EUROPESE
COMMISSIE

Brussel, 24.9.2020
COM(2020) 595 final

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)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

- Motivering en doel van het voorstel

Dit voorstel maakt deel uit van het pakket digitaal geldwezen, een pakket maatregelen om het potentieel van het digitale geldwezen verder te bevorderen en te ondersteunen en tegelijkertijd de daaruit voortvloeiende risico's te beperken. Het strookt met de prioriteiten van de Commissie om Europa klaar te maken voor het digitale tijdperk en een toekomstbestendige economie op te bouwen die werkt voor de mensen. Het pakket digitaal geldwezen omvat een nieuwe strategie voor het digitale geldwezen voor de financiële sector van de EU[1] om ervoor te zorgen dat de EU de digitale revolutie omarmt en stimuleert met een leidende rol voor innovatieve Europese bedrijven, zodat de voordelen van het digitale geldwezen beschikbaar komen voor consumenten en bedrijven. Naast dit voorstel omvat het pakket ook een voorstel voor een verordening betreffende markten voor cryptoactiva[2], een voorstel voor een verordening betreffende een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie (DLT)[3] en een voorstel voor een richtlijn om bepaalde gerelateerde EU-regels inzake financiële diensten te verduidelijken of te wijzigen[4]. Digitalisering en operationele veerkracht in de financiële sector zijn twee kanten van dezelfde medaille. Digitale technologieën of informatie- en communicatietechnologieën (ICT) brengen zowel kansen als risico's mee. Die moeten goed worden begrepen en beheerd, vooral in tijden van stress.

Beleidsmakers en toezichthouders hebben zich daarom steeds meer gericht op risico's die voortvloeien uit het gebruik van ICT. Zij hebben met name geprobeerd de veerkracht van bedrijven te vergroten door normen vast te stellen en regelgevings- of toezichtwerkzaamheden te coördineren. Dit werk is op internationaal en Europees niveau verricht, zowel sectoroverkoepelend als voor een aantal specifieke sectoren, waaronder financiële diensten.

ICT-risico's blijven echter een uitdaging vormen voor de operationele veerkracht, de prestaties en de stabiliteit van het financiële stelsel van de EU. De hervorming die volgde op de financiële crisis van 2008, heeft in de eerste plaats de financiële veerkracht[5] van de financiële sector van de EU versterkt en alleen indirect ICT-risico's op sommige gebieden aangepakt, als onderdeel van de maatregelen om operationele risico's in ruimere zin aan te pakken.

Hoewel de na de crisis in de EU-wetgeving inzake financiële diensten aangebrachte wijzigingen uitmondden in een gemeenschappelijk rulebook dat grote delen van de financiële risico's in verband met financiële diensten regelt, werd de digitale operationele veerkracht

---

1 Mededeling van de Commissie aan het Europees Parlement, de Europese Raad, de Raad, de Europese Centrale Bank, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over een EU-strategie voor het digitale geldwezen, COM(2020)591 final van 23 september 2020.

2 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Richtlijn (EU) 2019/1937, COM(2020) 593.

3 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie, COM(2020) 594.

4 Voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van de Richtlijnen 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 en EU/2016/2341, COM(2020) 596.

5 De verschillende genomen maatregelen zijn vooral bedoeld om de kapitaalmiddelen en de liquiditeit van financiële entiteiten te verhogen en de markt- en kredietrisico's te verminderen.

niet volledig behandeld. De in verband met dit laatste aspect genomen maatregelen hadden enkele kenmerken die de doeltreffendheid ervan beperkten. Zij waren bijvoorbeeld vaak ontworpen als richtlijnen voor minimumharmonisatie of op beginselen gebaseerde verordeningen, waardoor er aanzienlijke ruimte was voor uiteenlopende benaderingen binnen de eengemaakte markt. Voorts is er vaak slechts in beperkte of onvolledige mate aandacht besteed aan ICT-risico's in de context van het afdekken van operationeel risico. Tot slot variëren deze maatregelen in de sectorale wetgeving inzake financiële diensten. Het optreden op het niveau van de Unie strookte dus niet volledig met wat Europese financiële entiteiten nodig hadden voor het beheer van operationele risico's op een wijze die de gevolgen van ICT-incidenten kan weerstaan, tegengaan en goedmaken. Evenmin bood het de financiële toezichthouders de meest geschikte instrumenten om zich te kwijten van hun taak om financiële instabiliteit te voorkomen wanneer die ICT-risico's werkelijkheid worden.

Het ontbreken van gedetailleerde en alomvattende regels op EU-niveau inzake digitale operationele veerkracht heeft geleid tot een veelheid aan nationale regelgevingsinitiatieven (bv. inzake het testen van digitale operationele veerkracht) en toezichtbenaderingen (bv. het aanpakken van ICT-afhankelijkheid van derden). Maatregelen op het niveau van de lidstaten hebben echter slechts een beperkt effect gezien het grensoverschrijdende karakter van ICT-risico's. Bovendien hebben de ongecoördineerde nationale initiatieven geleid tot overlappingen, inconsistenties, dubbele vereisten, hoge administratieve en nalevingskosten – met name voor grensoverschrijdende financiële entiteiten – of ICT-risico's die niet worden ontdekt en dus niet worden aangepakt. Deze situatie versnippert de eengemaakte markt, ondermijnt de stabiliteit en integriteit van de financiële sector van de EU en brengt de bescherming van consumenten en beleggers in gevaar.

Daarom moet een gedetailleerd en alomvattend kader voor digitale operationele veerkracht van financiële entiteiten in de EU worden opgezet. Dit kader zal het onderdeel digitaalrisicobeheer van het gemeenschappelijk rulebook verdiepen. Het zal met name de uitvoering van ICT-risicobeheer door financiële entiteiten verbeteren en stroomlijnen, een grondige toetsing van ICT-systemen invoeren, toezichthouders beter bewust maken van cyberrisico's en ICT-gerelateerde incidenten waarmee financiële entiteiten te maken krijgen, en financiële toezichthouders bevoegdheden geven om toezicht te houden op risico's die voortvloeien uit het feit dat financiële entiteiten afhankelijk zijn van derde aanbieders van ICT-diensten. Het voorstel zal zorgen voor een consistent mechanisme voor het melden van incidenten om te helpen de administratieve lasten voor financiële entiteiten te verlichten en de doeltreffendheid van het toezicht te versterken.

- Verenigbaarheid met bestaande bepalingen op het beleidsterrein

Dit voorstel maakt deel uit van bredere werkzaamheden op Europees en internationaal niveau om de cyberbeveiliging van financiële diensten te versterken en bredere operationele risico's aan te pakken[6].

Het geeft ook gevolg aan het in 2019 uitgebrachte gezamenlijke technische advies[7] van de Europese toezichthoudende autoriteiten (ETA's), waarin werd opgeroepen tot een meer samenhangende aanpak van ICT-risico's in de financiële sector en de Commissie werd aanbevolen om op evenredige wijze de digitale operationele veerkracht van de

[6] Bazels Comité voor bankentoezicht, *Cyber-resilience: Range of practices*, december 2018 en *Principles for sound management of operational risk (PSMOR)*, oktober 2014.

[7] Gezamenlijk advies van de Europese toezichthoudende autoriteiten aan de Europese Commissie over de noodzaak van verbeterde wetgeving inzake ICT-risicobeheer in de financiële sector van de EU, JC 2019 26 (2019).

financiëledienstensector te versterken door middel van een sectorspecifiek EU-initiatief. Het advies van de ETA's was een reactie op het FinTech-actieplan van de Commissie uit 2018[8].

- Verenigbaarheid met andere beleidsterreinen van de Unie

Zoals voorzitter Von der Leyen in haar politieke beleidslijnen[9] heeft verklaard en nader is uitgewerkt in de mededeling "De digitale toekomst van Europa vormgeven"[10], is het van cruciaal belang dat Europa alle vruchten plukt van het digitale tijdperk en zijn industrie en innovatiecapaciteit versterkt, binnen veilige en ethische grenzen. De Europese datastrategie[11] omvat vier pijlers – gegevensbescherming, grondrechten, veiligheid en cyberbeveiliging – als essentiële voorwaarden voor een samenleving die sterk staat door slim datagebruik. Recenter is het werk van het Europees Parlement aan een verslag over het digitale geldwezen, waarin onder meer wordt opgeroepen tot een gemeenschappelijke aanpak inzake cyberveerkracht van de financiële sector[12].Een wetgevingskader ter versterking van de digitale operationele veerkracht van financiële entiteiten in de EU strookt met deze beleidsdoelstellingen. Het voorstel zou ook beleid ondersteunen dat gericht is op het herstel van de coronapandemie, aangezien het ervoor zou zorgen dat de toegenomen afhankelijkheid van het digitale geldwezen gepaard gaat met operationele veerkracht.

Het initiatief zou de voordelen van het horizontale kader voor cyberbeveiliging (bv. de richtlijn inzake de beveiliging van netwerk- en informatiesystemen, NIS-richtlijn) bewaren door de financiële sector binnen het toepassingsgebied ervan te houden. De financiële sector zou nauw verbonden blijven met het NIS-samenwerkingsorgaan en de financiële toezichthouders zouden relevante informatie kunnen uitwisselen binnen het bestaande NIS-ecosysteem. Het initiatief zou stroken met de richtlijn betreffende Europese kritieke infrastructuur, die momenteel wordt herzien om kritieke infrastructuren beter te beschermen en weerbaarder te maken tegen niet-cybergerelateerde dreigingen. Tot slot is dit voorstel volledig in overeenstemming met de strategie voor de veiligheidsunie[13], waarin werd opgeroepen tot een initiatief voor de digitale operationele veerkracht van de financiële sector gezien zijn grote afhankelijkheid van ICT-diensten en grote kwetsbaarheid voor cyberaanvallen.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- Rechtsgrondslag

Dit voorstel voor een verordening is gebaseerd op artikel 114 VWEU.

---

8 Europese Commissie, FinTech-actieplan, COM(2018) 109 final.

9 Voorzitter Ursula von der Leyen, Politieke beleidslijnen voor de volgende Europese Commissie, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

10 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's "De digitale toekomst van Europa vormgeven", COM(2020) 67 final.

11 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's "Een Europese datastrategie", COM(2020) 66 final.

12 Verslag met aanbevelingen aan de Commissie betreffende digitaal geldwezen: opkomende risico's in verband met cryptovaluta - uitdagingen inzake regelgeving en toezicht op het gebied van financiële diensten, instellingen en markten (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 Mededeling van de Commissie aan het Europees Parlement, de Europese Raad, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de EU-strategie voor de veiligheidsunie, COM(2020) 605 final.

Het neemt belemmeringen weg voor en verbetert de totstandbrenging en werking van de interne markt voor financiële diensten door de regels te harmoniseren die van toepassing zijn op het gebied van ICT-risicobeheer, rapportage, tests en ICT-risico van derde aanbieders. De huidige verschillen op dit gebied aan de wetgevings- en toezichtzijde en op nationaal en EU-niveau vormen obstakels voor de eengemaakte markt voor financiële diensten, omdat financiële entiteiten die grensoverschrijdende activiteiten verrichten, te maken hebben met verschillende – waar ze elkaar niet overlappen – wettelijke voorschriften of toezichtverwachtingen die de uitoefening van hun vrijheid van vestiging en van dienstverrichting kunnen belemmeren. Verschillende regels verstoren ook de concurrentie tussen hetzelfde type financiële entiteiten in verschillende lidstaten. Bovendien kan op gebieden waar harmonisatie geheel of gedeeltelijk ontbreekt, de ontwikkeling van uiteenlopende nationale regels of benaderingen – ongeacht of ze al gelden of zich nog in het proces van goedkeuring en tenuitvoerlegging op nationaal niveau bevinden – een afschrikkend effect hebben ten aanzien van de uitoefening van de vrijheden van de eengemaakte markt voor financiële diensten. Dit is met name het geval met betrekking tot digitale operationele testkaders en het toezicht op cruciale derde aanbieders van ICT-diensten.

Aangezien het voorstel gevolgen heeft voor verscheidene richtlijnen van het Europees Parlement en de Raad die zijn vastgesteld op basis van artikel 53, lid 1, VWEU, wordt tegelijkertijd ook een voorstel voor een richtlijn goedgekeurd om rekening te houden met de noodzakelijke wijzigingen van die richtlijnen.

- Subsidiariteit

Omdat financiële diensten sterk met elkaar samenhangen, financiële entiteiten in aanzienlijke mate grensoverschrijdend actief zijn en de financiële sector als geheel sterk afhankelijk is van derde aanbieders van ICT-diensten, moeten de voorwaarden worden geschapen voor een sterke digitale operationele veerkracht als aangelegenheid van gemeenschappelijk belang om de financiële markten van de EU gezond te houden. Verschillen die het gevolg zijn van ongelijke of gedeeltelijke regelingen, overlappingen of uiteenlopende verplichtingen voor dezelfde financiële entiteiten die grensoverschrijdend opereren of meerdere vergunningen[14] hebben op de eengemaakte markt, kunnen alleen efficiënt worden aangepakt op het niveau van de Unie.

