsgestuurde penetratietests in overeenstemming met de vereisten zijn verricht. De ***ene overheidsinstantie of Enisa, naargelang het geval, geeft*** een attest af ***waarin wordt bevestigd dat de test in overeenstemming met de op de documentatie gebaseerde vereisten is verricht om de wederzijdse erkenning van dreigingsgestuurde penetratietests tussen bevoegde autoriteiten mogelijk te maken***. ***Het attest wordt gedeeld met de bevoegde autoriteit van de financiële entiteit en, in voorkomend geval, met de leidende toezichthouder van de cruciale derde aanbieder van ICT-diensten.***

3. Financiële entiteiten***, of derde aanbieders van ICT-diensten die overeenkomstig lid 2 van dit artikel rechtstreeks contractuele regelingen met een externe tester mogen treffen,*** stellen overeenkomstig artikel 24 testers aan om dreigingsgestuurde penetratietests te verrichten.

Onverminderd de mogelijkheid om taken en bevoegdheden uit hoofde van dit artikel te delegeren aan andere bevoegde autoriteiten die met dreigingsgestuurde penetratietests belast zijn, bepalen de bevoegde autoriteiten ▌ welke financiële entiteiten op ***evenredige*** wijze dreigingsgestuurde penetratietests verrichten ▌ op basis van een beoordeling van:

a) effectgerelateerde factoren, met name het cruciale karakter van de diensten en de activiteiten van de financiële entiteit;

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

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

3 bis. De lidstaten wijzen één overheidsinstantie aan die op nationaal niveau verantwoordelijk is voor dreigingsgestuurde penetratietests in de financiële sector, met uitzondering van de identificatie van financiële entiteiten overeenkomstig lid 3, met inbegrip van dreigingsgestuurde penetratietests die worden uitgevoerd door financiële entiteiten en door derde aanbieders van ICT-diensten die rechtstreeks contractuele regelingen met externe testers treffen. De aangewezen ene overheidsinstantie wordt daartoe belast met alle nodige bevoegdheden en taken.

4. De ***ETA's*** ontwikkelen***, in coördinatie met Enisa,*** na raadpleging van de ECB en rekening houdend met de desbetreffende kaders in de Unie die van toepassing zijn op ***dreigingsgestuurde*** penetratietests, ***waaronder het TIBER-EU-kader, één reeks*** ontwerpen van technische reguleringsnormen tot nadere bepaling van:

a) de voor de toepassing van de tweede alinea van lid 3 van dit artikel gebruikte criteria;

b) de voorschriften met betrekking tot:

i) de toepassingssfeer van de dreigingsgestuurde penetratietests bedoeld in lid 2 van dit artikel;

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;

c) het soort samenwerking op het gebied van toezicht dat noodzakelijk is om dreigingsgestuurde penetratietests ten uitvoer te leggen ***en de wederzijdse erkenning ervan te vergemakkelijken*** in het geval van financiële entiteiten die in meer dan een lidstaat actief zijn ***en tests die worden uitgevoerd door externe testers die overeenkomstig lid 2 van dit artikel rechtstreeks contractuele regelingen met derde aanbieders van ICT-diensten hebben getroffen***, teneinde een passend niveau van betrokkenheid van toezichthouders en een flexibele tenuitvoerlegging mogelijk te maken rekening houdend met de specifieke kenmerken van financiële subsectoren of lokale financiële markten.

De ETA's leggen die gemeenschappelijke ontwerpen van technische reguleringsnormen uiterlijk op [OJ: insert date ***6*** months before the date of entry into force] voor aan de Commissie.

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

Artikel 24

Vereisten voor testers

1. Financiële entiteiten ***en derde aanbieders van ICT-diensten die overeenkomstig artikel 23, lid 2, rechtstreeks contractuele regelingen met externe testers mogen treffen,*** maken voor het uitvoeren van dreigingsgestuurde penetratietests alleen gebruik van testers die:

a) in de hoogste mate geschikt en deugdzaam zijn;

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

c) door een accrediteringsinstantie in een lidstaat zijn gecertificeerd of formele gedragscodes of ethische kaders in acht nemen***, ongeacht of de testers uit de Unie dan wel uit een derde land komen***;

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

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

e bis) in het geval van interne testers, mogen worden gebruikt van de relevante bevoegde autoriteit en de overeenkomstig artikel 23, lid 3 bis, aangewezen ene overheidsinstantie, en mits die autoriteiten hebben geverifieerd dat de financiële entiteit voldoende middelen heeft ingezet en ervoor heeft gezorgd dat belangenconflicten gedurende de hele ontwerp- en uitvoeringsfase van de test worden voorkomen.

2. Financiële entiteiten ***en derde aanbieders van ICT-diensten die overeenkomstig artikel 23, lid 2, rechtstreeks contractuele regelingen met externe testers mogen treffen,*** zorgen ervoor dat de ▌ met externe testers ***getroffen regelingen*** een degelijk beheer van de resultaten van de dreigingsgestuurde penetratietests opleggen en dat de verwerking daarvan, met inbegrip van het genereren, ontwerpen, opslaan, aggregeren, rapporteren, communiceren of vernietigen van resultaten, geen risico's voor de financiële entiteit meebrengt.

HOOFDSTUK V

BEHEER VAN ICT-RISICO VAN DERDE AANBIEDER

AFDELING I

BASISBEGINSELEN VOOR EEN DEGELIJK BEHEER VAN HET ICT-RISICO VAN DERDE AANBIEDER

Artikel 25

Algemene beginselen

Financiële entiteiten beheren het ICT-risico van derde aanbieders als integrerend onderdeel van het ICT-risico binnen hun kader voor ICT-risicobeheer en in overeenstemming met de volgende beginselen:

1. Financiële entiteiten die contractuele regelingen 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 de toepasselijke wetgeving inzake financiële diensten.

2. Het beheer van het ICT-risico van derde aanbieders door financiële entiteiten wordt ten uitvoer gelegd aan de hand van het evenredigheidsbeginsel, rekening houdend met:

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

b) de risico's die voortvloeien uit contractuele regelingen met derde aanbieders inzake het gebruik van ICT-diensten, rekening houdend met het cruciale karakter of het belang van de respectieve diensten, processen of functies en met de potentiële gevolgen voor de continuïteit en de kwaliteit van financiële diensten en activiteiten, op individueel en groepsniveau***;***

b bis) de vraag of een aanbieder van ICT-diensten een aanbieder van ICT-diensten binnen een groep is.

3. Als onderdeel van hun kader voor ICT-risicobeheer stellen financiële entiteiten die geen kleine micro-ondernemingen zijn een strategie inzake ICT-risico van derde aanbieders vast en herzien zij deze regelmatig ▌. Die strategie omvat een beleid inzake het gebruik van door derde aanbieders verleende ICT-diensten en is van toepassing op individuele en, in voorkomend geval, op gesubconsolideerde en geconsolideerde basis. Het leidinggevend orgaan evalueert regelmatig de vastgestelde risico's met betrekking tot de uitbesteding van cruciale of belangrijke functies.

4. 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 regelingen over het gebruik van door derde aanbieders verleende ICT-diensten ***die cruciale of belangrijke functies ondersteunen***.

De in de eerste alinea bedoelde contractuele regelingen worden naar behoren

gedocumenteerd ▌.

Tot de inwerkingtreding van de in lid 10, bedoelde technische uitvoeringsnormen volgen financiële entiteiten de door de ETA's en bevoegde autoriteiten uitgevaardigde richtsnoeren en andere maatregelen, indien die beschikbaar zijn.

Financiële entiteiten rapporteren ten minste jaarlijks aan de bevoegde autoriteiten over het aantal nieuwe regelingen inzake het gebruik van ICT-diensten ***die cruciale of belangrijke functies ondersteunen***, de categorieën van derde aanbieders van ICT-diensten, het soort contractuele regelingen en de 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 aanbestedingen van cruciale of belangrijke functies en van het feit dat een functie cruciaal of belangrijk is geworden.

5. Vóór het sluiten van een contractuele regeling inzake het gebruik van ICT-diensten:

   a) beoordelen financiële entiteiten of de contractuele regeling betrekking heeft op een cruciale of belangrijke functie;

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

   c) identificeren en beoordelen zij alle relevante risico's met betrekking tot de contractuele regeling, met inbegrip van de mogelijkheid dat deze contractuele regelingen kunnen leiden tot een versterking van het ICT-concentratierisico;

   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 regeling.

6. Financiële entiteiten mogen alleen contractuele regelingen sluiten met derde aanbieders van ICT-diensten die voldoen aan strenge, passende en ***actuele*** normen op het gebied van informatiebeveiliging. ***Om te bepalen of de gehanteerde beveiligingsnormen passend zijn, worden ook de meest recente normen in aanmerking genomen.***

7. Bij het uitoefenen van toegangs-, inspectie- en auditrechten ten aanzien van de derde aanbieder van ICT-diensten ***met betrekking tot cruciale of belangrijke functies,*** bepalen financiële entiteiten op basis van een risicogebaseerde benadering vooraf de frequentie van de audits en inspecties en 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 controlenormen.

   Voor contractuele regelingen die een ***gedetailleerde*** technologische complexiteit

inhouden, verifieert de financiële entiteit of interne auditors, pools van auditors of externe accountants over passende vaardigheden en kennis beschikken om de desbetreffende audits en beoordelingen doeltreffend uit te voeren.

8. Financiële entiteiten zorgen ervoor dat contractuele regelingen inzake het gebruik van ICT-diensten ***de financiële entiteiten in staat stellen om*** ten minste in de volgende omstandigheden ***passende corrigerende of remediërende maatregelen op grond van het toepasselijke recht te nemen, waaronder eventueel de volledige beëindiging van de regelingen indien geen rectificatie mogelijk is, of een gedeeltelijke beëindiging van de regelingen indien rectificatie mogelijk is***:

   a) bij ***een significante*** overtreding van de toepasselijke wetten, voorschriften of contractuele bepalingen door de derde aanbieder van ICT-diensten;

   a bis) een aanbeveling die overeenkomstig artikel 37 is uitgebracht door het orgaan voor gezamenlijk toezicht ten aanzien van een cruciale 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 regeling voorziet, met inbegrip van materiële wijzigingen die de regeling of de situatie van de derde aanbieder van ICT-diensten nadelig beïnvloeden;

   c) bij klaarblijkelijke zwakheden van de derde aanbieder van ICT-diensten ***met betrekking tot het*** algemene beheer van het ICT-risico ***van zijn contract met de financiële entiteit*** en in het bijzonder in de manier waarop de veiligheid en integriteit van vertrouwelijke, persoonlijke of anderszins gevoelige gegevens of niet-persoonsgebonden informatie wordt gewaarborgd;

   d) in omstandigheden waarin de bevoegde autoriteit ten gevolge van de desbetreffende contractuele regeling ***aantoonbaar*** niet langer doeltreffend toezicht op de financiële entiteit kan uitoefenen.