Dit voorstel harmoniseert de digitale operationele component van een sterk geïntegreerde en onderling verbonden sector die op de meeste andere belangrijke gebieden reeds profiteert van één enkel geheel van regels en toezicht. Voor zaken als ICT-gerelateerde incidentrapportage kunnen alleen geharmoniseerde regels van de Unie de administratieve lasten en financiële kosten terugdringen die het gevolg zijn van het feit dat hetzelfde ICT-incident aan verschillende autoriteiten van de Unie en de lidstaten moet worden gerapporteerd. EU-optreden is ook nodig om wederzijdse erkenning van resultaten van geavanceerde tests op digitale operationele veerkracht te vergemakkelijken voor entiteiten die grensoverschrijdend actief zijn, waarvoor – wanneer Unieregels ontbreken – in verschillende lidstaten verschillende kaders gelden of kunnen gelden. Alleen optreden op het niveau van de Unie kan verschillen in de door de lidstaten ingevoerde testmethoden aanpakken. EU-breed optreden is ook nodig om het gebrek aan passende toezichtsbevoegdheden aan te pakken voor het monitoren van risico's die voortvloeien uit derde aanbieders van ICT-diensten, waaronder concentratie- en besmettingsrisico's voor de financiële sector.

[14] Dezelfde financiële entiteit kan vergunningen als bank, beleggingsonderneming en betalingsinstelling hebben die allemaal door een verschillende toezichthouder in een of meer lidstaten zijn afgegeven.

- Evenredigheid

De voorgestelde regels gaan niet verder dan nodig is om de doelstellingen van het voorstel te verwezenlijken. Zij hebben alleen betrekking op de aspecten die de lidstaten zelf niet kunnen verwezenlijken en waarvoor de administratieve lasten en kosten in verhouding staan tot de specifieke en algemene doelstellingen die moeten worden bereikt.

De evenredigheid wordt qua reikwijdte en intensiteit bepaald aan de hand van kwalitatieve en kwantitatieve beoordelingscriteria. Die moeten ervoor zorgen dat de nieuwe regels enerzijds voor alle financiële entiteiten gelden en anderzijds zijn toegesneden op de risico's en behoeften van hun specifieke kenmerken qua omvang en bedrijfsprofiel. De evenredigheid is ook ingebed in de regels inzake ICT-risicobeheer, het testen van digitale veerkracht, de rapportage van ernstige ICT-gerelateerde incidenten en het toezicht op cruciale derde aanbieders van ICT-diensten.

- Keuze van het instrument

De maatregelen die nodig zijn voor ICT-risicobeheer, de rapportage van ICT-gerelateerde incidenten, testen en toezicht op cruciale derde aanbieders van ICT-diensten, moeten in een verordening worden opgenomen om ervoor te zorgen dat de gedetailleerde voorschriften op uniforme en doeltreffende wijze rechtstreeks van toepassing zijn, zonder afbreuk te doen aan de evenredigheid en de specifieke regels waarin deze verordening voorziet. Consistentie bij het aanpakken van digitale operationele risico's draagt bij tot een groter vertrouwen in het financiële stelsel en zorgt voor het behoud van de stabiliteit ervan. Aangezien het gebruik van een verordening helpt de complexiteit van de regelgeving te verminderen, de convergentie van het toezicht bevordert en de rechtszekerheid vergroot, draagt deze verordening ook bij tot het beperken van de nalevingskosten van financiële entiteiten, met name voor die welke grensoverschrijdend actief zijn, wat op zijn beurt helpt concurrentieverstoringen tegen te gaan.

Deze verordening maakt ook een einde aan verschillen in wetgeving en ongelijke nationale regelgevings- of toezichtsbenaderingen met betrekking tot ICT-risico's en neemt zo obstakels voor de eengemaakte markt voor financiële diensten weg, met name voor de vlotte uitoefening van de vrijheid van vestiging en het verlenen van diensten voor financiële entiteiten met grensoverschrijdende aanwezigheid.

Tot slot is het gemeenschappelijk rulebook vooral tot stand gekomen door middel van verordeningen, zodat bij de actualisering ervan met het onderdeel digitale operationele veerkracht hetzelfde instrument moet worden gekozen.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- Evaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan

Tot dusver is er geen Uniewetgeving inzake financiële diensten die focust op operationele veerkracht of die uit digitalisering voortvloeiende risico's grondig aanpakt; dat geldt ook voor de voorschriften die meer in het algemeen betrekking hebben op de operationeelrisicodimensie met ICT-risico als subcomponent. Het optreden van de Unie heeft tot nu toe geholpen tegemoet te komen aan de behoeften en problemen die zich voordeden in de nasleep van de financiële crisis van 2008: de kredietinstellingen waren onvoldoende gekapitaliseerd, de financiële markten waren onvoldoende geïntegreerd en de harmonisatie was tot op dat moment minimaal gehouden. ICT-risico werd toen niet als prioriteit

beschouwd, en als gevolg daarvan hebben de rechtskaders voor de verschillende financiële subsectoren zich op ongecoördineerde wijze ontwikkeld. Toch heeft het optreden van de Unie zijn doel bereikt van waarborging van de financiële stabiliteit en totstandbrenging van één set geharmoniseerde prudentiële en marktgedragsregels die gelden voor financiële entiteiten in de hele EU. Aangezien de factoren die in het verleden het wetgevende optreden van de Unie aanstuurden, geen aanleiding gaven tot specifieke of alomvattende regels die rekening houden met het wijdverbreide gebruik van digitale technologieën en de daaruit voortvloeiende risico's in de financiële sector, lijkt het moeilijk om een expliciete evaluatie uit te voeren. Een impliciete evaluatie en de daaruit voortvloeiende wetgevingswijzigingen komen tot uiting in elke pijler van deze verordening.

- Raadpleging van belanghebbenden

De Commissie heeft de belanghebbenden tijdens het gehele proces van voorbereiding van dit voorstel geraadpleegd:

i) De Commissie heeft een specifieke openbare raadpleging gehouden (19 december 2019 - 19 maart 2020)[15];

ii) De Commissie heeft het publiek geraadpleegd via een aanvangseffectbeoordeling (19 december 2019 - 16 januari 2020)[16];

iii) De diensten van de Commissie hebben tweemaal (op 18 mei 2020 en 16 juli 2020) deskundigen van de lidstaten geraadpleegd in de Deskundigengroep banken, betalingen en verzekeringen (EGBPI)[17];

iv) De diensten van de Commissie hebben een specifiek webinar over digitale operationele veerkracht gehouden als onderdeel van de reeks Digital Finance Outreach-evenementen van 2020 (19 mei 2020).

Het doel van de openbare raadpleging was de Commissie te informeren over de ontwikkeling van een mogelijk sectoroverkoepelend EU-kader voor digitale operationele veerkracht op het gebied van financiële diensten. Uit de reacties bleek dat er brede steun bestaat voor de invoering van een specifiek kader met acties die gericht zijn op de vier gebieden waarop de raadpleging betrekking had. Tegelijkertijd werd benadrukt dat de evenredigheid moet worden gewaarborgd en dat de wisselwerking met de horizontale regels van de NIS-richtlijn zorgvuldig moet worden behandeld en uitgelegd. De Commissie heeft twee reacties op de aanvangseffectbeoordeling ontvangen, waarin de respondenten specifieke aspecten aan de orde stelden die verband houden met hun werkterrein.

De lidstaten hebben tijdens de EGBPI-bijeenkomst van 18 mei 2020 sterke steun uitgesproken voor de versterking van de digitale operationele veerkracht van de financiële sector door middel van de geplande acties op basis van de vier door de Commissie geschetste elementen. De lidstaten hebben ook benadrukt dat de nieuwe regels goed moeten worden afgestemd op die welke operationeel risico behandelen (binnen de EU-wetgeving inzake financiële diensten) en op de horizontale regels inzake cyberbeveiliging (NIS-richtlijn). Tijdens de

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

tweede bijeenkomst hebben sommige lidstaten benadrukt dat de evenredigheid moet worden gewaarborgd en rekening moet worden gehouden met de specifieke situatie van kleine ondernemingen of dochterondernemingen van grotere groepen, en dat ook een sterk mandaat nodig is voor de nationale bevoegde autoriteiten die bij het toezicht betrokken zijn.

Het voorstel bouwt ook voort op en verwerkt de feedback die is vergaard tijdens bijeenkomsten met belanghebbenden en EU-autoriteiten en -instellingen. De belanghebbenden, inclusief derde aanbieders van ICT-diensten, steunen over het geheel genomen het voorstel. Uit een analyse van de ontvangen feedback blijkt dat ertoe werd opgeroepen bij het opstellen van regels de evenredigheid te vrijwaren en een op beginselen en risico's gebaseerde aanpak te volgen. Wat de instellingen betreft, was de belangrijkste input afkomstig van het Europees Comité voor systeemrisico's (ESRB), de ETA's, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en de Europese Centrale Bank (ECB), alsook van de bevoegde autoriteiten van de lidstaten.

- Bijeenbrengen en gebruik van expertise

Bij de voorbereiding van dit voorstel heeft de Commissie zich gebaseerd op kwalitatieve en kwantitatieve gegevens uit erkende bronnen, waaronder de twee gezamenlijke technische adviezen van de ETA's. Deze zijn aangevuld met vertrouwelijke input en openbare verslagen van toezichthoudende autoriteiten, internationale normalisatie-instellingen en toonaangevende onderzoeksinstellingen, alsook kwantitatieve en kwalitatieve input van geïdentificeerde belanghebbenden in de mondiale financiële sector.

- Effectbeoordeling

Dit voorstel gaat vergezeld van een effectbeoordeling[18], die op 29 april 2020 aan de Raad voor regelgevingstoetsing (RSB) is voorgelegd en op 29 mei 2020 goedkeuring kreeg. De RSB heeft op sommige gebieden verbeteringen aanbevolen om: i) meer informatie te verstrekken over de wijze waarop evenredigheid zou worden gewaarborgd; ii) beter te belichten in hoeverre de voorkeursoptie verschilt van het gezamenlijke technische advies van de ETA's en waarom die optie de beste is; en iii) te belichten wat de wisselwerking is tussen het voorstel en de bestaande EU-wetgeving, waaronder regels die momenteel worden herzien. De effectbeoordeling werd in die zin aangepast, waarbij ook rekening werd gehouden met de gedetailleerdere opmerkingen van de RSB.

De Commissie heeft een aantal beleidsopties overwogen voor de ontwikkeling van een kader voor digitale operationele veerkracht:

- "Niets doen": de regels inzake operationele veerkracht zouden nog steeds voortvloeien uit de huidige uiteenlopende reeks bepalingen inzake financiële diensten, gedeeltelijk uit de NIS-richtlijn, en uit bestaande of toekomstige nationale regelingen;
- Optie 1: versterking van de kapitaalbuffers: er zouden extra kapitaalbuffers worden ingevoerd om de financiële entiteiten beter in staat te stellen verliezen op te vangen

[18] Werkdocument van de diensten van de Commissie - Effectbeoordeling bij het document 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, SWD(2020)198 van 24.9.2020.

die zouden kunnen ontstaan als gevolg van een gebrek aan digitale operationele veerkracht;

- Optie 2: invoering van een wetgevingshandeling inzake digitale operationele veerkracht op het gebied van financiële diensten: de voorwaarden scheppen voor een alomvattend kader op EU-niveau met consistente regels om tegemoet te komen aan de behoeften inzake digitale operationele veerkracht van alle gereglementeerde financiële entiteiten en een kader voor toezicht op cruciale derde aanbieders van ICT-diensten oprichten;
- Optie 3: een wetgevingshandeling inzake digitale operationele veerkracht op het gebied van financiële diensten in combinatie met gecentraliseerd toezicht op cruciale derde aanbieders van ICT-diensten: naast een wetgevingshandeling inzake digitale operationele veerkracht (optie 2) zou een nieuwe autoriteit worden opgericht om toezicht te houden op de verlening van diensten door derde aanbieders van ICT-diensten.

De tweede optie werd gekozen omdat de meeste van de beoogde doelstellingen worden bereikt op een wijze die doeltreffend en doelmatig is en strookt met andere beleidsmaatregelen van de Unie. De meeste belanghebbenden geven ook de voorkeur aan deze optie.

De gekozen optie zou eenmalige en terugkerende kosten meebrengen[19]. De eenmalige kosten houden voornamelijk verband met investeringen in IT-systemen, en als zodanig zijn ze moeilijk te kwantificeren gezien de uiteenlopende staat van de complexe IT-landschappen van bedrijven, en met name van hun bestaande IT-systemen. Toch zullen deze kosten voor grote bedrijven waarschijnlijk beperkt zijn, gezien de aanzienlijke ICT-investeringen die zij reeds hebben gedaan. Ook voor kleinere bedrijven zullen de kosten naar verwachting beperkt zijn, omdat evenredige maatregelen zouden gelden wegens hun lagere risico.

De gekozen optie zou in economisch, sociaal en ecologisch opzicht positieve gevolgen hebben voor kleine en middelgrote bedrijven die in de financiëledienstensector actief zijn. Het voorstel zou kleine en middelgrote bedrijven duidelijkheid verschaffen over de vraag welke regels van toepassing zijn, wat de nalevingskosten zou verminderen.

Vooral consumenten en beleggers zouden te maken krijgen met de sociale gevolgen van de gekozen beleidsoptie. Meer digitale operationele veerkracht van het financiële stelsel van de EU zou het aantal incidenten en de gemiddelde kosten daarvan doen afnemen. De samenleving als geheel zou baat hebben bij het toegenomen vertrouwen in de financiëledienstensector.

Tot slot zou de gekozen beleidsoptie, wat de ecologische gevolgen betreft, een intensiever gebruik van de nieuwste generatie ICT-infrastructuren en -diensten aanmoedigen, die naar verwachting ecologisch duurzamer zullen worden.