8 bis. Om het risico op verstoringen op het niveau van de financiële entiteit te verminderen, mag de financiële entiteit, in naar behoren gemotiveerde omstandigheden en met instemming van de bevoegde autoriteiten, besluiten de contractuele regelingen met de derde aanbieder van ICT-diensten niet te beëindigen totdat zij kan overstappen naar een andere derde aanbieder van ICT-diensten of op interne oplossingen die stroken met de complexiteit van de verleende dienst, overeenkomstig de in lid 9 bedoelde exitstrategie.

8 ter. In gevallen waarin contractuele regelingen met derde aanbieders van ICT-diensten in een van de in lid 8, punten a) tot en met d), genoemde gevallen worden beëindigd, komen de kosten van het weghalen van gegevens bij de derde aanbieder van ICT-diensten niet voor rekening van de financiële entiteiten indien die kosten hoger zijn dan de kosten van het weghalen van gegevens waarin het oorspronkelijke contract voorziet.

9. ***Voor ICT-diensten die verband houden met cruciale of belangrijke functies voeren*** financiële entiteiten ▌ exitstrategieën in***, die periodiek worden herzien***. ***In de***

exitstrategieën ***wordt*** rekening ***gehouden*** met risico's die zich op het niveau van de derde aanbieder van ICT-diensten kunnen voordoen, met name een mogelijk falen van deze aanbieder, een verslechtering van de kwaliteit van de geleverde functies, verstoring van de bedrijfsactiviteiten ten gevolge van ongeschikte of falende dienstverlening of materiële risico's in verband met de passende en permanente inzet van de functie***, of indien contractuele regelingen met derde aanbieders van ICT-diensten worden beëindigd onder een van de in lid 8, punten a) tot en met d), bedoelde omstandigheden***.

Financiële entiteiten zorgen ervoor dat zij de mogelijkheid hebben om contractuele regelingen 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 hun dienstverlening aan cliënten.

De exitstrategieën zijn alomvattend, gedocumenteerd en, indien nodig, voldoende getest.

Financiële entiteiten bepalen alternatieve oplossingen en ontwikkelen overgangsplannen die hen in staat stellen de contractueel geregelde functies 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 nemen passende noodmaatregelen om de bedrijfscontinuïteit te handhaven in alle omstandigheden als bedoeld in de eerste alinea.

10. De ETA's ontwikkelen via het Gemengd Comité ontwerpen van technische uitvoeringsnormen tot vaststelling van standaardmodellen ten behoeve van het in lid 4 bedoelde informatieregister.

De ETA's leggen die ontwerpen van technische uitvoeringsnormen uiterlijk op [OJ: insert date 1 year after the date of entry into force of this Regulation] 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 respectievelijk de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1095/2010 en (EU) nr. 1094/2010.

11. De ETA's ontwikkelen via het Gemengd Comité ontwerpen van reguleringsnormen tot nadere omschrijving van:

a) de gedetailleerde inhoud van het in lid 3 bedoelde beleid met betrekking tot contractuele regelingen inzake het gebruik van door derde aanbieders verleende ICT-diensten, aan de hand van de voornaamste stadia van de levenscyclus van de desbetreffende regelingen inzake het gebruik van ICT-diensten;

b) het soort informatie dat moet worden opgenomen in het in lid 4 bedoelde

informatieregister.

De ETA's leggen die ontwerpen van technische reguleringsnormen uiterlijk op [PO: insert date ***18 months*** after the date of entry into force] voor aan de Commissie.

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

Artikel 26

Voorlopige beoordeling van het ICT-concentratierisico en verdere ***uitbestedingsregelingen***

1. Bij het identificeren en beoordelen van het in artikel 25, lid 5, punt c), bedoelde ICT-concentratierisico houden financiële entiteiten rekening met de vraag of het sluiten van een contractuele regeling inzake ICT-diensten ***die cruciale 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 regelingen inzake de verlening van ICT-diensten ***die cruciale 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 veerkracht voorziet.

2. Wanneer de contractuele regeling inzake het gebruik van ICT-diensten ***die cruciale of belangrijke functies ondersteunen,*** de mogelijkheid inhoudt dat een derde aanbieder van ICT-diensten een cruciale of belangrijke taak verder uitbesteedt aan andere derde aanbieders van ICT-diensten, wegen de financiële entiteiten de baten en risico's af die uit een dergelijke mogelijke uitbesteding kunnen voortkomen ▌.

   Wanneer contractuele regelingen inzake het gebruik van ICT-diensten ***die cruciale of belangrijke functies ondersteunen,*** met een ▌ derde aanbieder van ICT-diensten worden gesloten, schenken financiële entiteiten ten minste aandacht aan de volgende factoren:

   a) ▌

   b) ▌

   c) bepalingen van insolventierecht die in geval van faillissement van de derde aanbieder van ICT-diensten van toepassing zouden zijn; ***en***

   d) beperkingen die zich met betrekking tot het dringende herstel van de gegevens van de financiële entiteit zouden kunnen voordoen.

Wanneer contractuele regelingen inzake het gebruik van ICT-diensten die cruciale

of belangrijke functies ondersteunen, worden gesloten met een in een derde land gevestigde derde aanbieder van ICT-diensten, houden financiële entiteiten, naast de in de eerste en tweede alinea bedoelde overwegingen, ook rekening met:

i) de naleving van de gegevensbeschermingsregels van de Unie; en

ii) de effectieve handhaving van de in deze verordening vervatte regels.

Wanneer dergelijke contractuele regelingen uitbesteding van cruciale of belangrijke functies behelzen, beoordelen financiële entiteiten ▌ of en hoe potentieel lange of complexe uitbestedingsketens van invloed kunnen zijn op hun vermogen om de ***in de tweede en derde alinea genoemde factoren*** volledig te evalueren en 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 27

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, dat de overeenkomsten inzake dienstverleningsniveau omvat, wordt ***schriftelijk vastgelegd en*** voor de partijen beschikbaar ***gesteld*** op papier of in een downloadbaar en toegankelijk formaat.

2. ***Financiële entiteiten en derde aanbieders van ICT-diensten zorgen ervoor dat*** contractuele regelingen inzake het gebruik van ICT-diensten ▌ ten minste het volgende ***bevatten***:

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

   b) de locaties***, namelijk de regio's of landen,*** waar de contractueel overeengekomen of uitbestede ***ICT-functies*** en ***-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 ***van tevoren*** in kennis te stellen indien hij voornemens is van locatie te veranderen;

   c) bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, beveiliging***, vertrouwelijkheid*** en bescherming van ***gegevens, met inbegrip van*** persoonsgegevens***;***

   c bis) bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens en 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, stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten ***of in geval***

van beëindiging van de contractuele regelingen;

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

e) ▌

f) de verplichting van de derde aanbieder van ICT-diensten om in geval van een ***aan de geleverde dienst gerelateerd*** ICT-incident zonder extra kosten of tegen een vooraf bepaalde kostprijs bijstand te verlenen;

g) 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*** veilige dienstverlening in overeenstemming met haar regelgevingskader;

h) ▌

i) de verplichting van de derde aanbieder van ICT-diensten om volledig samen te werken met de bevoegde autoriteiten en afwikkelingsautoriteiten van de financiële entiteit, met inbegrip van de door hen aangestelde personen;

j) het recht van beëindiging en de bijbehorende minimale opzegtermijn voor de beëindiging van het contract, in overeenstemming met de verwachtingen van de bevoegde autoriteiten ***en de afwikkelingsautoriteiten en, indien die contractuele regeling gevolgen heeft voor een aanbieder van ICT-diensten binnen dezelfde groep, een analyse volgens een risicogebaseerde benadering***;

k) 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 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 kan veranderen naar gebruik van eigen diensten in overeenstemming met de complexiteit van de geleverde dienst***;***

ii bis) wanneer die contractuele regeling gevolgen heeft voor een aanbieder van ICT-diensten binnen dezelfde groep, wordt zij volgens een risicogebaseerde benadering geanalyseerd;

k bis) een bepaling betreffende de verwerking van persoonsgegevens door de derde aanbieder van ICT-diensten die in overeenstemming is met Verordening

(EU) 2016/679.

2 bis. De contractuele regelingen voor het verrichten van cruciale of belangrijke functies omvatten, in aanvulling op lid 2, ten minste het volgende:

a) 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 van ICT-diensten om cruciale of belangrijke functies doeltreffend uit te voeren in overeenstemming met de afgesproken dienstverleningsniveaus;

b) het recht om de prestaties van de derde aanbieder van ICT-diensten permanent te monitoren, met inbegrip van:

i) het recht van toegang, inspectie en audit door de financiële entiteit of een daartoe aangestelde derde, en het recht om ter plaatse kopieën van relevante documenten in te zien 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 regelingen of ander uitvoeringsbeleid;

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

iii) de toezegging van de derde aanbieder van ICT-diensten om tijdens de door de bevoegde autoriteiten, de leidende toezichthouder, de financiële entiteit of een aangewezen derde ter plaatse uitgevoerde inspecties en audits volledig mee te werken, alsmede bijzonderheden over het toepassingsgebied, het verloop en de frequentie van dergelijke inspecties en audits.

In afwijking van punt b) kunnen de derde aanbieder van ICT-diensten en de financiële entiteit overeenkomen dat de rechten van toegang, inspectie en audit mogen worden gedelegeerd aan een onafhankelijke derde partij die wordt aangewezen 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.

2 ter. De contractuele regelingen voor de levering van ICT-diensten door een in een derde land gevestigde en krachtens artikel 28, lid 9, als cruciaal aangemerkte derde aanbieder van ICT-diensten moeten, in aanvulling op de leden 2 en 2 bis van dit artikel:

a) bepalen dat het contract onder het recht van een lidstaat valt; en

b) garanderen dat het orgaan voor gezamenlijk toezicht en de leidende toezichthouder hun in artikel 30 omschreven taken kunnen uitvoeren op basis van hun in artikel 31 omschreven bevoegdheden.

Het is niet vereist dat de diensten waarvoor de contractuele regelingen worden getroffen, worden verricht door de onderneming die in de Unie is opgericht overeenkomstig het recht van een lidstaat.

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

3 bis. De bevoegde autoriteiten krijgen inzage in de in dit artikel bedoelde contractuele regelingen. De partijen bij die contractuele regelingen kunnen overeenkomen om commercieel gevoelige of vertrouwelijke informatie onleesbaar te maken voordat zij de bevoegde autoriteiten inzage geven, mits deze autoriteiten volledig in kennis worden gesteld van de omvang en de aard van de weglatingen.

4. De ETA's stellen via het Gemengd Comité ontwerpen van technische reguleringsnormen op tot nadere bepaling van de elementen die een financiële entiteit bij uitbesteding van cruciale of belangrijke functies moet vaststellen en beoordelen met het oog op een behoorlijke uitvoering van de bepalingen van lid 2, punt a). ***Bij het opstellen van die ontwerpen van technische reguleringsnormen houden de ETA's rekening met de omvang van financiële entiteiten, de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen, en hun algemene risicoprofiel.***

De ETA's leggen die ontwerpen van technische reguleringsnormen uiterlijk op [OJ: insert date ***18 months*** after the date of entry into force] 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 respectievelijk de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1095/2010 en (EU) nr. 1094/2010.