- Resultaatgerichtheid en vereenvoudiging

Door een einde te maken aan overlappende vereisten inzake ICT-gerelateerde incidentrapportage, zouden de administratieve lasten en de daarmee gemoeide kosten worden verminderd. Voorts zouden geharmoniseerde tests van de digitale operationele veerkracht met

[19] Ibid, blz. 89-94.

wederzijdse erkenning binnen de eengemaakte markt de kosten doen dalen, met name voor grensoverschrijdende bedrijven die anders met meerdere tests in verschillende lidstaten te maken zouden kunnen krijgen[20].

- Grondrechten

De EU hecht aan de waarborging van hoge normen inzake de bescherming van grondrechten. Alle vrijwillige regelingen voor het delen van informatie tussen financiële entiteiten die door deze verordening worden bevorderd, zouden worden uitgevoerd in vertrouwde omgevingen met volledige inachtneming van de gegevensbeschermingsregels van de Unie, met name Verordening (EU) 2016/679 van het Europees Parlement en de Raad[21], vooral wanneer de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke.

4. GEVOLGEN VOOR DE BEGROTING

Aangezien de huidige verordening de ETA's een grotere rol geeft door hun bevoegdheden te verlenen inzake passend toezicht op cruciale derde aanbieders van ICT-diensten, zou het voorstel qua gevolgen voor de begroting betekenen dat extra middelen moeten worden uitgetrokken, met name voor de uitvoering van de toezichttaken (zoals inspecties ter plaatse en online, en audits) en de inschakeling van personeel met specifieke ICT-beveiligingsexpertise.

De omvang en de verdeling van deze kosten zullen afhangen van de omvang van de nieuwe toezichtsbevoegdheden en de (precieze) taken die door de ETA's moeten worden uitgevoerd. Aan nieuwe personele middelen zullen de EBA, ESMA en Eiopa in totaal 18 voltijdwerknemers (vte) – 6 vte voor elke autoriteit – nodig hebben wanneer de verschillende bepalingen van het voorstel van toepassing worden (geraamd op 15,71 miljoen EUR voor de periode 2022-2027). De ETA's zullen ook extra IT-kosten, kosten van dienstreizen voor inspecties ter plaatse en vertaalkosten (geraamd op 12 miljoen EUR voor de periode 2022-2027), alsook andere administratieve kosten (geraamd op 2,48 miljoen EUR voor de periode 2022-2027) maken. De totale geraamde kosten bedragen dus ongeveer 30,19 miljoen EUR voor de periode 2022-2027.

Hoewel de personeelsbezetting (bv. nieuwe personeelsleden en andere uitgaven in verband met de nieuwe taken) die nodig is voor direct toezicht, in de loop der tijd zal afhangen van de ontwikkeling van het aantal en de omvang van de cruciale derde aanbieders van ICT-diensten, dient erop te worden gewezen dat de desbetreffende uitgaven volledig zullen worden gefinancierd door vergoedingen die bij die marktdeelnemers worden geïnd. Daarom zijn er geen gevolgen voor de EU-begrotingskredieten voorzien (behalve voor het extra personeel), aangezien deze kosten volledig door vergoedingen zullen worden gefinancierd.

De financiële gevolgen en de gevolgen voor de begroting van dit voorstel zijn in detail uiteengezet in het bij dit voorstel gevoegde financieel memorandum.

---

20 Ibid.

21 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).

5. OVERIGE ELEMENTEN

- Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage

Het voorstel bevat een algemeen plan voor het monitoren en evalueren van de gevolgen voor de specifieke doelstellingen, op grond waarvan de Commissie ten minste drie jaar na de inwerkingtreding een evaluatie moet verrichten en aan het Europees Parlement en de Raad verslag moet uitbrengen over haar belangrijkste bevindingen.

Die evaluatie zal worden verricht aan de hand van de richtsnoeren van de Commissie voor betere regelgeving.

- Artikelsgewijze toelichting

Het voorstel is opgebouwd rond verschillende belangrijke beleidsterreinen die onderling gerelateerde pijlers zijn waarover overeenstemming bestaat in de Europese en internationale richtsnoeren en beste praktijken ter versterking van de cyber- en operationele veerkracht van de financiële sector.

Toepassingsgebied van de verordening en evenredige toepassing van vereiste maatregelen (artikel 2)

Om te zorgen voor consistentie rond de vereisten inzake ICT-risicobeheer, heeft de verordening betrekking op een reeks financiële entiteiten die op Unieniveau worden gereglementeerd, namelijk kredietinstellingen, betalingsinstellingen, instellingen voor elektronisch geld, beleggingsondernemingen, aanbieders van cryptoactivadiensten, centrale effectenbewaarinstellingen, centrale tegenpartijen, handelsplatformen, transactieregisters, beheerders van alternatieve beleggingsinstellingen en beheermaatschappijen, aanbieders van datarapporteringsdiensten, verzekerings- en herverzekeringsondernemingen, verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen, instellingen voor bedrijfspensioenvoorziening, ratingbureaus, beheerders van cruciale benchmarks en aanbieders van crowdfundingdiensten.

Dit vergemakkelijkt een homogene en coherente toepassing van alle onderdelen van het risicobeheer op ICT-gerelateerde gebieden en waarborgt het gelijke speelveld tussen financiële entiteiten ten aanzien van hun wettelijke verplichtingen inzake ICT-risico's. Tegelijkertijd wordt in de verordening erkend dat er qua omvang, bedrijfsprofiel of blootstelling aan digitaal risico aanzienlijke verschillen tussen financiële entiteiten bestaan. Omdat grotere financiële entiteiten over meer middelen beschikken, zijn bijvoorbeeld alleen financiële entiteiten die niet als micro-onderneming worden aangemerkt, verplicht om complexe governanceregelingen en specifieke beheerfuncties in te stellen, diepgaande evaluaties uit te voeren na grote veranderingen in de infrastructuur van het netwerk en het informatiesysteem, regelmatig risicoanalyses met betrekking tot oude 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. Bovendien zullen alleen financiële entiteiten die voor geavanceerde tests op digitale veerkracht als significant worden beschouwd, verplicht zijn om dreigingsgestuurde penetratietests uit te voeren.

Het toepassingsgebied is weliswaar ruim, maar dekt niet alle entiteiten. Deze verordening heeft met name geen betrekking op systeemexploitanten in de zin van artikel 2, punt p), van

Richtlijn 98/26/EG[22] betreffende het definitieve karakter van de afwikkeling van betalingen en effectentransacties in betalings- en afwikkelingssystemen ("de finaliteitsrichtlijn"), en evenmin op systeemdeelnemers, tenzij die deelnemer zelf een op Unieniveau gereglementeerde financiële entiteit is en als zodanig al onder deze verordening zou vallen (d.w.z. kredietinstelling, beleggingsonderneming, CTP). Bovendien valt het EU-register voor emissierechten dat overeenkomstig Richtlijn 2003/87/EG[23] onder auspiciën van de Europese Commissie wordt beheerd, ook buiten het toepassingsgebied.

Dergelijke uitzonderingen op de finaliteitsrichtlijn houden rekening met de noodzaak van een verdere herziening van juridische en beleidskwesties die gevolgen hebben voor de systeemexploitanten en -deelnemers, en ook met het effect van de kaders die momenteel van toepassing zijn op door centrale banken beheerde betalingssystemen[24]. Aangezien deze kwesties aspecten kunnen omvatten die losstaan van de aangelegenheden die onder deze verordening vallen, zal de Commissie de noodzaak en het effect van een verdere uitbreiding van het toepassingsgebied van deze verordening tot entiteiten en ICT-infrastructuren die er momenteel buiten vallen, blijven beoordelen.

Vereisten in verband met governance (artikel 4)

Deze verordening is bedoeld om de bedrijfsstrategieën van financiële entiteiten en de uitvoering van het ICT-risicobeheer beter op elkaar af te stemmen. Daartoe moet het leidinggevend orgaan een cruciale, actieve rol blijven spelen bij het aansturen van het kader voor ICT-risicobeheer en blijven streven naar de inachtneming van een strikte cyberhygiëne. De volledige verantwoordelijkheid van het leidinggevend orgaan voor het beheer van het ICT-risico van de financiële entiteit zal een overkoepelend beginsel zijn dat verder moet worden vertaald in een reeks specifieke vereisten, zoals de toewijzing van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies, een voortdurende betrokkenheid bij de controle van de monitoring van het ICT-risicobeheer alsook bij het volledige spectrum van goedkeurings- en controleprocessen en een passende toewijzing van ICT-investeringen en opleidingen.

Vereisten inzake ICT-risicobeheer (artikelen 5 tot en met 14)

Digitale operationele veerkracht berust op een reeks belangrijke beginselen en vereisten inzake ICT-risicobeheer, in overeenstemming met het gezamenlijke technische advies van de ETA's. Deze vereisten, die geïnspireerd zijn op relevante internationale, nationale en door de sector vastgestelde normen, richtsnoeren en aanbevelingen, hebben te maken met specifieke functies op het gebied van ICT-risicobeheer (identificatie, bescherming en voorkoming, detectie, respons en herstel, scholing en ontwikkeling en communicatie). Om gelijke tred te houden met een snel evoluerend landschap van cyberdreigingen, zijn financiële entiteiten verplicht om veerkrachtige ICT-systemen en -instrumenten op te zetten en te onderhouden die de impact van ICT-risico's tot een minimum beperken, permanent alle bronnen van ICT-risico's te identificeren, beschermings- en preventiemaatregelen op te zetten, specifiek en

[22] Richtlijn 98/26/EG van het Europees Parlement en de Raad van 19 mei 1998 betreffende het definitieve karakter van de afwikkeling van betalingen en effectentransacties in betalings- en afwikkelingssystemen (PB L 166 van 11.6.1998, blz. 45).

[23] Richtlijn 2003/87/EG van het Europees Parlement en de Raad van 13 oktober 2003 tot vaststelling van een systeem voor de handel in broeikasgasemissierechten binnen de Unie en tot wijziging van Richtlijn 96/61/EG van de Raad (PB L 275 van 25.10.2003, blz. 32).

[24] Met name Verordening van de Europese Centrale Bank (EU) nr. 795/2014 van 3 juli 2014 met betrekking tot oversightvereisten voor systeemrelevante betalingssystemen.

alomvattend beleid inzake bedrijfscontinuïteit en rampen- en herstelplannen op te stellen als integrerend deel van het operationele bedrijfscontinuïteitsbeleid. De laatstgenoemde componenten zijn nodig voor een snel herstel na ICT-gerelateerde incidenten, met name cyberaanvallen, door de schade te beperken en prioriteit te geven aan een veilige hervatting van de activiteiten. De verordening legt zelf geen specifieke normalisatie op, maar bouwt veeleer voort op Europese en internationaal erkende technische normen of beste praktijken van de sector, voor zover deze volledig in overeenstemming zijn met de toezichtinstructies voor het gebruik en de integratie van dergelijke internationale normen. Deze verordening heeft ook betrekking op de integriteit, veiligheid en veerkracht van fysieke infrastructuren en faciliteiten die het gebruik van technologie en de relevante ICT-gerelateerde processen en personen ondersteunen, als onderdeel van de digitale voetafdruk van de activiteiten van een financiële entiteit.

ICT-gerelateerde incidentrapportage (artikelen 15 tot en met 20)

Harmonisatie en stroomlijning van de rapportage van ICT-gerelateerde incidenten wordt bereikt via, in de eerste plaats, een algemene verplichting voor financiële entiteiten om een beheerproces vast te stellen en uit te voeren om ICT-gerelateerde incidenten te monitoren en te registreren, gevolgd door een verplichting om deze te classificeren aan de hand van criteria die in de verordening zijn uiteengezet en door de ETA's verder zijn ontwikkeld door de verplichting om materialiteitsdrempels te specificeren. In de tweede plaats moeten alleen ICT-gerelateerde incidenten die belangrijk worden geacht, aan de bevoegde autoriteiten worden gerapporteerd. De rapportage moet worden verwerkt aan de hand van een gemeenschappelijke template volgens een door de ETA's ontwikkelde geharmoniseerde procedure. Financiële entiteiten moeten eerste, tussentijdse en eindverslagen indienen en hun gebruikers en cliënten informeren wanneer het incident gevolgen heeft of kan hebben voor hun financiële belangen. De bevoegde autoriteiten moeten relevante gegevens over de incidenten doorgeven aan andere instellingen of autoriteiten: aan de ETA's, de ECB en de krachtens Richtlijn (EU) 2016/1148 aangewezen centrale contactpunten.

Om een dialoog tussen financiële entiteiten en bevoegde autoriteiten op gang te brengen die zou helpen de impact tot een minimum te beperken en passende oplossingen te vinden, moet de rapportage van ernstige ICT-gerelateerde incidenten worden aangevuld met feedback en richtsnoeren van toezichthouders.

Tot slot moet de mogelijkheid van centralisatie op Unieniveau van de rapportage van ICT-gerelateerde incidenten verder worden onderzocht in een gezamenlijk verslag van de ETA's, de ECB en Enisa waarin de haalbaarheid wordt beoordeeld van de oprichting van één EU-hub voor de melding van ICT-gerelateerde incidenten door financiële entiteiten.

Tests op digitale operationele veerkracht (artikelen 21 tot en met 24)

De capaciteiten en functies van het kader voor ICT-risicobeheer moeten periodiek worden getest op paraatheid en identificatie van zwakke punten, gebreken of lacunes, alsook op de snelle tenuitvoerlegging van corrigerende maatregelen. Deze verordening maakt een evenredige toepassing van vereisten voor het testen van digitale operationele veerkracht mogelijk, afhankelijk van de omvang en het bedrijfs- en risicoprofiel van financiële entiteiten: hoewel alle entiteiten ICT-instrumenten en -systemen moeten testen, moeten alleen entiteiten die door de bevoegde autoriteiten (op basis van in deze verordening opgenomen en door de ETA's verder ontwikkelde criteria) als significant en cybervolwassen zijn aangemerkt, geavanceerde tests op basis van dreigingsgestuurde penetratietests uitvoeren. Deze verordening voorziet ook in vereisten voor testers en de erkenning van resultaten van dreigingsgestuurde penetratietests in de hele Unie voor financiële entiteiten die in verschillende lidstaten actief zijn.

ICT-risico van derde aanbieders (artikelen 25 tot en met 39)

De verordening is bedoeld om te zorgen voor een gedegen monitoring van het ICT-risico van derde aanbieders. Deze doelstelling zal ten eerste worden bereikt door naleving van op beginselen gebaseerde regels voor de monitoring door financiële entiteiten van het risico met betrekking tot derde aanbieders van ICT-diensten. Ten tweede harmoniseert deze verordening de belangrijkste elementen van de dienst en de relatie met derde aanbieders van ICT-diensten. Deze elementen hebben betrekking op minimumaspecten die cruciaal worden geacht om een volledige monitoring door de financiële entiteit van het ICT-risico van derde aanbieders mogelijk te maken gedurende alle fasen van hun relatie (sluiting, uitvoering, beëindiging van de overeenkomst en postcontractuele fase).

Met name moeten de contracten die op die relatie van toepassing zijn, een volledige beschrijving bevatten van de diensten, een vermelding van de locaties waar de gegevens moeten worden verwerkt, beschrijvingen van het niveau van volledige dienstverlening vergezeld van kwantitatieve en kwalitatieve prestatiedoelen, relevante bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens, en garanties voor toegang, herstel en teruggave in geval van falen van derde aanbieders van ICT-diensten, kennisgevingstermijnen en rapportageverplichtingen van de derde aanbieders van ICT-diensten, het recht van toegang, inspectie en audit door de financiële entiteit of een daartoe aangestelde derde, een duidelijk beëindigingsrecht en specifieke exitstrategieën. Bovendien bevordert de verordening, aangezien sommige van deze contractuele elementen kunnen worden gestandaardiseerd, een vrijwillig gebruik van modelcontractbepalingen die door de Commissie moeten worden ontwikkeld voor het gebruik van cloudcomputingdiensten.

Tot slot beoogt de verordening convergentie te bevorderen inzake de wijze waarop toezicht wordt gehouden op het ICT-risico van derde aanbieders in de financiële sector, door cruciale derde aanbieders van ICT-diensten aan een toezichtkader van de Unie te onderwerpen. Door middel van een nieuw geharmoniseerd wetgevingskader krijgt de ETA die voor elk van deze cruciale derde aanbieders van ICT-diensten als leidende toezichthouder is aangewezen, bevoegdheden, teneinde te garanderen dat aanbieders van technologiediensten die een cruciale rol vervullen voor de werking van de financiële sector, naar behoren worden gemonitord op pan-Europese schaal. Het toezichtkader waarin deze verordening voorziet, bouwt voort op de bestaande institutionele architectuur op het gebied van financiële diensten: zo zorgt het Gemengd Comité van de ETA's voor sectoroverschrijdende coördinatie met betrekking tot alle kwesties in verband met ICT-risico, overeenkomstig zijn taken op het gebied van cyberbeveiliging, ondersteund door het desbetreffende subcomité (het toezichtforum), dat voorbereidende werkzaamheden verricht voor individuele besluiten en collectieve aanbevelingen ten aanzien van cruciale derde aanbieders van ICT-diensten.

Uitwisseling van informatie (artikel 40)

Om ICT-risico's onder de aandacht te brengen, de verspreiding ervan zoveel mogelijk te beperken en de afweercapaciteiten en dreigingsdetectietechnieken van financiële entiteiten te ondersteunen, biedt de verordening aan financiële entiteiten de mogelijkheid regelingen te treffen om onderling informatie en inlichtingen over cyberdreigingen uit te wisselen.

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[25],

Gezien het advies van het Europees Economisch en Sociaal Comité[26],

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, is digitale veerkracht nog niet voldoende in hun operationele kaders 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, het afsluiten van verzekeringen, schadebeheer en backofficeverrichtingen. 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.

[25] [*referentie invoegen*] PB C van , blz. .

[26] [*referentie invoegen*] PB C van , blz. .

(3) Het Europees Comité voor systeemrisico's (ESRB) heeft in een in 2020 uitgebracht verslag over systemisch cyberrisico[27] 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[28] 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 van instrumenten om de veerkracht van hun financiële stelsels op te vijzelen.

(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[29] 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

---

27 Verslag van het ESRB "Systemic Cyber Risk", februari 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 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.

29 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 "FinTech-actieplan: voor een meer concurrerende en innovatieve Europese financiële sector", COM(2018) 109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

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 te verruimen van de financiële toezichthouders die de financiële stabiliteit en de marktintegriteit moeten monitoren en beschermen.

(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.

(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.

(13) Financiële entiteiten moeten 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 overmatig gebruik 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.

(15) Naast de wetgeving inzake financiële diensten is Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[30] 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 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, aangezien dit zou zorgen voor samenhang met de reeds door de lidstaten ingevoerde cyberbeveiligingsstrategieën, en financiële toezichthouders zo kunnen worden gewezen 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 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. 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.

(18) Het is ook belangrijk te zorgen voor consistentie met de richtlijn betreffende Europese kritieke infrastructuur, die momenteel wordt herzien om kritieke infrastructuur beter te beschermen en weerbaarder te maken tegen niet-cybergerelateerde dreigingen, met mogelijke gevolgen voor de financiële sector[31].

---

30 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).

31 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

(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. 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 beheren van het ICT-risico van derde aanbieders. 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 voor financiële entiteiten die micro-ondernemingen zijn in de zin van Aanbeveling 2003/361/EG van de Commissie[32].

(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)[33] 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.

(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 de regeling voor het melden van ICT-gerelateerde incidenten aan te vullen met

---

beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

32 Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van micro-, kleine en middelgrote ondernemingen (PB L 124 van 20.5.2003, blz. 36).

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

voorschriften die momenteel ontbreken in de wetgeving inzake financiële subsectoren, 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 alleen aan hun bevoegde autoriteiten rapporteren. Daarnaast moeten de ETA's de bevoegdheid krijgen elementen van de rapportage van ICT-gerelateerde incidenten verder uit te werken, zoals taxonomie, 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 ongecoördineerde nationale kaders waarin dezelfde kwesties op verschillende manieren worden aangepakt. Dit leidt tot dubbele kosten voor grensoverschrijdende financiële entiteiten en bemoeilijkt de wederzijdse erkenning van resultaten. 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[34], 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 voor financiële entiteiten cruciale derde aanbieders van ICT-diensten voortdurend te kunnen monitoren.

(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.

(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

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

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.

(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[35] 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[36], 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 rekening worden gehouden met aanzienlijke verschillen tussen financiële entiteiten qua omvang, bedrijfsprofiel of blootstelling aan digitaal risico. Als algemeen beginsel geldt dat financiële entiteiten, wanneer zij middelen en capaciteiten vrijmaken voor de uitvoering van het kader voor ICT-risicobeheer, hun ICT-gerelateerde behoeften naar behoren moeten afstemmen op hun omvang en bedrijfsprofiel, terwijl de 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

---

35 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).

36 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).

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 kosten en verliezen als gevolg van ICT-verstoringen en over de resultaten van post-incidentenevaluaties na zware 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[37], 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

[37] 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.

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. 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 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 EU-hub 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 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.

(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 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 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.

(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 de beëindiging van contracten moet worden voorafgegaan door 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, met name wanneer die worden gesloten met in een derde land gevestigde aanbieders van ICT-diensten. 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. De ETA die is aangewezen om toezicht te houden op elke cruciale derde aanbieder van ICT-diensten ("de leidende toezichthouder"), moet 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 moet, wanneer dat risico wordt vastgesteld, voorzien in een dialoog met cruciale derde aanbieders van ICT-diensten[38].

(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

[38] 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.

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 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, zonder dat extra kosten worden aangerekend, of tegen vooraf vastgestelde kosten.

(53) Rechten van toegang, inspectie en audit door de financiële entiteit of een aangewezen derde zijn cruciale instrumenten voor de permanente monitoring door de financiële entiteit van de prestaties van de derde aanbieder van ICT-diensten, evenals de volledige medewerking van laatstgenoemde tijdens inspecties. Evenzo moet de bevoegde autoriteit 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.

(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.

(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 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.

(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 op Eurosysteemniveau ter ondersteuning van de in artikel 127, lid 2, van het Verdrag betreffende de werking van de Europese Unie bedoelde taken, moeten worden vrijgesteld.

(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.

(59) Dit 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, ondersteund door een nieuw subcomité (het toezichtforum), dat voorbereidende werkzaamheden verricht voor individuele besluiten 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 voor elke cruciale derde aanbieder van ICT-diensten een van de ETA's als leidende toezichthouder worden aangewezen.

(62) Leidende toezichthouders moeten de nodige bevoegdheden hebben om onderzoeken, inspecties ter plaatse en elders 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.

Om de systemische dimensie van ICT-risico's in de financiële sector te onderkennen en aan te pakken, is het een voorwaarde dat de leiding over het toezicht aan de ETA's 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 moeten leidende toezichthouders 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 de leidende toezichthouders in acht worden genomen.

(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 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[39] van de Raad zijn opgedragen, en voor overleg met de ETA's.

(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.

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[40]. 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[41] 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.

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.

---

39 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).

40 PB L 123 van 12.5.2016, blz. 1.

41 [*Gelieve volledige verwijzing in te voegen*]

(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 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 omvang en de complexiteit 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;

   – het testen van de digitale operationele veerkracht;

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

   – maatregelen voor een goed 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.

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 van cryptoactivadiensten, emittenten van asset-referenced tokens en emittenten van significante asset-referenced tokens,

(f) centrale effectenbewaarinstellingen,

(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,

(o) instellingen voor bedrijfspensioenvoorziening,

(p) ratingbureaus,

(q) wettelijke auditors en auditkantoren,

(r) beheerders van cruciale benchmarks,

(s) aanbieders van crowdfundingdiensten,

(t) securitisatieregisters;

(u) derde aanbieders van ICT-diensten,

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

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 uit technologisch oogpunt op te bouwen, te waarborgen en te evalueren, door direct of indirect via gebruik van diensten van derde ICT-aanbieders te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die nodig zijn voor de beveiliging van de netwerk- en informatiesystemen waarvan een financiële entiteit gebruikmaakt, en die de permanente verlening van financiële diensten en de kwaliteit ervan ondersteunen;

(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 – met inbegrip van verstoring, capaciteitsoverschrijding, uitval, ontwrichting, belemmering, verkeerd gebruik, verlies of ander soort kwaadwillige of niet-kwaadwillige gebeurtenis – die, indien zij

zich voordoet, de beveiliging van het netwerk- en informatiesysteem, van technologisch geregelde instrumenten of processen, de exploitatie en het procesverloop, of de levering van de diensten in gevaar kan brengen, waarbij de integriteit of beschikbaarheid van gegevens, van de software of enig andere component van ICT-diensten en infrastructuren wordt aangetast of een inbreuk op de vertrouwelijkheid, een beschadiging van fysieke ICT-infrastructuur of andere nadelige effecten worden veroorzaakt;

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

(6) "ICT-gerelateerd incident": een onvoorzien geïdentificeerd voorval in de netwerk- en informatiesystemen, dat al dan niet het gevolg is van kwaadwillige activiteiten, dat de beveiliging in gevaar brengt van netwerk- en informatiesystemen of van de informatie die deze systemen verwerken, opslaan of doorgeven, of nadelige gevolgen heeft voor de beschikbaarheid, vertrouwelijkheid, continuïteit of authenticiteit van de door de financiële entiteit verleende financiële diensten;

(7) "ernstig ICT-gerelateerd incident": een ICT-gerelateerd incident met potentieel grote nadelige gevolgen voor de netwerk- en informatiesystemen die cruciale functies van de financiële entiteit ondersteunen;

(8) "cyberdreiging": cyberdreiging in de zin van artikel 2, punt 8), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad[42];

(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 dreiging 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;

---

[42] 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).

(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 digitale en datadiensten aanbiedt, met inbegrip van aanbieders van cloudcomputingdiensten, software, gegevensanalysediensten, datacentra, 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[43];

(16) “ICT-diensten”: digitale en gegevensdiensten die via de ICT-systemen aan een of meer interne of externe gebruikers worden verleend, met inbegrip van de verstrekking van gegevens, gegevensinvoer, gegevensopslag, gegevensverwerking en rapportagediensten, gegevensmonitoring en op gegevens gebaseerde bedrijfs- en beslissingsondersteunende diensten;

(17) “cruciale of belangrijke functie”: een functie 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, of aan haar financiële prestaties of aan de soliditeit of de continuïteit van haar diensten en activiteiten;

(18) “cruciale derde aanbieder van ICT-diensten”: een derde aanbieder van ICT-diensten die overeenkomstig artikel 29 is aangewezen en onderworpen is aan het toezichtkader bedoeld in de artikelen 30 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, geen bedrijf/aanwezigheid in de Unie heeft opgezet 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, geen bedrijf/aanwezigheid in de Unie heeft opgezet 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 het vermogen van een financiële entiteit, en uiteindelijk van het financiële stelsel van de Unie in zijn geheel, om cruciale 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

[43] 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).