AFDELING II

TOEZICHTKADER VOOR CRUCIALE DERDE AANBIEDERS VAN ICT-DIENSTEN

Artikel 28

Aanwijzing van cruciale derde aanbieders van ICT-diensten

1. ***Na raadpleging van Enisa zorgen*** de ETA's ▌ via het Gemengd Comité en op aanbeveling van het overeenkomstig artikel 29, lid 1, opgerichte ***toezichtorgaan*** voor het volgende:

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

   b) zij stellen de EBA, de ESMA of de Eiopa aan als leidende toezichthouder voor elke cruciale derde aanbieder van ICT-diensten, naargelang de totale waarde van de activa van financiële entiteiten die gebruikmaken van de diensten van de cruciale derde aanbieder van ICT-diensten en die onder respectievelijk Verordening (EU) nr. 1093/2010, (EU) nr. 1094/2010 of (EU) nr. 1095/2010 vallen, meer dan de helft vertegenwoordigt van de waarde van de totale activa van alle financiële entiteiten die gebruikmaken van de diensten van de cruciale derde aanbieder van ICT-diensten, zoals deze resulteert uit de geconsolideerde balansen, of uit de individuele balans wanneer de balansen niet geconsolideerd zijn, van deze financiële entiteiten.

   De overeenkomstig de eerste alinea, punt b), aangestelde leidende toezichthouder is verantwoordelijk voor het dagelijkse toezicht op de cruciale derde aanbieder van ICT-diensten.

2. De in lid 1, punt a), bedoelde aanwijzing is gebaseerd op alle volgende criteria:

   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 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 cruciale 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 mate van vervangbaarheid 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 om de relevante gegevens en werklast geheel of gedeeltelijk te migreren van de desbetreffende derde aanbieder van ICT-diensten naar een andere, hetzij ten gevolge van hoge financiële kosten, de tijd of andere soorten middelen die het migratieproces kan meebrengen, of de hogere ICT-risico's of andere operationele risico's waaraan de financiële entiteit kan worden blootgesteld door een dergelijke migratie;

e) het aantal lidstaten waarin de betrokken derde aanbieder ICT-diensten verleent;

f) het aantal lidstaten waarin financiële entiteiten die gebruik maken van de desbetreffende derde aanbieder van ICT-diensten, actief zijn.

f bis) de materialiteit en het belang van de door de betrokken derde aanbieder van ICT-diensten verleende diensten.

2 bis. Voordat de beoordeling met het oog op de in lid 1, punt a), bedoelde aanwijzing wordt aangevat, stelt het orgaan voor gezamenlijk toezicht de derde aanbieder van ICT-diensten hiervan in kennis.

Het orgaan voor gezamenlijk toezicht stelt de derde aanbieder van ICT-diensten in kennis van de uitkomst van de in de eerste alinea bedoelde beoordeling door een ontwerpaanbeveling inzake het cruciale karakter te verstrekken. Binnen zes weken na de datum van ontvangst van die ontwerpaanbeveling kan de derde aanbieder van ICT-diensten bij het orgaan voor gezamenlijk toezicht een met redenen omklede verklaring over de beoordeling indienen. Die met redenen omklede verklaring bevat alle relevante aanvullende informatie die de derde aanbieder van ICT-diensten passend acht om de volledigheid en nauwkeurigheid van de aanwijzingsprocedure te ondersteunen of om de ontwerpaanbeveling inzake het cruciale karakter aan te vechten. Het gemengd comité van de ETA's houdt terdege rekening met de met redenen omklede verklaring en kan de derde aanbieder van ICT-diensten om aanvullende informatie of bewijzen verzoeken alvorens een besluit over de aanwijzing te nemen.

Het gemengd comité van de ETA's stelt de derde aanbieder van ICT-diensten ervan in kennis dat hij als cruciaal is aangemerkt. De derde aanbieder van ICT-diensten krijgt, te rekenen vanaf de datum van ontvangst van de kennisgeving, ten minste

drie maanden de tijd om de nodige aanpassingen te doen opdat het orgaan voor gezamenlijk toezicht zijn taken uit hoofde van artikel 30 kan uitvoeren, en om de financiële entiteiten waaraan de derde aanbieder van ICT-diensten diensten verleent, in kennis te stellen. Op naar behoren gemotiveerd verzoek van de derde aanbieder van ICT-diensten kan het orgaan voor gezamenlijk toezicht de termijn voor aanpassingen met maximaal drie maanden verlengen.

3. De Commissie is bevoegd overeenkomstig artikel 50 ***een*** gedelegeerde ***handeling*** vast te stellen ***tot nadere bepaling*** van de in lid 2 bedoelde criteria.

4. Het in lid 1, punt a), bedoelde aanwijzingsmechanisme wordt niet gebruikt totdat de Commissie een gedelegeerde handeling overeenkomstig lid 3 heeft vastgesteld.

5. Het in lid 1, punt a), bedoelde aanwijzingsmechanisme is niet van toepassing op derde aanbieders van ICT-diensten die onderworpen zijn aan toezichtkaders die zijn vastgesteld ter ondersteuning van de in artikel 127, lid 2, van het Verdrag betreffende de werking van de Europese Unie bedoelde taken.

6. ***Het orgaan voor gezamenlijk toezicht stelt in overleg met Enisa*** een lijst op van aanbieders van cruciale derde aanbieders van ICT-diensten op het niveau van de Unie, ***publiceert*** deze en ***actualiseert*** deze ***regelmatig***.

7. Voor de toepassing van lid 1, punt a), zenden de bevoegde autoriteiten de in artikel 25, lid 4, bedoelde verslagen jaarlijks en op geaggregeerde basis toe aan het overeenkomstig artikel 29 opgerichte ***orgaan voor gezamenlijk toezicht***. Het ***orgaan voor gezamenlijk toezicht*** 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.

8. ***De*** derde aanbieders van ICT-diensten die niet in de lid 6 bedoelde lijst zijn opgenomen, kunnen verzoeken om opname in die lijst.

   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 in die lijst op te nemen in overeenstemming met 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.

8 bis. Het gemengd comité van de ETA's wijst, op aanbeveling van het orgaan voor gezamenlijk toezicht, de in een derde land gevestigde derde aanbieders van ICT-diensten aan die overeenkomstig lid 1, punt a), cruciaal zijn voor financiële entiteiten.

Bij de aanwijzing als bedoeld in de eerste alinea van dit lid volgen de ETA's en het orgaan voor gezamenlijk toezicht de in lid 2 bis beschreven procedurele stappen.

9. Financiële entiteiten maken geen gebruik van een in een derde land gevestigde ***cruciale*** derde aanbieder van ICT-diensten ***tenzij die derde aanbieder van ICT-diensten een in de Unie krachtens het recht van een lidstaat opgerichte dochteronderneming heeft en contractuele regelingen heeft getroffen overeenkomstig artikel 27, lid 2 ter***.

Artikel 29

Structuur van het toezichtkader

1. ***Het orgaan voor gezamenlijk toezicht wordt opgericht om toezicht te houden op het*** ICT-risico van derde aanbieder in alle financiële sectoren ***en om direct toezicht te houden op derde aanbieders van ICT-diensten die op grond van artikel 28 als cruciaal worden aangewezen***.

   De rol van het orgaan voor gezamenlijk toezicht is beperkt tot toezichtbevoegdheden met betrekking tot ICT-risico's in verband met de ICT-diensten die cruciale derde aanbieders van ICT-diensten verlenen aan financiële entiteiten.

   Het ***orgaan voor gezamenlijk toezicht*** bespreekt regelmatig relevante ontwikkelingen inzake ICT-risico's en -kwetsbaarheden en bevordert een consistente aanpak bij de monitoring van het ICT-risico van derde aanbieders op het niveau van de Unie.

2. Het ***orgaan voor gezamenlijk toezicht*** verricht jaarlijks een collectieve beoordeling van de resultaten en bevindingen van de toezichtactiviteiten voor alle cruciale derde aanbieders van ICT-diensten en bevordert coördinatiemaatregelen om de digitale operationele veerkracht 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.

   Het ***orgaan voor gezamenlijk toezicht*** dient alomvattende benchmarks voor cruciale 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.

3. Het ***orgaan voor gezamenlijk toezicht i***s samengesteld uit de ***uitvoerend directeuren*** van de ETA's, één vertegenwoordiger op hoog niveau van het huidige personeel van de ***ETA's en één vertegenwoordiger op hoog niveau van ten minste acht van de nationale bevoegde autoriteiten***. Eén vertegenwoordiger van de Europese Commissie, het ESRB, de ECB en Enisa ***en ten minste één overeenkomstig lid 3 bis van dit artikel aangestelde onafhankelijke deskundige*** nemen ▌ deel als waarnemer.

   Na de jaarlijkse aanwijzing van cruciale derde aanbieders van ICT-diensten overeenkomstig artikel 28, lid 1, punt a), besluit het gemengd comité van de ETA's welke nationale bevoegde autoriteiten lid worden van het orgaan voor gezamenlijk toezicht, rekening houdend met de volgende factoren:

   a) het aantal cruciale derde aanbieders van ICT-diensten dat in een lidstaat is gevestigd of er diensten verleent;

   b) de afhankelijkheid van de financiële entiteiten in een lidstaat van cruciale derde aanbieders van ICT-diensten;

   c) de relatieve deskundigheid van een nationale bevoegde autoriteit;

   d) de beschikbare middelen en capaciteit van een nationale bevoegde autoriteit;

   e) de noodzaak van een gestroomlijnde, slanke en efficiënte werking en

besluitvorming van het orgaan voor gezamenlijk toezicht.

Het orgaan voor gezamenlijk toezicht deelt zijn documentatie en besluiten met alle nationale bevoegde autoriteiten die geen lid zijn van het orgaan voor gezamenlijk toezicht.

Het orgaan voor gezamenlijk toezicht wordt bij zijn werkzaamheden ondersteund en bijgestaan door speciaal personeel van de verschillende ETA's.

3 bis. De in lid 3 van dit artikel bedoelde onafhankelijke deskundige wordt na een openbare en transparante sollicitatieprocedure aangesteld als waarnemer.

De onafhankelijke deskundige wordt voor een termijn van twee jaar aangesteld op basis van zijn deskundigheid op het gebied van financiële stabiliteit, digitale operationele veerkracht en ICT-beveiliging.

De aangestelde onafhankelijke deskundige bekleedt geen functie op nationaal, Unie- of internationaal niveau. De onafhankelijke deskundige handelt onafhankelijk, objectief en uitsluitend in het belang van de Unie als geheel, en vraagt noch aanvaardt instructies van instellingen of organen van de Unie, van de regering van een lidstaat of van andere publieke of particuliere organen.