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[44], of artikel 3, lid 1, punt u), van Verordening (EU) 20xx/xx van het Europees Parlement en de Raad[45] [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[46];

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

(25) “betalingsinstelling”: een betalingsinstelling in de zin van artikel 1, lid 1, punt d), 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[47];

(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;

(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;

---

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

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

46 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).

47 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).

(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, punt 3), van Richtlijn (EU) 2016/97;

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

(38) "herverzekeringstussenpersoon": een herverzekeringstussenpersoon in de zin van artikel 2, 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 n), 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 h), 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*];

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

(47) “beheerder van cruciale benchmarks”: een beheerder van cruciale benchmarks in de zin van artikel x, punt x), van Verordening 202x/xx [*OJ: insert reference to Benchmark Regulation*];

(48) “aanbieder van crowdfundingdiensten”: een aanbieder van crowdfundingdiensten in de zin van artikel x, punt x), van Verordening 202x/xx [*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-onderneming": een micro-onderneming in de zin van artikel 2, lid 3, van de bijlage bij Aanbeveling 2003/361/EG.

HOOFDSTUK II

ICT-RISICOBEHEER

AFDELING I

Artikel 4

Governance en organisatie

1. Financiële entiteiten beschikken over interne governance- en controlekaders die een doeltreffend en prudent beheer van alle ICT-risico's waarborgen.

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;

   (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;

   (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 opleiding inzake ICT-risico's en -vaardigheden voor het betrokken 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 inwinnen van informatie over 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 met derde aanbieders van ICT-diensten met betrekking tot het gebruik van deze diensten te monitoren, of wijzen een lid van het hoger leidinggevend personeel aan dat verantwoordelijk is voor het toezicht op de desbetreffende risicoblootstelling en de relevante documentatie.

4. De leden van het leidinggevend orgaan volgen regelmatig specifieke opleidingen teneinde voldoende kennis en vaardigheden te verwerven en te onderhouden om ICT-risico's en de gevolgen daarvan voor de activiteiten van de financiële entiteit te begrijpen en te beoordelen.

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 dat overeenstemt met hun zakelijke behoeften, omvang en complexiteit.

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, zoals vereist door de bevoegde autoriteiten.

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, en zij herzien dit regelmatig.

5. Andere financiële entiteiten dan micro-ondernemingen garanderen een passende scheiding 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.

7. Het in lid 1 bedoelde kader voor ICT-risicobeheer wordt 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 en terdege de aard, de omvang en de complexiteit van de diensten en activiteiten van de financiële entiteiten in aanmerking worden genomen.

9. Het in lid 1 bedoelde kader voor ICT-risicobeheer omvat een strategie voor digitale 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-referentiearchitectuur toe te lichten alsmede eventuele wijzigingen daarin die noodzakelijk zijn om specifieke bedrijfsdoelstellingen te bereiken;

   (e) de verschillende mechanismen te beschrijven die zijn ingesteld om 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) op het niveau van de entiteit een holistische multi-vendorstrategie inzake ICT te bepalen waarin de voornaamste afhankelijkheden ten aanzien van derde aanbieders van ICT-diensten worden aangegeven en de motivering met betrekking tot de mix van aanbestedingen bij derde aanbieders van ICT-diensten nader wordt toegelicht;

   (h) tests te verrichten van de digitale operationele veerkracht;

   (i) een communicatiestrategie uit te stippelen in het geval van ICT-gerelateerde incidenten.

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

Artikel 6

ICT-systemen, -protocollen en -instrumenten

1. Financiële entiteiten gebruiken en onderhouden geactualiseerde ICT-systemen, -protocollen en -instrumenten die aan de volgende voorwaarden voldoen:

   (a) de systemen en instrumenten zijn afgestemd op de aard, de verscheidenheid, de complexiteit en 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 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 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 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 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 ICT-activa en de verbanden en onderlinge afhankelijkheden tussen de verschillende ICT-activa.

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

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, in het bijzonder voor en na de aansluiting van oude en nieuwe 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 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 geavanceerde ICT-technologieën en -processen die:

   (a) de beveiliging van de middelen voor overdracht van informatie waarborgen;

   (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 slecht bestuur of risico's bij de verwerking, met inbegrip van ontoereikende registratie.

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

   (a) zij ontwikkelen en documenteren een beleid inzake informatiebeveiliging waarin regels worden vastgesteld om de vertrouwelijkheid, integriteit en beschikbaarheid van hun eigen ICT-middelen, -gegevens en -informatieactiva en die van hun klanten te beschermen;

   (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, met inbegrip van de toepassing van geautomatiseerde mechanismen om in geval van cyberaanvallen de getroffen informatieactiva te isoleren;

   (c) zij voeren een beleid 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, en voeren met dat doel een reeks beleidslijnen, procedures en controles in om bevoorrechte toegang en een degelijk beheer daarvan te waarborgen;

   (d) zij voeren beleidslijnen en protocollen in voor strenge authenticatiemechanismen die gebaseerd zijn op relevante normen en specifieke controlesystemen om toegang tot cryptografische sleutels te

voorkomen, waarbij gegevens worden versleuteld uitgaande van de resultaten van goedgekeurde processen van gegevensclassificatie en risicobeoordeling;

(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 onmiddellijk 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 alle potentiële zwakke fysieke punten (“single points of failure”) te identificeren.

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

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

3. Financiële entiteiten zetten, rekening houdend met hun omvang, bedrijfs- en risicoprofiel, 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.

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 specifiek en alomvattend beleid inzake ICT-bedrijfscontinuïteit als integrerend onderdeel van het beleid inzake operationele bedrijfscontinuïteit van de financiële entiteit.

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:

   (a) alle ICT-gerelateerde incidenten te registreren;

   (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:

   (g) ten minste jaarlijks en na substantiële wijzigingen in de ICT-systemen het beleid inzake ICT-bedrijfscontinuïteit en het ICT-noodherstelplan;

   (h) 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, backups 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 die 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 bepaalt.

7. Financiële entiteiten houden registers bij van hun 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 kosten en verliezen als gevolg van ICT-verstoringen en ICT-gerelateerde incidenten.

Artikel 11

Backupbeleid 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 backupbeleid 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. Backupsystemen starten 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 backupgegevens herstellen met behulp van eigen systemen, maken zij gebruik van ICT-systemen met een andere werkconfiguratie dan de hoofdconfiguratie, die niet rechtstreeks aan deze laatste is gekoppeld en die tegen ongeoorloofde toegang of beschadiging van ICT is 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 houden ICT-capaciteiten in reserve met middelen, capaciteiten en functionaliteiten die toereikend en adequaat zijn om te voorzien in de zakelijke behoeften.

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) onmiddellijk toegankelijk voor het personeel van de financiële entiteit om de continuïteit van cruciale diensten 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 het potentiële algemene effect op de marktefficiëntie. Deze tijdsdoelstellingen zorgen ervoor dat de overeengekomen niveaus in extreme scenario's worden gehaald.

7. Bij herstel van een ICT-gerelateerd incident verrichten financiële entiteiten meerdere controles, waaronder afstemmingen, om ervoor te zorgen dat het hoogste niveau van gegevensintegriteit wordt bereikt. 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 die overeenstemmen met hun omvang, bedrijfs- en risicoprofiel, 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 ICT-gerelateerde post-incidentevaluaties 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 delen andere financiële entiteiten dan micro-ondernemingen deze mee aan de bevoegde autoriteiten.

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 is 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 worden 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, 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. Deze zijn van toepassing op alle werknemers en op het hoger leidinggevend personeel.

Financiële entiteiten 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 ICT-gerelateerde incidenten of ernstige kwetsbaarheden op verantwoordelijke wijze bekend te maken aan cliënten en tegenpartijen en, in voorkomend geval, aan het publiek.

2. Als onderdeel van het kader voor ICT-risicobeheer 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 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 te waarborgen;

(b) te bepalen hoe in de beleidslijnen, procedures en instrumenten met betrekking tot ICT-beveiliging als bedoeld in artikel 8, lid 2, vanaf het begin (beveiliging door ontwerp) veiligheidscontroles in de systemen worden opgenomen, aanpassingen aan het veranderende landschap van veiligheidsdreigingen mogelijk worden gemaakt en in het gebruik van technologie voor verdediging in de diepte wordt voorzien;

(c) de passende technieken, methodes en protocollen als bedoeld in artikel 8, lid 4, punt b), nader te specificeren;

(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.

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 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 weggenomen om 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 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 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, en de vraag of het ICT-gerelateerde incident reputatieschade heeft veroorzaakt;

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

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

   (d) de gegevensverliezen ten gevolge van het ICT-gerelateerde incident, 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 na overleg 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 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 leggen die gemeenschappelijke ontwerpen van technische reguleringsnormen uiterlijk op [*PO: insert date 1 year 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.

2. Wanneer een ernstig ICT-gerelateerd incident gevolgen heeft of kan hebben voor de financiële belangen van gebruikers van diensten en van cliënten, stellen financiële entiteiten hun gebruikers van diensten en hun cliënten onverwijld in kennis van het ernstige ICT-gerelateerde incident en melden zij hun zo spoedig mogelijk alle maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk incident te beperken.

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

   (a) een eerste kennisgeving, onverwijld maar uiterlijk aan het einde van de werkdag, of, in het geval van een ernstig ICT-gerelateerd incident dat zich later dan twee uur voor het einde van de werkdag heeft voorgedaan, uiterlijk vier uur na de aanvang van de volgende werkdag, of, indien er geen meldingskanalen beschikbaar zijn, zodra deze beschikbaar zijn;

   (b) een tussentijds verslag, uiterlijk een week 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 verzending van het eerste verslag.

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.

5. Na ontvangst van het in lid 1 bedoelde verslag verstrekt de bevoegde autoriteit onverwijld nadere bijzonderheden over het 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 centraal contactpunt aangewezen krachtens artikel 8 van Richtlijn (EU) 2016/1148.

6. De EBA, de ESMA of de Eiopa en de ECB 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;

   (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 lid 1, punt a), en de gemeenschappelijke ontwerpen van technische uitvoeringsnormen bedoeld in lid 1, punt b), uiterlijk op xx 202x [*PO: insert date 1 year 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 1, punt a), 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 lid 1, punt b), 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.

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:

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

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

(c) elementen van operationeel beheer;

(d) de voorwaarden voor het lidmaatschap;

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

(f) een voorlopige beoordeling van de financiële kosten voor de oprichting van het operationele platform ter ondersteuning van de 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.

2. De ETA's brengen jaarlijks via het Gemengd Comité een geanonimiseerd en geaggregeerd verslag uit over de meldingen van 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 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.

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 financiële entiteiten, rekening houdend met hun omvang, bedrijfs- en risicoprofiel, 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.

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 te verhelpen, en stellen interne valideringsmethoden vast om na te gaan of alle vastgestelde zwakheden, gebreken of lacunes volledig worden aangepakt.

6. Financiële entiteiten testen ten minste eenmaal per jaar 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 waaronder 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.

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 lid 4 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 functies en diensten van een financiële entiteit en worden uitgevoerd op systemen die prestaties in het reële leven verrichten ter ondersteuning van deze functies. De precieze omvang van dreigingsgestuurde penetratietests, op basis van de beoordeling van cruciale functies en diensten, wordt door financiële entiteiten vastgesteld en wordt door de bevoegde autoriteiten gevalideerd.

Voor de toepassing van de eerste alinea bepalen financiële entiteiten alle relevante onderliggende ICT-processen, -systemen en technologieën ter ondersteuning van

cruciale functies en diensten, met inbegrip van uitbestede of met derde aanbieders van ICT-diensten contractueel overeengekomen functies en diensten.

Wanneer 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.

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

Na afloop van de test, nadat overeenstemming is bereikt over verslagen en correctieplannen, verstrekken de financiële entiteit en de externe testers aan de bevoegde autoriteit de documenten waarmee wordt bevestigd dat de dreigingsgestuurde penetratietests in overeenstemming met de vereisten zijn verricht. De bevoegde autoriteiten valideren de documenten en geven een attest af.

3. Financiële entiteiten stellen overeenkomstig artikel 24 testers aan om dreigingsgestuurde penetratietests te verrichten.

De bevoegde autoriteiten bepalen welke financiële entiteiten op zodanige wijze dreigingsgestuurde penetratietests verrichten dat deze evenredig zijn met de omvang, de schaal, de activiteit en het algemene risicoprofiel van de financiële entiteit, 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.

4. De EBA, de ESMA en de Eiopa ontwikkelen, na raadpleging van de ECB en rekening houdend met de desbetreffende kaders in de Unie die van toepassing zijn op op inlichtingen gebaseerde penetratietests, ontwerpen van technische reguleringsnormen tot nadere bepaling van:

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

(b) de voorschriften met betrekking tot:

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

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

(c) 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 in het geval van financiële entiteiten die in meer dan een lidstaat actief zijn, teneinde een passend niveau van betrokkenheid van toezichthouders en een flexibele 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 2 months before 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 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 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;

   (d) in het geval van externe testers, 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 bedrijfsrisio's van de financiële entiteit;

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

2. Financiële entiteiten zorgen ervoor dat de overeenkomsten met externe testers 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 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.

3. Als onderdeel van hun kader voor ICT-risicobeheer stellen financiële entiteiten een strategie inzake ICT-risico van derde aanbieders vast en herzien zij deze regelmatig, rekening houdend met de in artikel 5, lid 9, punt g), bedoelde multi-vendorstrategie. 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.

   De in de eerste alinea bedoelde contractuele regelingen worden naar behoren gedocumenteerd, met een onderscheid tussen die welke van toepassing zijn op cruciale of belangrijke functies en die welke daarop niet van toepassing zijn.

Financiële entiteiten rapporteren ten minste jaarlijks aan de bevoegde autoriteiten over het aantal nieuwe regelingen inzake het gebruik van ICT-diensten, 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 de meest recente normen op het gebied van informatiebeveiliging.

7. Bij het uitoefenen van toegangs-, inspectie- en auditrechten ten aanzien van de derde aanbieder van ICT-diensten bepalen financiële entiteiten op basis van een risicogebaseerde benadering vooraf de frequentie van de audits en inspecties 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 hoog niveau van 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 ten minste in de volgende omstandigheden worden beëindigd:

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

   (b) in omstandigheden die in de loop van de monitoring van het ICT-risico van derde aanbieders worden vastgesteld, waarvan wordt aangenomen dat deze wijzigingen kunnen brengen in de uitvoering van de functies waarin de

contractuele 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 in zijn algemeen beheer van het ICT-risico 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 niet langer doeltreffend toezicht op de financiële entiteit kan uitoefenen.

9. Financiële entiteiten voeren exitstrategieën in om rekening te houden 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.

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 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 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 onderaanbestedingsregelingen

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 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; dan wel

   (b) zij beschikken over meerdere contractuele regelingen met betrekking tot de verlening van ICT-diensten 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 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, met name in het geval van een in een derde land gevestigde ICT-subcontractant.

   Wanneer contractuele regelingen inzake het gebruik van ICT-diensten met een in een derde land gevestigde derde aanbieder van ICT-diensten worden gesloten, schenken financiële entiteiten ten minste aandacht aan de volgende factoren:

   (a) de naleving van gegevensbescherming;

   (b) de doeltreffende handhaving van de wet;

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

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

Financiële entiteiten beoordelen of en hoe potentieel lange of complexe uitbestedingsketens van invloed kunnen zijn op hun vermogen om de contractueel overeengekomen functies volledig te monitoren en op het vermogen van de bevoegde autoriteit om in dat verband doeltreffend toezicht uit te oefenen op de financiële entiteit.

Artikel 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 opgenomen in één schriftelijk document dat voor de partijen beschikbaar is op papier of in een downloadbaar en toegankelijk formaat.

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

   (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 waar de contractueel overeengekomen of uitbestede 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 in kennis te stellen indien hij voornemens is van locatie te veranderen;

   (c) 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 of stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten;

   (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) 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;

(f) de verplichting van de derde aanbieder van ICT-diensten om in geval van een 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 op passende wijze kan zorgen voor een veilige dienstverlening in overeenstemming met haar regelgevingskader;

(h) 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 kopieën te maken van relevante documenten, 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 verbintenis om tijdens de door de financiële entiteit ter plaatse uitgevoerde inspecties volledig mee te werken, alsmede bijzonderheden over het toepassingsgebied, het verloop en de frequentie van audits op afstand;

(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;

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

(a) 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;

(b) 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.

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.

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).

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 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. De ETA's zorgen via het Gemengd Comité en op aanbeveling van het overeenkomstig artikel 29, lid 1, opgerichte toezichtforum 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.

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

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

ii) moeilijkheden 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.

3. De Commissie is bevoegd overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen ter aanvulling 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. De ETA's stellen via het Gemengd Comité een lijst op van aanbieders van cruciale derde aanbieders van ICT-diensten op het niveau van de Unie, publiceren deze en actualiseren deze jaarlijks.

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 toezichtforum. Het toezichtforum 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. 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.

9. Financiële entiteiten maken geen gebruik van een in een derde land gevestigde derde aanbieder van ICT-diensten die overeenkomstig lid 1, punt a), als cruciaal zou worden aangewezen indien hij in de Unie was gevestigd.

Artikel 29

Structuur van het toezichtkader

1. Het Gemengd Comité richt overeenkomstig artikel 57 van Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 het toezichtforum op als subcomité ter ondersteuning van de werkzaamheden van het Gemengd Comité en de leidende toezichthouder als bedoeld in artikel 28, lid 1, punt b), op het gebied van ICT-risico van derde aanbieder in alle financiële sectoren. Het toezichtforum stelt de ontwerpen van gemeenschappelijke standpunten en gemeenschappelijke handelingen van het Gemengd Comité op dat gebied op.

   Het toezichtforum 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 toezichtforum 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.

3. Het toezichtforum 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.

4. Het toezichtforum is samengesteld uit de voorzitters van de ETA's en één vertegenwoordiger op hoog niveau van het huidige personeel van de desbetreffende bevoegde autoriteit van elke lidstaat. De uitvoerend directeur van elke ETA en één vertegenwoordiger van de Europese Commissie, het ESRB, de ECB en Enisa nemen aan het toezichtforum deel als waarnemer.

5. 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 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 de ETA's en nadere details over de uitwisseling van informatie die de bevoegde autoriteiten nodig hebben ten behoeve van de follow-up van aanbevelingen van leidende toezichthouders aan cruciale derde aanbieders van ICT-diensten in overeenstemming met artikel 31, lid 1, punt d).

6. 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.

7. De ETA's dienen, via het Gemengd Comité en op basis van de voorbereidende werkzaamheden van het toezichtforum, 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 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.

2. De in lid 1 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 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 bedoelde beoordeling stelt de leidende toezichthouder een duidelijk, gedetailleerd en met redenen omkleed individueel toezichtplan op voor elke cruciale derde aanbieder van ICT-diensten. Dat plan wordt jaarlijks aan de cruciale derde aanbieder van ICT-diensten meegedeeld.

4. Zodra de in lid 3 bedoelde jaarlijkse toezichtplannen zijn overeengekomen 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 de leidende toezichthouder.

Artikel 31

Bevoegdheden van de leidende toezichthouder

1. Voor de uitvoering van de in deze afdeling omschreven taken beschikt de leidende toezichthouder over de bevoegdheid om:

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

   (b) algemene onderzoeken en inspecties 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 punt d) bedoelde aanbevelingen;

   (d) 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 de leidende toezichthouder relevant acht om de ICT-beveiliging van diensten voor financiële entiteiten te waarborgen;

      ii) het gebruik van voorwaarden, met inbegrip van de technische uitvoering ervan, voor het verlenen van ICT-diensten aan financiële entiteiten door derde aanbieders, die de toezichthouder 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 de leidende toezichthouder 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;

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

2. De leidende toezichthouder overlegt met het toezichtforum vooraleer hij de in lid 1 bedoelde bevoegdheden uitoefent.

3. Cruciale derde aanbieders van ICT-diensten werken te goeder trouw samen met de leidende toezichthouder en ondersteunen hem bij de uitvoering van zijn taken.

4. De leidende toezichthouder kan een dwangsom opleggen om de cruciale derde aanbieder van ICT-diensten ertoe te dwingen lid 1, punten a), b) en c), na te komen.

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 1 % van de wereldwijde gemiddelde dagomzet van de cruciale derde aanbieder van ICT-diensten in het voorafgaande boekjaar.

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.

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 informatieverstrekking gelast, neemt hij het volgende in acht:

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

(b) hij geeft het doel van het besluit aan;

(c) hij vermeldt welke informatie wordt verlangd;

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

(e) hij vermeldt welke dwangsom overeenkomstig artikel 31, lid 4, wordt opgelegd indien de gevraagde informatie niet volledig wordt overgelegd;

(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 34, lid 1, bedoelde onderzoeksteam, bij derde aanbieders van ICT-diensten de nodige onderzoeken verrichten.

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) voor echt gewaarmerkte kopieën of uittreksels te maken of te verkrijgen van deze registers, gegevens, procedures en ander materiaal;

(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.

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 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 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 de leidende toezichthouder, na raadpleging van het toezichtforum, 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 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 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 de leidende toezichthouder 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 de leidende toezichthouder overeenkomstig artikel 31, lid 1, punt d), delen cruciale derde aanbieders van ICT-diensten deze toezichthouder mee of zij voornemens zijn die aanbevelingen te volgen. De leidende toezichthouder deelt deze informatie onmiddellijk mee aan de bevoegde autoriteiten.

2. De bevoegde autoriteiten monitoren of de financiële entiteiten rekening houden met de risico's vastgesteld in de aanbevelingen die de leidende toezichthouder overeenkomstig artikel 31, lid 1, punt d), aan cruciale derde aanbieders van ICT-diensten heeft gedaan.

3. De bevoegde autoriteiten kunnen financiële entiteiten overeenkomstig artikel 44 ertoe verplichten het gebruik of de uitrol van een door de cruciale derde aanbieder van ICT-diensten geleverde dienst geheel of gedeeltelijk op te schorten totdat de risico's zijn verholpen die in de aanbevelingen aan de cruciale derde aanbieder van ICT-diensten zijn vastgesteld. Wanneer nodig kunnen zij financiële entiteiten ertoe verplichten de desbetreffende contractuele regelingen met de cruciale derde aanbieders van ICT-diensten geheel of gedeeltelijk te beëindigen.

4. Bij het vaststellen van de in lid 3 bedoelde besluiten kunnen de bevoegde autoriteiten rekening houden 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.

5. De bevoegde autoriteiten informeren de leidende toezichthouders regelmatig over de aanpak en de maatregelen die zij in het kader van hun toezichttaken ten aanzien van financiële entiteiten hebben gehanteerd, alsmede over de contractuele maatregelen die deze laatste hebben genomen wanneer cruciale derde aanbieders van ICT-diensten geheel of gedeeltelijk niet zijn ingegaan op de aanbevelingen van de leidende toezichthouders.

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 administratieve kosten en staat in verhouding tot zijn omzet.

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 kunnen onderling informatie en inlichtingen over cyberdreiging uitwisselen, 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 te versterken, met name via bewustmaking met betrekking tot cyberdreigingen, beperking of belemmering van de mogelijkheid tot verdere verspreiding van cyberdreigingen, ondersteuning van het gamma aan defensieve capaciteiten van financiële entiteiten, dreigingsdetectietechnieken, risicobeperkende strategieën of respons- en herstelfasen;

   (b) plaatsvindt binnen vertrouwensgemeenschappen van financiële entiteiten;

   (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[48] en de richtsnoeren inzake mededingingsbeleid[49].

[48] 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).

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.

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 Verordening (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 van cryptoactiva, emittenten 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, 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;

---

[49] 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).

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

(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/EG;

(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 xx/202x;*

(r) voor aanbieders van crowdfundingdiensten, de bevoegde autoriteit aangewezen overeenkomstig *artikel x van Verordening xx/202x*;

(s) voor securitisatieregisters, de bevoegde autoriteit aangewezen overeenkomstig artikel 10 en artikel 14, lid 1, van Verordening (EU) nr. 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, kunnen de ETA's en de bevoegde autoriteiten verzoeken om te worden uitgenodigd voor de werkzaamheden van de samenwerkingsgroep.

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.

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 en het ESRB 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 daarmee verband houdende dreiging 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 en de ECB 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 de bevoegde autoriteit strijdig acht 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 sanctie

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 1 year 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 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].

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 twee 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. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee 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, met betrekking tot de criteria voor de aanwijzing van cruciale derde aanbieders van ICT-diensten in artikel 28, lid 2.

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].".

(4) In lid 6 wordt de eerste alinea vervangen door:

"Een CSD is belast met het identificeren, monitoren en beheersen van de risico's die belangrijke deelnemers aan het effectenafwikkelingssysteem dat zij exploiteert alsook dienstverrichters en aanbieders van hulpprogramma's en andere CSD's of andere marktinfrastructuren voor haar bedrijfsactiviteiten kunnen inhouden. Zij verstrekt desgevraagd de bevoegde en de relevante autoriteiten informatie over eventuele geïdentificeerde risico's. Zij stelt de bevoegde autoriteit en de relevante autoriteiten ook onverwijld in kennis van andere operationele incidenten ten gevolge van deze risico's dan die welke betrekking hebben op ICT-risico's.".

(5) In lid 7 wordt de eerste alinea vervangen door:

"De ESMA ontwikkelt, in nauwe samenwerking met de leden van het ESCB, ontwerpen van technische reguleringsnormen tot nadere bepaling van de in de leden 1 tot en met 6 bedoelde operationele risico's die geen ICT-risico's zijn, en de methoden om die risico's te testen, aan te pakken of te beperken, met inbegrip van het bedrijfscontinuïteitsbeleid en de noodherstelplannen bedoeld in de leden 3 en 4 en de methoden om die te beoordelen.".

Artikel 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) “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 - 12 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.

Gedaan te Brussel,

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

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en)

1.3. Aard van het voorstel/initiatief

1.4. Doelstelling(en)

1.5. Motivering van het voorstel/initiatief

1.6. Duur en financiële gevolgen van het voorstel/initiatief

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesyste(e)m(en)

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarige financiële kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

3.2.2. Geraamde gevolgen voor de kredieten

3.2.3. Geraamde gevolgen voor personele middelen

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

Bijlage

Algemene aannames

Toezichtbevoegdheden

FINANCIEEL MEMORANDUM "AGENTSCHAPPEN"

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad inzake de digitale operationele veerkracht van de financiële sector.