Het orgaan voor gezamenlijk toezicht kan besluiten meer dan één onafhankelijke deskundige als waarnemer aan te stellen.

4. Overeenkomstig artikel 16 van 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 [OJ: insert date 18 months after the date of entry into force of this Regulation]*** richtsnoeren uit over de samenwerking tussen de ETA's en de bevoegde autoriteiten inzake de nadere procedures en voorwaarden voor de uitvoering van taken door de bevoegde autoriteiten en ***het orgaan voor gezamenlijk toezicht*** en nadere details over de uitwisseling van informatie die de bevoegde autoriteiten nodig hebben ten behoeve van de follow-up van aanbevelingen van ***het orgaan voor gezamenlijk toezicht*** aan cruciale derde aanbieders van ICT-diensten in overeenstemming met artikel 31, lid 1, punt d).

5. De in deze afdeling gestelde vereisten doen geen afbreuk aan de toepassing van Richtlijn (EU) 2016/1148 en van andere Unieregels inzake toezicht die van toepassing zijn op aanbieders van cloudcomputingdiensten.

6. ▌Het ***orgaan voor gezamenlijk toezicht dient*** bij het Europees Parlement, de Raad en de Commissie jaarlijks een verslag in over de toepassing van deze afdeling.

Artikel 30

Taken van de leidende toezichthouder

1. De ***overeenkomstig artikel 28, lid 1, punt b), aangewezen*** leidende toezichthouder ***leidt en coördineert het dagelijkse toezicht op cruciale derde aanbieders van ICT-diensten van derden en is het eerste contactpunt voor die derde aanbieders van ICT-diensten***.

1 bis. De ***leidende toezichthouder*** beoordeelt of elke cruciale derde aanbieder van ICT-diensten over uitgebreide, deugdelijke en doeltreffende regels, procedures,

mechanismen en regelingen beschikt voor het beheer van de ICT-risico's die hij voor financiële entiteiten kan inhouden. ***Die beoordeling heeft in de eerste plaats betrekking op de door de cruciale derde aanbieder van ICT-diensten aan financiële entiteiten verleende ICT-diensten die cruciale of belangrijke functies ondersteunen, maar kan ook ruimer zijn indien dat relevant is voor de beoordeling van de risico's voor die functies.***

2. De in lid ***1 bis*** bedoelde beoordeling heeft betrekking op:

   a) ICT-voorschriften om met name de veiligheid, beschikbaarheid, continuïteit, schaalbaarheid en kwaliteit van diensten die de cruciale derde aanbieder van ICT-diensten aan financiële entiteiten verleent, te garanderen alsmede het vermogen om te allen tijde hoge normen inzake beveiliging, vertrouwelijkheid en integriteit 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, de ICT-bedrijfscontinuïteit en de ICT-noodherstelplannen;

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

   e) de opsporing, monitoring en snelle rapportage van ***ernstige*** ICT-gerelateerde incidenten aan de 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.

3. Op basis van de in lid ***1 bis*** bedoelde beoordeling ***door de leidende toezichthouder wordt door het orgaan voor gezamenlijk toezicht, onder coördinatie en leiding van*** de leidende toezichthouder***,*** een duidelijk, gedetailleerd en met redenen omkleed ***ontwerp van*** individueel toezichtplan voor elke cruciale derde aanbieder van ICT-diensten ***opgesteld en voorgelegd***.

   Bij het voorbereiden van het ontwerptoezichtplan raadpleegt het orgaan voor gezamenlijk toezicht alle betrokken in artikel 8 van Richtlijn (EU) 2016/1148 bedoelde bevoegde autoriteiten en centrale contactpunten om ervoor te zorgen dat er geen inconsistenties of overlappingen zijn met de verplichtingen van de cruciale derde aanbieder van ICT-diensten uit hoofde van die richtlijn.

   Het toezichtplan wordt jaarlijks vastgesteld door de raad van bestuur van de leidende toezichthouder.

Voordat het wordt vastgesteld, wordt het ontwerptoezichtplan aan de cruciale derde aanbieder van ICT-diensten meegedeeld.

Na ontvangst van het ontwerptoezichtplan beschikt de cruciale derde aanbieder van ICT-diensten over een termijn van zes weken om het ontwerptoezichtplan te beoordelen en een met redenen omklede verklaring in te dienen. Een dergelijke met redenen omklede verklaring mag alleen worden ingediend indien de cruciale derde aanbieder van ICT-diensten kan aantonen dat de uitvoering van het toezichtplan onevenredige gevolgen zou hebben of verstoring zou veroorzaken voor cliënten die niet onder deze verordening vallen, of dat er een effectievere of efficiëntere oplossing is om de vastgestelde ICT-risico's te beheren. Indien een dergelijke verklaring wordt ingediend, stelt de cruciale derde aanbieder van ICT-diensten het orgaan voor gezamenlijk toezicht een effectievere of efficiëntere oplossing voor om de doelstellingen van het ontwerptoezichtplan te verwezenlijken.

Alvorens het toezichtplan vast te stellen, houdt de raad van bestuur van de leidende toezichthouder terdege rekening met de met redenen omklede verklaring en kan hij de derde aanbieder van ICT-diensten om aanvullende informatie of bewijzen vragen.

4. Zodra de in lid 3 bedoelde jaarlijkse toezichtplannen zijn ***vastgesteld*** en aan de cruciale derde aanbieder van ICT-diensten zijn meegedeeld, kunnen de bevoegde autoriteiten maatregelen met betrekking tot cruciale derde aanbieders van ICT-diensten alleen nemen in overeenstemming met ***het orgaan voor gezamenlijk toezicht***.

Artikel 31

Toezichtsbevoegdheden

1. Voor de uitvoering van de in deze afdeling omschreven taken beschikt de leidende toezichthouder ***ten aanzien van de door de cruciale derde aanbieder van ICT-diensten aan financiële entiteiten verleende diensten*** over de bevoegdheid om:

   a) alle relevante informatie en documentatie overeenkomstig artikel 32 op te vragen;

   b) algemene onderzoeken en inspecties ***ter plaatse*** te verrichten overeenkomstig de artikelen 33 en 34;

   c) na afloop van de toezichtactiviteiten te verzoeken om verslagen, met vermelding van de ondernomen acties of de corrigerende maatregelen die door de cruciale derde aanbieders van ICT-diensten zijn genomen met betrekking tot de in ***lid 1 bis*** bedoelde aanbevelingen;

1 bis. Voor de uitvoering van de in deze afdeling omschreven taken en op basis van de door de leidende toezichthouder verkregen informatie en de resultaten van de door de leidende toezichthouder verrichte onderzoeken beschikt het orgaan voor gezamenlijk toezicht over de bevoegdheid om aanbevelingen te doen met betrekking tot de in artikel 30, lid 2, 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 ***het orgaan voor gezamenlijk toezicht*** relevant acht om de ICT-beveiliging van diensten voor financiële entiteiten te waarborgen;

ii) het hanteren van voorwaarden, met inbegrip van de technische uitvoering ervan, voor het verlenen van diensten aan financiële entiteiten door cruciale derde aanbieders van ICT-diensten, die ***het orgaan voor gezamenlijk toezicht*** relevant acht om het ontstaan van zwakke punten ("single points of failure") of 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) na onderzoek overeenkomstig de artikelen 32 en 33 van uitbestedingsregelingen, inclusief verdere onderaanbestedingsregelingen die de cruciale derde aanbieders van ICT-diensten voornemens zijn te sluiten met andere derde aanbieders van ICT-diensten of met in een derde land gevestigde subcontractanten, elke voorgenomen uitbesteding, waaronder verdere onderaanbestedingen, wanneer ***het orgaan voor gezamenlijk toezicht*** van oordeel is dat verdere onderaanbesteding risico's voor de levering van diensten door de financiële entiteit of risico's voor de financiële stabiliteit kan meebrengen;

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

– de beoogde subcontractant is een in een derde land gevestigde derde aanbieder van ICT-diensten of ICT-subcontractant ***en heeft geen onderneming die in de Unie is opgericht overeenkomstig het recht van een lidstaat***;

– de onderaanbesteding heeft betrekking op een cruciale of belangrijke functie van de financiële entiteit***;***

– ***de uitbesteding leidt tot ernstige en duidelijke risico's voor de financiële entiteit of voor de financiële stabiliteit van het financiële stelsel van de Unie.***

1 ter. De in de leden 1 en 1 bis bedoelde bevoegdheden worden, waar nodig, uitgeoefend met betrekking tot de ICT-diensten ter ondersteuning van niet-kritieke of niet-belangrijke functies, die door de cruciale derde aanbieder van ICT-diensten worden geleverd.

1 quater. Bij het uitoefenen van de in de leden 1 en 1 bis van dit artikel bedoelde bevoegdheid houden de leidende toezichthouder en het orgaan voor gezamenlijk toezicht naar behoren rekening met het bij Richtlijn (EU) 2016/1148 vastgestelde kader en raadplegen zij waar nodig de relevante bevoegde autoriteiten als ingesteld bij die richtlijn, ter voorkoming van onnodige duplicatie van technische en organisatorische maatregelen die mogelijk uit hoofde van die richtlijn op cruciale derde aanbieders van ICT-diensten van toepassing zijn.

2. ***Alvorens overeenkomstig lid 1 bis aanbevelingen af te ronden en uit te brengen, stelt het orgaan voor gezamenlijk toezicht de cruciale derde aanbieder van ICT-diensten in kennis van zijn voornemen en biedt het deze de gelegenheid informatie te verstrekken waarvan hij redelijkerwijs vindt dat daarmee rekening moet worden gehouden voordat de aanbeveling wordt afgerond of teneinde bezwaar te maken tegen de beoogde aanbevelingen. Gronden om bezwaar te maken tegen een aanbeveling zijn onder meer dat deze onevenredige gevolgen zou hebben voor klanten op wie deze verordening niet van toepassing is of de diensten die aan deze klanten worden geleverd zou verstoren, of dat er een doelmatiger of doeltreffender oplossing is om het geïdentificeerde risico te beheren.***

3. Cruciale derde aanbieders van ICT-diensten werken te goeder trouw samen met de leidende toezichthouder ***en het orgaan voor gezamenlijk toezicht*** en ondersteunen ***deze*** bij de uitvoering van ***hun*** taken.

4. De leidende toezichthouder kan***, in geval van gehele of gedeeltelijke niet-naleving van de overeenkomstig lid 1, punten a), b) of c), te nemen maatregelen en na het verstrijken van een termijn van ten minste 60 kalenderdagen vanaf de datum waarop de cruciale derde aanbieder van ICT-diensten een kennisgeving van de maatregel heeft ontvangen, besluiten*** een dwangsom ***op te leggen*** om de cruciale derde aanbieder van ICT-diensten ***tot nakoming te dwingen***.