1.2. Betrokken beleidsterrein(en)

Beleidsterrein: Financiële stabiliteit, financiële diensten en kapitaalmarktenunie

Activiteit: Digitale operationele veerkracht

1.3. Het voorstel betreft

☑ **een nieuwe actie**

☐ **een nieuwe actie na een proefproject / voorbereidende actie**[50]

☐ **de verlenging van een bestaande actie**

☐ **een samenvoegen van één of meer acties tot een andere / een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

De algemene doelstelling van het initiatief is een versterking van de digitale operationele veerkracht van de entiteiten van de financiële sector van de EU door de bestaande regels te stroomlijnen en te verbeteren en door nieuwe vereisten in te voeren wanneer er lacunes zijn. Daardoor zou ook de digitale dimensie van het gemeenschappelijk rulebook worden versterkt.

De overkoepelende doelstelling kan worden gestructureerd in drie algemene doelstellingen: (1) een vermindering van het risico op verstoring en instabiliteit van de financiële wereld, (2) een vermindering van de administratieve last en een verhoging van de doeltreffendheid van het toezicht, en (3) meer bescherming voor consumenten en beleggers.

1.4.2. Specifieke doelstelling(en)

De specifieke doelstellingen van het voorstel zijn:

de risico's in informatie- en communicatietechnologieën (ICT) grondiger aanpakken en het algemene niveau van digitale veerkracht van de financiële sector versterken;

de rapportage op het gebied van ICT-gerelateerde incidenten stroomlijnen en overlappende rapportagevereisten aanpakken;

de financiële toezichthouders in staat stellen toegang te verkrijgen tot informatie over ICT-gerelateerde incidenten;

[50] In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

ervoor zorgen dat onder dit voorstel vallende financiële entiteiten de doeltreffendheid van hun maatregelen op het gebied van preventie en veerkracht evalueren en ICT-gerelateerde kwetsbaarheden identificeren;

de versnippering van de interne markt verminderen en grensoverschrijdende aanvaarding van testresultaten mogelijk maken;

de contractuele waarborgen voor financiële entiteiten bij het gebruik van ICT-diensten versterken, onder meer voor uitbestedingsregels die het toezicht op derde aanbieders van ICT-diensten (“third-party providers”, “ICT-TPP’s”) regelen;

het toezicht op de activiteiten van cruciale ICT-TPP’s mogelijk maken;

de uitwisseling van informatie over bedreigingen in de financiële sector stimuleren.

1.4.3. Verwacht(e) resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen.

Met een wettelijk instrument inzake digitale operationele veerkracht voor de financiële sector wordt een algemeen kader verzekerd dat alle aspecten op het gebied van digitale operationele veerkracht zou dekken en de algemene operationele veerkracht van de financiële sector op doeltreffende wijze zou verbeteren. Het zou de duidelijkheid en de samenhang binnen het gemeenschappelijk rulebook verzekeren.

Het zou ook de interactie met de NIS-richtlijn en de herziening daarvan duidelijker stellen en meer samenhang daarin brengen. Het zou financiële entiteiten duidelijkheid verschaffen over de verschillende regels inzake digitale operationele veerkracht waaraan zij moeten voldoen, met name voor de financiële entiteiten die meerdere vergunningen hebben en werkzaam zijn op verschillende markten binnen de EU.

1.4.4. Prestatie-indicatoren

Vermeld de indicatoren voor de monitoring van de voortgang en de beoordeling van de resultaten

Mogelijke indicatoren:

Aantal ICT-gerelateerde incidenten in de financiële sector van de EU en de impact daarvan

Aantal ernstige ICT-gerelateerde incidenten die bij prudentiële toezichthouders zijn gemeld

Aantal financiële entiteiten die de verplichting opgelegd krijgen dreigingsgestuurde penetratietests (“threat-led penetration tests”, “TLPT”) te verrichten

Aantal financiële entiteiten die standaardcontractbepalingen gebruiken om contractuele overeenkomsten aan te gaan met ICT-TPP’s

Aantal cruciale ICT-TPP’s waarop toezicht wordt uitgeoefend door de ETA’s/prudentiële toezichthouders

Aantal financiële entiteiten die deelnemen aan oplossingen voor het uitwisselen van inlichtingen inzake dreigingen

Aantal autoriteiten die verslagen ontvangen over hetzelfde ICT-gerelateerde incident

Aantal grensoverschrijdende TLPT’s

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

De financiële sector is in grote mate afhankelijk van informatie- en communicatietechnologieën (ICT). Ondanks de aanzienlijke vooruitgang die geboekt is via gerichte nationale en Europese beleids- en wetgevingsinitiatieven, blijven ICT-risico’s een uitdaging vormen voor de operationele veerkracht, de prestaties en de stabiliteit van het financiële stelsel van de Unie. De hervorming die op de financiële crisis van 2008 volgde, heeft in de eerste plaats de financiële veerkracht van de financiële sector van de EU versterkt en had als doel het concurrentievermogen en de stabiliteit van de EU te waarborgen uit economisch, prudentieel en marktgedragsoogpunt. Hoewel ICT-beveiliging en algemene digitale operationele veerkracht deel uitmaken van het operationele risico, hebben zij na de crisis in de regelgevingsagenda minder aandacht gekregen en zijn ze alleen op sommige gebieden van het beleid en de regelgeving inzake financiële markten van de Unie ontwikkeld,

of alleen in enkele lidstaten. Dit geeft aanleiding tot de volgende uitdagingen die door middel van het voorstel moeten worden aangepakt:

Het rechtskader van de EU voor ICT-risico's en operationele veerkracht in de hele financiële sector is versnipperd en niet volledig consistent.

Het gebrek aan consistente rapportagevereisten van ICT-gerelateerde incidenten brengt mee dat toezichthouders een onvolledig overzicht hebben van de aard, de frequentie, de significantie en de impact van incidenten.

Sommige financiële entiteiten worden geconfronteerd met complexe, overlappende en potentieel inconsistente rapportagevereisten voor hetzelfde ICT-incident.

Door ontoereikende informatie-uitwisseling en samenwerking op het gebied van inlichtingen over cyberdreigingen op strategisch, tactisch en operationeel niveau is het voor individuele financiële entiteiten onmogelijk om cyberdreigingen adequaat te beoordelen en te monitoren, en om het verweer en de respons op passende wijze te verzekeren.

In een aantal financiële subsectoren kunnen er meerdere en ongecoördineerde kaders zijn voor het testen van de penetratie en de veerkracht, in combinatie met het uitblijven van grensoverschrijdende erkenning van de resultaten, en in andere subsectoren ontbreken dan weer dergelijke testkaders.

Door het gebrek aan inzicht bij de uitoefening van het toezicht op de activiteiten van financiële entiteiten waar ICT-TPP's diensten aanbieden, zijn financiële entiteiten individueel en het financiële stelsel in zijn geheel blootgesteld aan operationele risico's.

Financiële toezichthouders beschikken niet over een toereikend mandaat of over instrumenten om de concentratie- en systeemrisico's te monitoren en te beheren die voortvloeien uit het feit dat de financiële entiteiten afhankelijk zijn van derde ICT-aanbieders.

1.5.2. Toegevoegde waarde van de deelname van de Unie (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de deelname van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaat zou zijn gecreëerd.

Redenen voor maatregelen op Europees niveau (ex ante):

Digitale operationele veerkracht is een kwestie van gemeenschappelijk belang voor de financiële markten van de EU. Maatregelen op EU-niveau zouden meer voordelen en meer waarde opleveren dan afzonderlijke maatregelen op nationaal niveau. Zonder deze operationele bepalingen over ICT-risico's zou het gemeenschappelijk rulebook wel de instrumenten bieden om alle andere risico's op Europees niveau aan te pakken, maar zouden de aspecten die te maken hebben met digitale operationele veerkracht, uitgesloten blijven of alleen aangepakt worden met versnipperde en ongecoördineerde initiatieven op nationaal niveau. Het voorstel zou juridische duidelijkheid verschaffen over de vraag of en hoe regelingen inzake digitale operationele veerkracht worden toegepast, vooral op grensoverschrijdende financiële entiteiten. Het zou ook komaf maken met de behoefte die lidstaten voelen om afzonderlijk verbeteringen aan te brengen in regels, normen en verwachtingen met betrekking tot operationele veerkracht en cyberbeveiliging, als respons op de huidige beperkte reikwijdte van de EU-regels en de algemene aard van de NIS-richtlijn.

Verwachte gegenereerde toegevoegde waarde van de Unie (ex post):

Het optreden van de Unie zou de doeltreffendheid van het beleid aanzienlijk vergroten en tegelijkertijd de complexiteit verminderen en de financiële en administratieve lasten voor alle financiële entiteiten verlichten. Het zou een onderdeel van de economie harmoniseren dat sterk geïnterconnecteerd en geïntegreerd is en dat reeds profiteert van één geheel van regels en toezicht. Wat de rapportage van ICT-gerelateerde incidenten betreft, zou het voorstel de lasten van de rapportage – en de daaraan verbonden kosten – verminderen voor hetzelfde ICT-gerelateerde incident dat aan verschillende EU- en/of nationale autoriteiten wordt gemeld. Het zal ook de wederzijdse erkenning/aanvaarding vergemakkelijken van de testresultaten van grensoverschrijdend opererende entiteiten die in verschillende lidstaten aan uiteenlopende testkaders onderworpen zijn.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

Nieuw initiatief

1.5.4. Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten

De doelstelling van dit voorstel is in overeenstemming met een aantal andere EU-beleidsmaatregelen en lopende initiatieven, met name de richtlijn netwerk- en informatiebeveiliging (NIS) en de richtlijn betreffende Europese kritieke infrastructuur (ECI). Het initiatief zou de voordelen van het horizontale kader voor cyberbeveiliging bewaren door de drie financiële subsectoren binnen het toepassingsgebied van de NIS-richtlijn te houden. Door verbonden te blijven met het NIS-ecosysteem zouden financiële toezichthouders in staat zijn relevante informatie uit te wisselen met de NIS-autoriteiten en deel te nemen aan de NIS-samenwerkingsgroep. Het voorstel zou geen gevolgen hebben voor de NIS-richtlijn maar daar veeleer op voortbouwen en mogelijke overlappingen aanpakken via de vrijstelling van een lex specialis. De interactie tussen de verordening financiële diensten en de NIS-richtlijn zou nog steeds onder een lex-specialisclausule vallen, waardoor financiële entiteiten worden vrijgesteld van de materiële vereisten van de NIS-richtlijn en overlappingen tussen de twee handelingen worden vermeden. Daarnaast is het voorstel consistent met de richtlijn betreffende Europese kritieke infrastructuur, die momenteel wordt herzien om kritieke infrastructuur beter te beschermen en weerbaarder te maken tegen niet-cybergerelateerde dreigingen.

Dit voorstel zou geen gevolgen hebben voor het meerjarig financieel kader (MFK). In de eerste plaats zal het toezichtkader voor cruciale derde aanbieders van ICT-diensten volledig worden gefinancierd door vergoedingen die van deze aanbieders worden gevraagd; in de tweede plaats zullen de bijkomende regelgevingstaken met betrekking tot digitale operationele veerkracht waarmee de ETA's worden belast, worden verzekerd door interne herschikking van het bestaande personeel.

Dit zal aanleiding geven tot een voorstel om het gemachtigde personeel van het agentschap uit te breiden tijdens de komende jaarlijkse begrotingsprocedure. Het agentschap zal blijven streven naar maximale synergie en efficiëntiewinst (onder meer via IT-systemen) en zal nauwlettend toezien op de extra werklast ten gevolge van dit voorstel, die tot uiting zou komen in het aantal geautoriseerde personeelsleden dat door het agentschap in de jaarlijkse begrotingsprocedure wordt gevraagd.

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

Er zijn verschillende financieringsmogelijkheden overwogen:

In de eerste plaats konden de extra kosten via het gebruikelijke financieringsmechanisme van de ETA's worden gefinancierd. Dit zou echter leiden tot een aanzienlijke verhoging van de EU-bijdrage aan de financiële middelen van de ETA's.

Deze optie wordt gekozen voor de kosten die verband houden met de uit dit voorstel voortvloeiende regelgevingstaken. De ETA's zal immers worden gevraagd het bestaande personeel te herschikken om een aantal technische normen te ontwikkelen. De extra kosten ten gevolge van het toezicht op cruciale derde aanbieders konden echter niet worden gedekt via een herschikking van middelen binnen de ETA's, die naast de taken waarin dit voorstel en andere onderdelen van de Uniewetgeving voorzien, ook andere taken hebben. Voorts vereisen toezichttaken in verband met digitale operationele veerkracht specifieke technische kennis en deskundigheid. Aangezien het huidige niveau van deze middelen bij de ETA's ontoereikend is, zijn extra middelen nodig.