4 bis. ***De in lid 4 bedoelde dwangsom wordt door de leidende toezichthouder slechts in laatste instantie opgelegd en uitsluitend in gevallen waarin de cruciale derde aanbieder van ICT-diensten niet heeft voldaan aan de overeenkomstig lid 1, punten a), b) of c), te nemen maatregelen.***

5. De in lid 4 bedoelde dwangsom wordt dagelijks opgelegd tot aan de verplichtingen is voldaan, gedurende een termijn van ten hoogste zes maanden volgend op de kennisgeving aan de cruciale derde aanbieder van ICT-diensten.

6. Het bedrag van de dwangsom, berekend vanaf de datum die is vastgesteld in het besluit tot oplegging van de dwangsom, bedraagt ***ten hoogste*** 1 % van de gemiddelde wereldwijde dagomzet ***in verband met diensten die*** de cruciale derde aanbieder van ICT-diensten in het voorafgaande boekjaar ***heeft verleend aan onder deze verordening onderworpen financiële entiteiten***.

7. Dwangsommen hebben een administratief karakter en zijn afdwingbaar. De tenuitvoerlegging geschiedt volgens de bepalingen van burgerlijke rechtsvordering 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.

8. De ETA's maken alle opgelegde dwangsommen openbaar, tenzij die openbaarmaking de financiële markten ernstig in gevaar zou brengen of onevenredige schade zou toebrengen aan de betrokken partijen.

9. Alvorens een dwangsom op grond van lid 4 op te leggen, stelt de leidende toezichthouder de vertegenwoordigers van de cruciale 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 cruciale 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. Zij zijn gerechtigd toegang tot het dossier te krijgen, 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 interne voorbereidende documenten van de leidende toezichthouder.

Artikel 32

Verzoek om informatie

1. De leidende toezichthouder kan cruciale 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 cruciale derde aanbieder van ICT-diensten operationele functies of activiteiten heeft uitbesteed.

   Van cruciale derde aanbieders van ICT-diensten kan alleen worden verlangd dat zij de in de eerste alinea bedoelde informatie verstrekken met betrekking tot de diensten die worden verleend aan financiële entiteiten die aan deze verordening onderworpen zijn en die voor cruciale of belangrijke functies gebruikmaken van de diensten van cruciale derde aanbieders van ICT-diensten. Cruciale derde aanbieders van ICT-diensten stellen bij een verzoek om informatie met betrekking tot een specifieke financiële entiteit de betrokken financiële entiteit van dit verzoek in kennis.

2. Bij het toezenden van een verzoek om informatie krachtens lid 1 neemt de leidende toezichthouder 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 cruciale derde aanbieder van ICT-diensten mee dat deze niet verplicht is de informatie te verstrekken maar dat, als vrijwillig op het verzoek wordt ingegaan, de verstrekte informatie niet onjuist en misleidend mag zijn.

3. Wanneer de leidende toezichthouder 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 ***redelijke*** termijn de informatie moet worden verstrekt;

e) hij vermeldt welke dwangsom overeenkomstig artikel 31, lid 4, wordt opgelegd indien de gevraagde informatie niet volledig wordt overgelegd ***of wanneer deze informatie niet binnen de in punt d) 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 respectievelijk Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 of (EU) nr. 1095/2010.

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

5. De leidende toezichthouder zendt onverwijld een afschrift van het besluit inzake informatieverstrekking aan de bevoegde autoriteiten van de financiële entiteiten die gebruikmaken van de ICT-diensten van cruciale derde aanbieders.

Artikel 33

Algemene onderzoeken

1. Voor de uitvoering van zijn taken uit hoofde van deze verordening kan de leidende toezichthouder, ondersteund door het in artikel 35, lid 1, bedoelde onderzoeksteam, bij derde aanbieders van ICT-diensten de nodige onderzoeken verrichten***, daarbij rekening houdend met het evenredigheidsbeginsel***. ***Bij het verrichten van onderzoeken betracht de leidende toezichthouder de nodige voorzichtigheid en zorgt hij ervoor dat de rechten van de klanten van cruciale derde aanbieders van ICT-diensten op wie deze verordening niet van toepassing is, worden beschermd, onder meer wat betreft de gevolgen voor het niveau van de dienstverlening, beschikbaarheid van gegevens en vertrouwelijkheid.***

2. De leidende toezichthouder is bevoegd om:

a) registers, gegevens, procedures of alle ander voor de uitvoering van zijn taken relevant materiaal, te onderzoeken, ongeacht de drager waarop deze zijn opgeslagen;

b) ***op beveiligde wijze*** voor echt gewaarmerkte kopieën of uittreksels van deze registers, gegevens, procedures en ander materiaal ***in te zien***;

c) vertegenwoordigers van derde aanbieders van ICT-diensten op te roepen en te verzoeken om mondelinge of schriftelijke toelichting bij feiten of documenten met betrekking tot het onderwerp en het doel van het onderzoek, en de antwoorden op te tekenen;

d) alle andere natuurlijke personen of rechtspersonen te horen die daarin toestemmen, om informatie betreffende het onderwerp van een onderzoek te verzamelen;

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

3. De functionarissen van de leidende toezichthouder en andere door hem ten behoeve 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 die machtiging worden eveneens de in artikel 31, lid 4, bedoelde dwangsommen vermeld wanneer de vereiste registers, gegevens, procedures of enig ander materiaal of de antwoorden op vragen aan vertegenwoordigers van derde aanbieders van ICT-diensten niet of onvolledig worden verstrekt.

4. De vertegenwoordigers van de derde aanbieders van ICT-diensten zijn verplicht zich aan het onderzoek te onderwerpen op basis van een besluit van de leidende toezichthouder. Het besluit vermeldt het onderwerp en het doel van het onderzoek, de dwangsommen die overeenkomstig artikel 31, lid 4, 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 tegen het besluit in beroep te gaan.

5. De leidende toezichthouders stellen de bevoegde organen van de financiële entiteiten die gebruikmaken van de betrokken derde aanbieder van ICT-diensten, geruime tijd vooraf in kennis van het onderzoek en van de identiteit van de gemachtigde personen.

Artikel 34

Inspecties ter plaatse

1. Voor de uitvoering van zijn taken uit hoofde van deze verordening kan de leidende toezichthouder, ondersteund door de in artikel 35, lid 1, bedoelde onderzoeksteams, alle nodige inspecties ter plaatse verrichten in alle bedrijfsruimten, terreinen of eigendommen van de derde aanbieders van ICT-diensten, zoals hoofdkantoren, operationele centra en secundaire locaties, alsmede off-site-inspecties verrichten.

De in de eerste alinea bedoelde bevoegdheid om inspecties ter plaatse te verrichten omvat niet uitsluitend locaties in de Unie maar ook locaties in derde landen, mits daarbij aan elk van de volgende voorwaarden is voldaan:

- ***de inspectie is noodzakelijk om de leidende toezichthouder in staat te stellen zijn taken uit hoofde van deze verordening te vervullen;***
- ***de inspectie houdt rechtstreeks verband met de levering van ICT-diensten aan financiële entiteiten van de Unie;***
- ***de inspectie is van belang met het oog op een lopend onderzoek.***

1 bis. Bij het verrichten van inspecties ter plaatse betrachten de leidende toezichthouder en het onderzoeksteam de nodige voorzichtigheid en zorgen zij ervoor dat de rechten van de klanten van cruciale derde aanbieders van ICT-diensten op wie deze verordening niet van toepassing is, worden beschermd, onder meer wat betreft de

gevolgen voor het niveau van de dienstverlening, beschikbaarheid van gegevens en vertrouwelijkheid.

2. De ambtenaren en andere personen die door de leidende toezichthouder gemachtigd zijn tot het verrichten van inspecties ter plaatse, kunnen deze bedrijfsruimten, terreinen of eigendommen betreden en beschikken over alle bevoegdheden om bedrijfsruimten, boeken en registers te verzegelen voor de duur van en voor zover nodig is voor het onderzoek.

   Zij oefenen hun 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 31, lid 4, wanneer de vertegenwoordigers van de betrokken derde aanbieders van ICT-diensten zich niet aan de inspectie onderwerpen.

3. De leidende toezichthouders stellen de bevoegde autoriteiten van de financiële entiteiten die gebruikmaken van de betrokken derde aanbieder van ICT-diensten, geruime tijd voor de inspectie daarvan in kennis.

4. De inspecties hebben betrekking op het hele gamma van relevante ICT-systemen, -netwerken, -apparatuur, -informatie en -gegevens ***die de leidende toezichthouder gepast en technologisch relevant acht en*** die worden gebruikt voor of bijdragen tot de verlening van diensten aan financiële entiteiten.

5. Vóór een geplande inspectie ter plaatse verleent de leidende toezichthouder de cruciale derde aanbieder van ICT-diensten een redelijke kennisgevingstermijn, tenzij dit niet mogelijk is vanwege een nood- of crisissituatie of zou leiden tot een situatie waarin de inspectie of audit niet langer doeltreffend zou zijn.

6. De cruciale derde aanbieder van ICT-diensten onderwerpt zich aan de inspecties ter plaatse die bij besluit van de leidende toezichthouder zijn gelast. Het besluit vermeldt het onderwerp en het doel van de inspectie, de datum waarop de inspectie zal aanvangen, de dwangsommen bedoeld in artikel 31, lid 4, 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. Wanneer de ambtenaren en andere personen die door de leidende toezichthouder daartoe gemachtigd zijn, vaststellen dat een cruciale derde aanbieder van ICT-diensten zich verzet tegen een krachtens dit artikel gelaste inspectie, stelt de leidende toezichthouder de cruciale derde aanbieder van ICT-diensten in kennis van de gevolgen van dit verzet, met inbegrip van de mogelijkheid voor de bevoegde autoriteiten van de desbetreffende financiële entiteiten om de contractuele regelingen met die cruciale derde aanbieder van ICT-diensten te beëindigen.

Artikel 35

Doorlopend toezicht

1. Bij het uitvoeren van algemene onderzoeken of inspecties ter plaatse wordt de leidende toezichthouder bijgestaan door een gezamenlijk onderzoeksteam dat voor elke cruciale derde aanbieder van ICT-diensten wordt opgericht.

2. Het in lid 1 bedoelde gezamenlijke onderzoeksteam is samengesteld uit

personeelsleden van de leidende toezichthouder***, van de andere ETA's*** en van de desbetreffende autoriteiten die bevoegd zijn voor het toezicht op de financiële entiteiten waaraan de cruciale derde aanbieder ICT-diensten verleent, die deelnemen aan de voorbereiding en uitvoering van de toezichtactiviteiten, met ten hoogste tien leden. Alle leden van het gezamenlijke onderzoeksteam beschikken over deskundigheid in ICT- en operationeel risico. Het gezamenlijke onderzoeksteam werkt onder de coördinatie van een aangewezen personeelslid van de ETA ("coördinator van de leidende toezichthouder").

3. De ETA's ontwikkelen via het Gemengd Comité gemeenschappelijke ontwerpen van technische reguleringsnormen tot nadere omschrijving van de aanwijzing van de leden van het gezamenlijke onderzoeksteam die van de desbetreffende bevoegde autoriteiten afkomstig zijn, alsmede van de taken en werkregelingen van het onderzoeksteam. De ETA's leggen die ontwerpen van technische reguleringsnormen uiterlijk op [OJ: insert date 1 year after the date of entry into force] voor aan de Commissie.

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

4. Binnen drie maanden na de voltooiing van een onderzoek of een inspectie ter plaatse stelt ***het orgaan voor gezamenlijk toezicht*** aanbevelingen vast die overeenkomstig de in artikel 31 bedoelde bevoegdheden aan de cruciale derde aanbieder van ICT-diensten moeten worden gericht.

5. De in lid 4 bedoelde aanbevelingen worden onmiddellijk meegedeeld aan de cruciale derde aanbieder van ICT-diensten en aan de bevoegde autoriteiten van de financiële entiteiten waaraan hij diensten verleent.

   Voor de uitvoering van de toezichtactiviteiten kunnen leidende toezichthouders ***en het orgaan voor gezamenlijk toezicht*** rekening houden met relevante certificeringen van derden en interne of externe auditverslagen die door de cruciale derde aanbieder van ICT-diensten beschikbaar zijn gesteld.

Artikel 36

Harmonisatie van de voorwaarden voor de uitoefening van het toezicht

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

   a) de door de cruciale derde aanbieder van ICT-diensten te verstrekken informatie bij het verzoek om een vrijwillige opt-in als bedoeld in artikel 28, lid 8;

   b) de inhoud en het formaat van de verslagen die voor de toepassing van artikel 31, lid 1, punt c), kunnen worden gevraagd;

   c) de presentatie van de informatie, met inbegrip van de structuur, formaten en methoden, die een cruciale derde aanbieder van ICT-diensten overeenkomstig artikel 31, lid 1, moet indienen, bekendmaken of rapporteren;

d) de nadere gegevens over de beoordeling die de bevoegde autoriteiten overeenkomstig artikel 37, lid 2, verrichten van de door cruciale derde aanbieders van ICT-diensten op basis van de aanbevelingen van ***het orgaan voor gezamenlijk toezicht*** genomen maatregelen.

2. De ETA's leggen die gemeenschappelijke ontwerpen van technische reguleringsnormen uiterlijk op 1 januari 20xx [OJ: insert date 1 year after the date of entry into force] voor aan de Commissie.

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

Artikel 37

Follow-up door de bevoegde autoriteiten

1. Binnen 30 kalenderdagen na ontvangst van de aanbevelingen van ***het orgaan voor gezamenlijk toezicht*** overeenkomstig artikel 31, ***lid 1 bis***, delen cruciale derde aanbieders van ICT-diensten ***het orgaan voor gezamenlijk toezicht*** mee of zij voornemens zijn die aanbevelingen te volgen. ***Het orgaan voor gezamenlijk toezicht*** deelt deze informatie onmiddellijk mee aan de bevoegde autoriteiten ***van de betrokken financiële entiteiten***.

2. De bevoegde autoriteiten ***stellen financiële entiteiten die contractuele regelingen hebben gesloten met cruciale derde aanbieders van ICT-diensten in kennis van de risico's die zijn vastgesteld in de aanbevelingen van het orgaan voor gezamenlijk toezicht aan die cruciale derde aanbieders van ICT-diensten overeenkomstig artikel 31, lid 1 bis,*** en monitoren of de financiële entiteiten rekening houden met de vastgestelde risico's. ***Het orgaan voor gezamenlijk toezicht bewaakt of de cruciale derde aanbieders van ICT-diensten de in die aanbevelingen vastgestelde risico's hebben aangepakt.***

3. ***Wanneer de regelgevingsdoelstellingen niet door andere maatregelen kunnen worden verwezenlijkt en de getroffen financiële entiteiten door de bevoegde nationale autoriteiten zijn gewaarschuwd op basis van door het orgaan voor gezamenlijk toezicht verstrekte informatie, kan de raad van bestuur van de leidende toezichthouder op aanbeveling van het orgaan voor gezamenlijk toezicht en na overleg met*** de bevoegde autoriteiten ***van de getroffen*** financiële entiteiten ***besluiten het gebruik of de uitrol van een dienst die geleverd wordt aan financiële entiteiten die worden blootgesteld aan de risico's die in*** de aanbevelingen aan de cruciale derde aanbieder van ICT-diensten zijn vastgesteld***, tijdelijk geheel of gedeeltelijk op te schorten totdat deze risico's zijn verholpen***. Wanneer nodig***, en slechts in laatste instantie,*** kunnen zij ***de cruciale derde aanbieders van ICT-diensten*** ertoe verplichten de desbetreffende contractuele regelingen met de ***financiële entiteiten die blootgesteld worden aan de vastgestelde risico's*** geheel of gedeeltelijk te beëindigen.

4. Bij het vaststellen van de in lid 3 bedoelde besluiten ***houdt de raad van bestuur van de leidende toezichthouder rekening*** met het soort en de omvang van het risico dat de

cruciale derde aanbieder van ICT-diensten niet heeft verholpen, alsook met de ernst van de niet-naleving, 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 cruciale derde aanbieder van ICT-diensten;

c) de vraag of financiële delicten door de niet-naleving zijn vergemakkelijkt of veroorzaakt of op andere wijze daaraan kunnen worden toegeschreven;

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

d bis) de vraag of de opschorting of beëindiging een risico vormt voor de bedrijfscontinuïteit van de gebruiker van de diensten van de cruciale derde aanbieder van ICT-diensten.

4 bis. De in lid 3 bedoelde besluiten worden pas uitgevoerd wanneer alle getroffen financiële entiteiten naar behoren zijn geïnformeerd. De getroffen financiële entiteiten wordt enige tijd geboden, doch niet meer tijd dan strikt noodzakelijk is, om hun uitbestedings- en contractuele regelingen met cruciale derde aanbieders van ICT-diensten aldus aan te passen dat de digitale operationele veerkracht niet in gevaar komt, en om uitvoering te geven aan hun exitstrategieën en overgangsplannen als bedoeld in artikel 25.

De cruciale derde aanbieders van ICT-diensten op wie de in lid 3 bedoelde besluiten betrekking hebben, verlenen volledige medewerking aan de getroffen financiële entiteiten.

5. De bevoegde autoriteiten informeren ***het orgaan voor gezamenlijk toezicht*** regelmatig over de aanpak en de maatregelen die zij in het kader van hun toezichttaken ten aanzien van financiële entiteiten hebben gehanteerd.

Artikel 38

Toezichtvergoedingen

1. De ETA's brengen cruciale derde aanbieders van ICT-diensten vergoedingen in rekening die de noodzakelijke uitgaven van de ETA's met betrekking tot de uitvoering van toezichttaken uit hoofde van deze verordening volledig dekken, met inbegrip van de vergoeding voor eventuele kosten ten gevolge van activiteiten van bevoegde autoriteiten die overeenkomstig artikel 35 aan de toezichtactiviteiten deelnemen.

Het bedrag van een vergoeding die de cruciale derde aanbieder van ICT-diensten in rekening wordt gebracht, dekt alle ***kosten die voortvloeien uit de uitvoering van de in deze afdeling voorziene taken*** en staat in verhouding tot zijn omzet.

1 bis. Indien een administratieve regeling wordt getroffen met een regelgevende en toezichthoudende autoriteit van een derde land overeenkomstig lid 1 van dit artikel, kan die autoriteit deel uitmaken van het in artikel 35, lid 1, bedoelde onderzoeksteam.

2. De Commissie is bevoegd om overeenkomstig artikel 50 een gedelegeerde handeling

in aanvulling op deze verordening aan te nemen om het bedrag van de vergoedingen en de wijze van betaling daarvan vast te stellen.

Artikel 39

Internationale samenwerking

1. De EBA, de ESMA en de Eiopa kunnen overeenkomstig artikel 33 van respectievelijk Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 administratieve regelingen sluiten met regelgevende en toezichthoudende autoriteiten van derde landen om de internationale samenwerking op het gebied van het ICT-risico van derde aanbieders te bevorderen in verschillende financiële sectoren, met name door de ontwikkeling van beste praktijken voor de evaluatie van ICT-risicobeheerpraktijken en -controles, risicobeperkende maatregelen en respons op incidenten.

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

HOOFDSTUK VI

REGELINGEN VOOR INFORMATIE-UITWISSELING

Artikel 40

Regelingen voor uitwisseling van informatie en inlichtingen over cyberdreiging

1. Financiële entiteiten ***streven ernaar*** onderling ***en met cruciale derde aanbieders van ICT-diensten*** informatie en inlichtingen over cyberdreiging ***uit te wisselen***, met inbegrip van indicators of compromise, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten, voor zover deze uitwisseling van informatie en inlichtingen:

   a) tot doel heeft de digitale operationele veerkracht van financiële entiteiten ***en derde aanbieders van ICT-diensten*** te versterken, met name via bewustmaking met betrekking tot cyberdreigingen, beperking of belemmering van de mogelijkheid tot verdere verspreiding van cyberdreigingen, ondersteuning van defensieve capaciteiten, dreigingsdetectietechnieken, risicobeperkende strategieën of respons- en herstelfasen;

   b) plaatsvindt binnen vertrouwensgemeenschappen van financiële entiteiten ***en derde aanbieders van ICT-diensten***;

   c) ten uitvoer wordt gelegd via regelingen voor informatie-uitwisseling die de potentieel gevoelige aard van de gedeelde informatie beschermen en aan gedragsregels zijn onderworpen met volledige inachtneming van de vertrouwelijkheid van bedrijfsinformatie, de bescherming van persoonsgegevens[26] en de richtsnoeren inzake mededingingsbeleid[27].

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 vastgesteld inzake de betrokkenheid van overheidsinstanties en de hoedanigheid waarin deze instanties bij de regelingen voor informatie-uitwisseling kunnen worden betrokken, alsmede inzake operationele elementen, met inbegrip van het gebruik van specifieke IT-platforms.

3. Financiële entiteiten stellen de bevoegde autoriteiten in kennis van hun deelname aan de in lid 1 bedoelde regelingen voor informatie-uitwisseling, na validering van hun lidmaatschap of, in voorkomend geval, van de beëindiging van hun lidmaatschap, zodra deze beëindiging van kracht wordt.

---

[26] In overeenstemming met 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).

[27] Mededeling van de Commissie "Richtsnoeren inzake de toepasselijkheid van artikel 101 van het Verdrag betreffende de werking van de Europese Unie op horizontale samenwerkingsovereenkomsten" (PB C 11 van 14.1.11, blz. 1).

HOOFDSTUK VII

BEVOEGDE AUTORITEITEN

Artikel 41

Bevoegde autoriteiten

Onverminderd de bepalingen inzake het toezichtkader voor cruciale derde aanbieders van ICT-diensten als bedoeld in afdeling II van hoofdstuk V van deze verordening wordt de naleving van de in deze verordening vastgestelde verplichtingen in overeenstemming met de bij de respectieve rechtshandelingen verleende bevoegdheden gewaarborgd door de volgende bevoegde autoriteiten:

a) voor kredietinstellingen, de bevoegde autoriteit aangewezen overeenkomstig artikel 4 van Richtlijn 2013/36/EU, onverminderd de specifieke taken die bij Verordening (EU) nr. 1024/2013 aan de ECB zijn opgedragen;

b) voor betalingsdienstaanbieders, de bevoegde autoriteit aangewezen overeenkomstig artikel 22 van Richtlijn (EU) nr. 2015/2366;

c) voor instellingen voor elektronisch geld, de bevoegde autoriteit aangewezen overeenkomstig artikel 37 van Richtlijn 2009/110/EG;

d) voor beleggingsondernemingen, de bevoegde autoriteit aangewezen overeenkomstig artikel 4 van Richtlijn (EU) nr. 2019/2034;

e) voor aanbieders van cryptoactivadiensten, emittenten ***en aanbieders*** van cryptoactiva, emittenten ***en aanbieders*** van asset-referenced tokens en emittenten van significante asset-referenced tokens, de bevoegde autoriteit aangewezen overeenkomstig artikel 3, lid 1, punt ee), eerste streepje, van [Regulation (EU) 20xx MiCA Regulation];

f) voor centrale effectenbewaarinstellingen ***en exploitanten van effectenafwikkelingssystemen***, de bevoegde autoriteit aangewezen overeenkomstig artikel 11 van Verordening (EU) nr. 909/2014;

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

h) voor handelsplatformen en aanbieders van datarapporteringsdiensten, de bevoegde autoriteit aangewezen overeenkomstig artikel 67 van Richtlijn 2014/65/EU;

i) voor transactieregisters, de bevoegde autoriteit aangewezen overeenkomstig artikel 55 van Verordening (EU) nr. 648/2012;

j) voor beheerders van alternatieve beleggingsinstellingen, de bevoegde autoriteit aangewezen overeenkomstig artikel 44 van Richtlijn 2011/61/EU;

k) voor beheermaatschappijen, de bevoegde autoriteit aangewezen overeenkomstig artikel 97 van Richtlijn 2009/65/EG;

l) voor verzekerings- en herverzekeringsondernemingen, de bevoegde autoriteit

aangewezen overeenkomstig artikel 30 van Richtlijn 2009/138/EG;

m) voor verzekerings- of herverzekeringstussenpersonen, de bevoegde autoriteit aangewezen overeenkomstig artikel 12 van Richtlijn (EU) 2016/97;

n) voor instellingen voor bedrijfspensioenvoorziening, de bevoegde autoriteit aangewezen overeenkomstig artikel 47 van Richtlijn (EU) 2016/2341;

o) voor ratingbureaus, de bevoegde autoriteit aangewezen overeenkomstig artikel 21 van Verordening (EG) nr. 1060/2009;

p) voor wettelijke auditors en auditkantoren, de bevoegde autoriteit aangewezen overeenkomstig artikel 3, lid 2, en artikel 32 van Richtlijn 2006/43/EG;

q) voor beheerders van cruciale benchmarks, de bevoegde autoriteit aangewezen overeenkomstig de artikelen 40 en 41 van Verordening ***(EU) 2016/1011***;

r) voor aanbieders van crowdfundingdiensten, de bevoegde autoriteit aangewezen overeenkomstig artikel ***29*** van Verordening ***(EU) 2020/1503***;

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

Artikel 42

Samenwerking met structuren en autoriteiten ingesteld bij Richtlijn (EU) 2016/1148

1. Om samenwerking te bevorderen en uitwisseling op het gebied van toezicht mogelijk te maken tussen de krachtens deze verordening aangewezen bevoegde autoriteiten en de bij artikel 11 van Richtlijn (EU) 2016/1148 ingestelde samenwerkingsgroep, ***worden*** de ETA's en de bevoegde autoriteiten ***uitgenodigd deel te nemen aan de werkzaamheden van de samenwerkingsgroep, voor zover die werkzaamheden betrekking hebben op de toezichthoudende activiteiten met betrekking tot de onder punt 7), van bijlage II bij Richtlijn (EU) 2016/1148 vermelde entiteiten die ook krachtens artikel 28 van deze verordening zijn aangewezen als cruciale derde aanbieders van ICT-diensten***.

2. De bevoegde autoriteiten kunnen indien noodzakelijk overleggen met het centraal contactpunt en de nationale Computer security incident response teams bedoeld in respectievelijk de artikelen 8 en 9 van Richtlijn (EU) 2016/1148.

2 bis. Voorafgaand aan het verrichten van algemene onderzoeken en inspecties ter plaatse overeenkomstig de artikelen 33 en 34 van deze verordening stelt de leidende toezichthouder de overeenkomstig Richtlijn (EU) 2016/1148 aangewezen bevoegde autoriteiten hiervan in kennis en werkt hij met hen samen.

Artikel 43

Financiële sectoroverschrijdende oefeningen, communicatie en samenwerking

1. De ETA's kunnen via het Gemengd Comité en in samenwerking met de bevoegde autoriteiten, de ECB, het ESRB ***en, voor informatie met betrekking tot entiteiten die***

onder het toepassingsgebied van Verordening (EU) nr. 806/2014 vallen, de Gemeenschappelijke Afwikkelingsraad mechanismen invoeren om de uitwisseling van doeltreffende praktijken tussen financiële sectoren mogelijk te maken met het oog op de verbetering van de situatiekennis en de aanwijzing van gemeenschappelijke cyberkwetsbaarheden en sectoroverschrijdende risico's.

Zij kunnen crisisbeheer- en noodoefeningen met cyberaanvalsscenario's ontwikkelen om communicatiekanalen te ontwikkelen en geleidelijk een doeltreffende gecoördineerde respons op EU-niveau mogelijk te maken in geval van een ernstig grensoverschrijdend ICT-gerelateerd incident of een ***significante cyberdreiging*** met een systemisch effect op de financiële sector van de Unie in zijn geheel.

Deze oefeningen kunnen indien noodzakelijk ook testen in welke mate de financiële sector afhankelijk is van andere economische sectoren.

2. De bevoegde autoriteiten, de EBA, de ESMA of de Eiopa, de ECB, ***nationale afwikkelingsautoriteiten en, voor informatie met betrekking tot entiteiten die onder het toepassingsgebied van Verordening (EU) nr. 806/2014 vallen, de Gemeenschappelijke Afwikkelingsraad*** werken onderling nauw samen en wisselen informatie uit om hun taken overeenkomstig de artikelen 42 tot en met 48 uit te voeren. De bevoegde autoriteiten coördineren nauw hun toezicht teneinde inbreuken op deze verordening vast te stellen en te remediëren, goede praktijken te ontwikkelen en te bevorderen, samenwerking te faciliteren, een consistente interpretatie te bevorderen en in geval van meningsverschil rechtsgebiedoverschrijdende beoordelingen te verstrekken.

Artikel 44

Administratieve sancties en remediërende maatregelen

1. De bevoegde autoriteiten hebben alle toezichts-, onderzoeks- en sanctiebevoegdheden die noodzakelijk zijn om hun taken uit hoofde van deze verordening te vervullen.
2. De in lid 1 bedoelde bevoegdheden omvatten ten minste de bevoegdheid om:
   a) toegang te verkrijgen tot documenten of gegevens, in enigerlei vorm, die de bevoegde autoriteit relevant acht voor de uitoefening van haar taken, en een afschrift hiervan te ontvangen of te maken;
   b) inspecties of onderzoeken ter plaatse te verrichten;
   c) corrigerende en remediërende maatregelen te eisen voor inbreuken op de voorschriften van deze verordening.
3. Onverminderd het recht om overeenkomstig artikel 46 strafrechtelijke sancties op te leggen stellen de lidstaten regels vast met het oog op de invoering van passende administratieve sancties en remediërende maatregelen voor inbreuken op deze verordening, en waarborgen zij de doeltreffende toepassing daarvan.

Deze sancties en maatregelen moeten doeltreffend, evenredig en afschrikkend zijn.

4. De lidstaten verlenen de bevoegde autoriteiten de bevoegdheid om in geval van inbreuk op deze verordening ten minste de volgende administratieve sancties of remediërende maatregelen toe te passen:

a) het bevel waarbij de natuurlijke of rechtspersoon wordt gelast de gedraging te staken en af te zien van herhaling ervan;

b) de eis dat praktijken of gedragingen die ***in strijd worden geacht*** met de bepalingen van deze verordening, tijdelijk of definitief worden gestaakt, en dat herhaling van die praktijk of gedraging wordt voorkomen;

c) elk soort maatregel, onder meer van geldelijke aard, om te waarborgen dat financiële entiteiten aan de wettelijke vereisten blijven voldoen;

d) de eis, voor zover bij nationaal recht toegestaan, dat bestaande overzichten van gegevensverkeer die in het bezit zijn van een telecommunicatie-exploitant, worden overgelegd, indien er een redelijk vermoeden van inbreuk op deze verordening bestaat en deze overzichten van belang kunnen zijn voor een onderzoek naar inbreuken op deze verordening; en

e) publieke mededelingen, met inbegrip van publieke verklaringen waarbij de identiteit van de natuurlijke of rechtspersoon en de aard van de inbreuk worden bekendgemaakt.

5. Indien de bepalingen bedoeld in lid 2, punt c), en lid 4, van toepassing zijn op rechtspersonen, verlenen de lidstaten de desbetreffende autoriteiten de bevoegdheid om de administratieve sancties en remediërende maatregelen, met inachtneming van de voorwaarden waarin het nationale recht voorziet, toe te passen op leden van het leidinggevend orgaan en op andere personen die op grond van het nationale recht verantwoordelijk zijn voor de inbreuk.

6. De lidstaten zorgen ervoor dat het besluit waarbij administratieve sancties of remediërende maatregelen als bedoeld in lid 2, punt c), worden opgelegd, naar behoren gemotiveerd is en vatbaar is voor beroep.

Artikel 45

Uitoefening van de bevoegdheid tot het opleggen van administratieve sancties en remediërende maatregelen

1. De bevoegde autoriteiten oefenen de bevoegdheden tot het opleggen van administratieve sancties en remediërende maatregelen als bedoeld in artikel 44 uit in overeenstemming met hun nationale rechtskader, naargelang van het geval:

a) op rechtstreekse wijze;

b) in samenwerking met andere autoriteiten;

c) onder eigen verantwoordelijkheid door middel van delegatie aan andere autoriteiten;

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 44 opgelegde administratieve sanctie of remediërende maatregel rekening met de vraag in hoeverre de inbreuk opzettelijk is dan wel het resultaat van nalatigheid, en met andere relevante omstandigheden waaronder, in voorkomend geval:

a) de materialiteit, de ernst en de duur van de inbreuk;

b) de mate van verantwoordelijkheid van de voor de inbreuk verantwoordelijke natuurlijke of rechtspersoon;

c) de financiële draagkracht van de verantwoordelijke natuurlijke of rechtspersoon;

d) de omvang van de door de verantwoordelijke natuurlijke of rechtspersoon behaalde winsten of vermeden verliezen, voor zover deze kunnen worden bepaald;

e) de verliezen voor derde partijen ten gevolge van de inbreuk, voor zover deze kunnen worden vastgesteld;

f) de mate van medewerking van de verantwoordelijke natuurlijke of rechtspersoon met de bevoegde autoriteit, onverminderd de noodzaak om de terugbetaling van de door die persoon behaalde winsten of vermeden verliezen te garanderen;

g) eerdere inbreuken van de verantwoordelijke natuurlijke of rechtspersoon.

Artikel 46

Strafrechtelijke sancties

1. De lidstaten kunnen besluiten geen regels voor administratieve sancties of remediërende maatregelen vast te stellen met betrekking tot inbreuken waarop krachtens hun nationale recht strafrechtelijke sancties staan.

2. Indien de lidstaten ervoor hebben gekozen strafrechtelijke sancties te stellen op inbreuken op deze verordening, zorgen zij voor passende maatregelen waardoor de bevoegde autoriteiten over alle noodzakelijke bevoegdheden beschikken om met de gerechtelijke, met vervolging belaste of strafrechtelijke autoriteiten in hun rechtsgebied contacten te onderhouden met het oog op het inwinnen van specifieke informatie met betrekking tot strafrechtelijke onderzoeken of procedures ten aanzien van mogelijke inbreuken op deze verordening, en het verstrekken van deze informatie aan andere bevoegde autoriteiten en aan de EBA, de ESMA of de Eiopa, teneinde te voldoen aan hun verplichting tot samenwerking voor de toepassing van deze verordening.

Artikel 47

Kennisgevingsverplichting

De lidstaten doen uiterlijk op [OJ: insert date ***12 months*** after the date of entry into force] aan de Commissie, de ESMA, de EBA en de Eiopa kennisgeving van de wettelijke en

bestuursrechtelijke bepalingen ter uitvoering van dit hoofdstuk, met inbegrip van de toepasselijke strafrechtelijke bepalingen. De lidstaten doen aan de Commissie, de ESMA, de EBA en de Eiopa onverwijld kennisgeving van latere wijzigingen daarvan.

Artikel 48

Bekendmaking van administratieve sancties

1. De bevoegde autoriteiten maken op hun officiële website onverwijld alle niet voor beroep vatbare besluiten tot oplegging van een administratieve sanctie bekend, nadat de betrokken persoon van die sanctie in kennis is gesteld.

2. De in lid 1 bedoelde bekendmaking bevat informatie over het type en de aard van de inbreuk, ***de opgelegde sancties en, in uitzonderlijke gevallen,*** de identiteit van de verantwoordelijke personen en de opgelegde sancties.

3. Wanneer de bevoegde autoriteit na een per geval uitgevoerde beoordeling 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 onevenredig zou zijn, de stabiliteit van de financiële markten of het verloop van een lopend onderzoek in gevaar zou brengen, of, voor zover kan worden vastgesteld, de betrokken personen onevenredige schade zou berokkenen, kiest zij een van de volgende oplossingen met betrekking tot het besluit waarbij de administratieve sanctie wordt opgelegd:

   a) zij stelt de bekendmaking van het besluit uit totdat alle redenen voor niet-bekendmaking vervallen;

   b) zij zorgt voor een bekendmaking op basis van anonimiteit in overeenstemming met het nationale recht; of

   c) zij onthoudt zich van de bekendmaking wanneer de in punten a) en b) vermelde keuzemogelijkheden ontoereikend worden geacht om de afwezigheid van gevaar voor de stabiliteit van de financiële markten te garanderen of wanneer de bekendmaking niet evenredig zou zijn met de clementie van de opgelegde sanctie.

4. In het geval van een besluit tot bekendmaking van een administratieve sanctie op basis van anonimiteit als bedoeld in lid 3, punt b), kan de bekendmaking van de betrokken gegevens worden uitgesteld.

5. Wanneer een bevoegde autoriteit een besluit tot oplegging van een administratieve sanctie bekendmaakt dat vatbaar is voor beroep bij de betrokken gerechtelijke autoriteiten, maken de bevoegde autoriteiten deze informatie en in een later stadium verdere informatie over het resultaat van een dergelijk beroep onmiddellijk kenbaar op hun officiële website. Elke rechterlijke beslissing tot nietigverklaring van een besluit waarbij een administratieve sanctie wordt opgelegd, wordt eveneens bekendgemaakt.

6. De bevoegde autoriteiten zorgen ervoor dat een besluit als bedoeld in de leden 1 tot en met 4 gedurende een periode van ten minste vijf jaar na de bekendmaking ervan op hun officiële website blijft staan. In de bekendmaking opgenomen persoonsgegevens worden op de officiële website van de bevoegde autoriteit niet langer bewaard dan

noodzakelijk is overeenkomstig de toepasselijke voorschriften inzake gegevensbescherming.

Artikel 49

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 uit hoofde van 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 mag aan geen enkele andere persoon of autoriteit worden verstrekt, tenzij op grond van Unierechtelijke of nationaalrechtelijke bepalingen.
4. Alle uitwisseling van informatie tussen de bevoegde autoriteiten uit hoofde van 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.

HOOFDSTUK VIII

GEDELEGEERDE HANDELINGEN

Artikel 50

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 28, lid 3, en artikel 38, lid 2, bedoelde gedelegeerde handelingen vast te stellen wordt aan de Commissie verleend voor een termijn van vier jaar vanaf [PO: insert date 5 years after the date of entry into force of this Regulation]. ***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 28, lid 3, en artikel 38, 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 28, lid 3, en artikel 38, 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 51

Herzieningsclausule

Uiterlijk [PO: insert date 5 years after the date of entry into force of this Regulation] voert de Commissie, na raadpleging van de EBA, de ESMA, de Eiopa 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. ***In het verslag wordt ten minste het volgende beoordeeld:***

a) ***de mogelijkheid om het toepassingsgebied van deze verordening uit te breiden tot beheerders van betalingssystemen;***

b) ***het vrijwillige karakter van het melden van significante cyberdreigingen;***

c) de criteria voor de aanwijzing van cruciale derde aanbieders van ICT-diensten in artikel 28, lid 2; ***en***

d) ***de doeltreffendheid van de besluitvorming van het orgaan voor gezamenlijk toezicht en de uitwisseling van informatie tussen het orgaan voor gezamenlijk toezicht en nationale bevoegde autoriteiten die geen lid zijn van het orgaan voor gezamenlijk toezicht.***

AFDELING II

WIJZIGINGEN

Artikel 52

Wijzigingen in Verordening (EG) nr. 1060/2009

In bijlage I bij Verordening (EG) nr. 1060/2009 wordt de eerste alinea van afdeling A, punt 4, 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) 2021/xx van het Europees Parlement en de Raad* [DORA].

* Verordening (EU) 2021/xx van het Europees Parlement en de Raad […] (PB L XX, DD.MM.YYYY, blz. X).".

Artikel 53

Wijzigingen in 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) 2021/xx van het Europees Parlement en de Raad * [DORA].

* Verordening (EU) 2021/xx van het Europees Parlement en de Raad […] (PB L XX, DD.MM.YYYY, blz. X).".

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 bedrijfscontinuïteits- en noodherstelplan, dat ICT-continuïteits- en noodherstelplannen omvat die zijn opgezet in overeenstemming met Verordening (EU) 2021/xx [DORA], 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:

"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, met uitsluiting van ICT-continuïteits- en noodherstelplannen, worden gespecificeerd.”.

(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) 2021/xx [DORA].

2. Een transactieregister zorgt voor de opstelling, uitvoering en instandhouding van een passend bedrijfscontinuïteits- en noodherstelplan, met inbegrip van ICT-continuïteits- en noodherstelplannen die zijn opgezet in overeenstemming met Verordening (EU) 2021/xx [DORA], 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) Artikel 80, lid 1, wordt geschrapt.

Artikel 54

Wijzigingen in 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) 2021/xx van het Europees Parlement en de Raad* [DORA], alsmede via andere relevante passende instrumenten, controles en procedures voor andere soorten operationele risico’s, inclusief voor alle effectenafwikkelingssystemen die zij exploiteert.

* Verordening (EU) 2021/xx van het Europees Parlement en de Raad […] (PB L XX, DD.MM.YYYY, blz. X).”.

(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-continuïteits- en noodherstelplannen die zijn opgezet in overeenstemming met Verordening (EU) 2021/xx [DORA], 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 11, leden 5 en 7, van Verordening (EU) 2021/xx [DORA].”.

I

Artikel 55

Wijzigingen in 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 geschrapt;

b) lid 8, punt c), wordt vervangen door:

“c) de concrete organisatorische eisen die zijn vastgelegd in de leden 3 en 5.”.

(2) Artikel 27 novies wordt als volgt gewijzigd:

a) lid 5 wordt geschrapt;

b) in lid 8 wordt punt e), vervangen door:

“e) de concrete organisatorische eisen die zijn vastgelegd in lid 4.”.

(3) Artikel 27 decies wordt als volgt gewijzigd:

a) lid 3 wordt geschrapt;

b) in lid 5 wordt punt b) vervangen door:

“b) de concrete organisatorische eisen die zijn vastgelegd in de leden 2 en 4.”.

Artikel 56

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 [PO: insert date ***24*** months after the date of entry into force].

De artikelen 23 en 24 zijn evenwel van toepassing met ingang van [PO: insert date 36 months after the date of entry into force of this Regulation].

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

lidstaat.

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

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

PROCEDURE VAN DE BEVOEGDE COMMISSIE

Titel	Digitale operationele veerkracht voor de financiële sector en wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014
Document- en procedurenummers	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Datum indiening bij EP	24.9.2020
Bevoegde commissie Datum bekendmaking	ECON 17.12.2020
Adviserende commissies Datum bekendmaking	ITRE IMCO 17.12.2020 17.12.2020
Geen advies Datum besluit	ITRE IMCO 15.10.2020 27.10.2020
Rapporteurs Datum benoeming	Billy Kelleher 15.10.2020
Behandeling in de commissie	14.4.2021 14.6.2021
Datum goedkeuring	1.12.2021
Uitslag eindstemming	+: 44 –: 5 0: 5
Bij de eindstemming aanwezige leden	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Bij de eindstemming aanwezige vaste plaatsvervangers	Lefteris Christoforou
Datum indiening	7.12.2021

HOOFDELIJKE EINDSTEMMING IN DE BEVOEGDE COMMISSIE

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Lefteris Nikolaou-Alavanos

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Verklaring van de gebruikte tekens:
+ : voor
- : tegen
0 : onthouding