Ten slotte zullen volgens het voorstel vergoedingen worden gevraagd van de onder toezicht staande cruciale ICT-TPP's. Het is de bedoeling om daarmee alle extra middelen te financieren die de ETA's nodig hebben om hun nieuwe taken en bevoegdheden uit te voeren.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☐ **beperkte geldigheidsduur**

☐ Voorstel/initiatief is van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

☑ **onbeperkte geldigheidsduur**

Uitvoering met een opstartperiode vanaf 2021

gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)[51]

Direct beheer door de Commissie via

☐ uitvoerende agentschappen

☐ **Gedeeld beheer** met lidstaten

☑ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

☐ internationale organisaties en hun agentschappen (geef aan welke);

☐ de EIB en het Europees Investeringsfonds;

☑ de in de artikelen 70 en 71 bedoelde organen;

☐ publiekrechtelijke organen;

☐ privaatrechtelijke organen met een openbare dienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

[51] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

Opmerkingen

n.v.t.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

In lijn met de reeds bestaande regelingen stellen de ETA's regelmatig verslagen op over hun activiteiten (waaronder interne rapportage aan het senior management, rapportage aan de raden en het jaarverslag) en zijn zij onderworpen aan audits door de Rekenkamer en de dienst voor interne audit van de Commissie over hun gebruik van middelen en prestaties. De monitoring en rapportage van de in het voorstel opgenomen acties zal in overeenstemming zijn met reeds bestaande vereisten en met alle nieuwe vereisten die uit voorliggend voorstel voortvloeien.

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

Het beheer zal indirect via de ETA's verlopen. Het financieringsmechanisme zou worden ingevoerd via vergoedingen die van de betrokken ICT-TPP's worden gevraagd.

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

Met betrekking tot het juridische, economische, efficiënte en effectieve gebruik van uit het voorstel voortvloeiende kredieten vallen geen nieuwe significante risico's te verwachten die niet in een bestaand kader voor interne controle aan bod komen. Een nieuwe uitdaging zou echter te maken kunnen hebben met de tijdige inning van vergoedingen van de betrokken cruciale ICT-TPP's.

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).

De beheers- en controlesystemen waarin de ETA-verordeningen voorzien, zijn reeds geïmplementeerd. De ETA's werken nauw samen met de dienst voor interne audit van de Commissie om ervoor te zorgen dat op alle gebieden van het internecontrolekader aan de passende normen wordt voldaan. Deze regelingen gelden eveneens ten aanzien van de rol van de ETA's in het kader van het onderhavige voorstel. Bovendien verleent het Europees Parlement op aanbeveling van de Raad elk begrotingsjaar kwijting aan elke ETA voor de uitvoering van haar begroting.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen, bijvoorbeeld in het kader van de fraudebestrijdingsstrategie.

Met het oog op de bestrijding van fraude, corruptie en andere onwettige activiteiten is Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11 september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) zonder enige beperking van toepassing op de ETA's.

De ETA's beschikken over een specifieke fraudebestrijdingsstrategie en een daaruit resulterend actieplan. De versterkte acties van de ETA's op het gebied van fraudebestrijding zullen in overeenstemming zijn met de regels en richtsnoeren van het Financieel Reglement (fraudebestrijdingsmaatregelen als onderdeel van goed financieel beheer), het fraudepreventiebeleid van OLAF, de bepalingen van de fraudebestrijdingsstrategie van de Commissie (COM(2011)376) en van de gemeenschappelijke aanpak van gedecentraliseerde EU-agentschappen (juli 2012) en de bijbehorende routekaart.

Daarnaast bevatten de verordeningen tot oprichting van de ETA's en de financiële verordeningen van de ETA's bepalingen over de uitvoering en controle van de begroting van de ETA's en de toepasselijke financiële regels, met inbegrip van die ter voorkoming van fraude en onregelmatigheden.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarige financiële kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarige financiële kader en de begrotingsonderdelen.

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Nummer	GK/ NGK[52]	van EVA-landen[53]	van kandidaat-lidstaten[54]	van derde landen	in de zin van artikel 21, lid 2, punt b), van het Financieel Reglement

Te creëren nieuwe begrotingsonderdelen

In volgorde van de rubrieken van het meerjarige financiële kader en de begrotingsonderdelen.

Rubriek van het meerjarige financiële kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	Nummer	GK/ NGK	van EVA-	van kandidaat-	van derde	in de zin van artikel 21, lid 2,

[52] GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

[53] EVA: Europese Vrijhandelsassociatie.

[54] Kandidaat-lidstaten en, in voorkomend geval, aspirant-kandidaten van de Westelijke Balkan.

			landen	lidstaten	landen	punt b), van het Financieel Reglement

3.2. Geraamde gevolgen voor de uitgaven

3.3. Samenvatting van de geraamde gevolgen voor de uitgaven

in miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarige financiële kader	Nummer	Post

DG : <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAAL**
	Vastleggingen	(1)									
	Betalingen	(2)									
TOTAAL kredieten voor DG <>	Vastleggingen										
	Betalingen										

Rubriek van het meerjarige financiële kader		

in miljoen EUR (tot op drie decimalen)

		2022	2023	2024	2025	2026	2027	**TOTAAL**
DG's:								
• Personele middelen								
• Andere administratieve uitgaven <>								
TOTAAL DG's	Kredieten							

TOTAAL kredieten voor RUBRIEK van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)							

in miljoen EUR (tot op drie decimalen)

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAAL**
TOTAAL kredieten voor RUBRIEKEN 1 van het meerjarige financiële kader	Vastleggingen							
	Betalingen							

3.3.1. Geraamde gevolgen voor de kredieten

☑ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

☐ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, in miljoen EUR (tot op drie decimalen) in constante prijzen

Vermeld doelstellingen en outputs ⇩			2022		2023		2024		2025		2026		2027		**TOTAAL**	
	OUTPUTS															
	Soort[55]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[56]…																
- Output																
Subtotaal voor specifieke doelstelling nr. 1																
SPECIFIEKE DOELSTELLING NR. 2…																
- Output																
Subtotaal voor specifieke doelstelling nr. 2																
TOTALE KOSTEN																

55 Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

56 Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

3.3.2. Geraamde gevolgen voor personele middelen

3.3.2.1. Samenvatting

☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoen EUR (tot op drie decimalen) in constante prijzen

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**TOTAAL**
Tijdelijke functionarissen (AD-rangen)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Tijdelijke functionarissen (AST-rangen)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Arbeidscontractanten							
Gedetacheerde nationale deskundigen							
TOTAAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personeelsvereisten (VTE):

EBA, EIOPA, ESMA & EEA	2022	2023	2024	2025	2026	2027	**TOTAAL**
Tijdelijke functionarissen (AD-rangen) EBA=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Tijdelijke functionarissen (AST-rangen) EBA=1, EIOPA=1, ESMA=1	3	3	3	3	3	3	3
Arbeidscontractanten							
Gedetacheerde nationale deskundigen							
TOTAAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Geraamde behoefte aan personele middelen voor de (verantwoordelijke) DG's

☑ Voor het voorstel/initiatief zijn geen personele middelen nodig

☐ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in een geheel getal (of met hoogstens 1 decimaal)

		2022	2023	2024	2025	2026	2027
• **Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)**							
• **Extern personeel (in voltijdequivalenten VTE)**[57]							
XX 01 02 01 (AC, END, SNE van de "totale financiële middelen")							
XX 01 02 02 (AC, AL, END, INT en JPD in de delegaties)							
XX 01 04 ***jj***[58]	- in de hoofdzetel[59]						
	- in delegaties						
XX 01 05 02 (AC, END, INT – onderzoek door derden)							
10 01 05 02 (AC, END, SNE – eigen onderzoek)							
Ander begrotingsonderdeel (te vermelden)							
TOTAAL							

XX is het beleidsterrein of de begrotingstitel.

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	
Extern personeel	

[57] AC= Agent Contractuel (arbeidscontractant); AL= Agent Local (plaatselijk functionaris); END= Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

[58] Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

[59] Voornamelijk voor de structuurfondsen, het Europees Landbouwfonds voor plattelandsontwikkeling (Elfpo) en het Europees Visserijfonds (EVF).

De beschrijving van de kostenberekening per voltijdequivalent dient in het derde onderdeel van bijlage V te worden opgenomen.

3.3.3. Verenigbaarheid met het huidige meerjarige financiële kader

☑ Het voorstel/initiatief is verenigbaar met het huidige meerjarige financiële kader.

☐ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarige financiële kader.

☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarige financiële kader[60].

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen en de desbetreffende bedragen. […]

3.3.4. Bijdragen van derden

☐ Het voorstel/initiatief voorziet niet in medefinanciering door derden

☑ Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder wordt geraamd:

in miljoen EUR (tot op drie decimalen)

EBA

	2022	2023	2024	2025	2026	2027	Totaal
De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[61].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAAL medegefinancierde kredieten	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Totaal

[60] Zie de artikelen 11 en 17 van Verordening (EU, Euratom) nr. 1311/2013 tot bepaling van het meerjarig financieel kader voor de jaren 2014-2020.

[61] 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[62].	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAAL medegefinancierde kredieten	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Totaal
De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[63].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAAL medegefinancierde kredieten	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Geraamde gevolgen voor de ontvangsten

☑ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

☐ voor de eigen middelen

☐ voor overige ontvangsten

☐ Geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven

in miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[64]						
		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel ….								

62 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

63 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

64 Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.

Vermeld voor de diverse bestemmingsontvangsten het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

[…]

Vermeld de wijze van berekening van de gevolgen voor de ontvangsten.

[…]

BIJLAGE

Algemene aannames

Titel 1 - Personeelsuitgaven

De volgende specifieke aannames zijn toegepast bij de berekening van de personeelsuitgaven op basis van de vastgestelde personeelsbehoeften die hieronder zijn uiteengezet:

- In 2022 aangeworven extra personeelsleden worden begroot voor zes maanden, gezien de tijd die naar verwachting nodig is om de extra personeelsleden aan te werven.
- De gemiddelde jaarlijkse kostprijs van een tijdelijke functionaris is 150 000 EUR; dit omvat 25 000 EUR aan "habillage"-kosten (gebouwen, IT enz.).
- De correctiecoëfficiënten voor salariskosten in Parijs (EBA en ESMA) en Frankfurt (Eiopa) bedragen respectievelijk 117,7 en 99,4.
- De pensioenpremies van werkgevers voor tijdelijke functionarissen zijn gebaseerd op de in de standaard gemiddelde jaarlijkse kosten vervatte standaardbasissalarissen, d.w.z. 95 660 EUR.
- De extra tijdelijke functionarissen zijn AD5's en AST's.

Titel 2 − Infrastructuur- en operationele uitgaven

De kosten zijn gebaseerd op een vermenigvuldiging van het aantal personeelsleden met het deel van het jaar dat zij in dienst zijn, met het de standaardkosten voor "habillage", d.w.z. 25 000 EUR.

Titel III: Operationele uitgaven

De kosten worden geraamd aan de hand van de volgende aannames:

- Vertaalkosten worden bepaald op 350 000 EUR per jaar voor elk van de ETA's.
- Voor de eenmalige IT-kosten van 500 000 EUR per ETA is de aanname dat deze over de twee jaren 2022 en 2023 worden gemaakt, op basis van een 50 % – 50 %-splitsing. De jaarlijkse onderhoudskosten vanaf 2024 worden op 50 000 EUR geraamd per ETA.
- De jaarlijkse kosten voor toezicht ter plaatse worden per ETA op 200 000 EUR geraamd.

De hier gepresenteerde ramingen leiden tot de volgende kosten per jaar:

Rubriek van het meerjarige financiële kader	Nummer	

Constante prijzen

EBA:			2022	2023	2024	2025	2026	2027	**TOTAAL**
Titel 1:	Vastleggingen	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Betalingen	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titel 2:	Vastleggingen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalingen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Vastleggingen	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Betalingen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAAL kredieten voor EBA	Vastleggingen	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Betalingen	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**TOTAAL**
Titel 1:	Vastleggingen	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Betalingen	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Titel 2:	Vastleggingen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalingen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Vastleggingen	(3 a)	0,800	0,800	0,600	0,600	0.600	0.600	4,000
	Betalingen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAAL kredieten	Vastleggingen	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

voor EIOPA	Betalingen	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**TOTAAL**
Titel 1:	Vastleggingen	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Betalingen	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titel 2:	Vastleggingen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalingen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Vastleggingen	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Betalingen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAAL kredieten voor ESMA	Vastleggingen	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Betalingen	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Voor het voorstel zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten in miljoen EUR (tot op drie decimalen) in constante prijzen

EBA

Vermeld doelstellingen en outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Soort[65]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal nr.	Totale kosten
SPECIFIEKE DOELSTELLING nr. 1[66] Rechtstreeks toezicht op cruciale ICT-TPP's																
Output				0,800		0,800		0,600		0,600		0,600		0.600		4,000
Subtotaal voor specifieke doelstelling nr. 1																
SPECIFIEKE DOELSTELLING NR. 2…																
Output																
Subtotaal voor specifieke doelstelling nr. 2																
TOTALE KOSTEN				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Vermeld doelstellingen en outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Soort[67]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING nr. 1[68] Rechtstreeks toezicht op cruciale																

[65] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[66] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

[67] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[68] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

ICT-TPP's																
Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotaal voor specifieke doelstelling nr. 1																
SPECIFIEKE DOELSTELLING nr. 2…																
Output																
Subtotaal voor specifieke doelstelling nr. 2																
TOTALE KOSTEN				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Vermeld doelstellingen en outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Soort[69]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING nr. 1[70] Rechtstreeks toezicht op cruciale ICT-TPP's																
Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotaal voor specifieke doelstelling nr. 1																
SPECIFIEKE DOELSTELLING nr. 2…																
Output																
Subtotaal voor specifieke doelstelling nr. 2																
TOTALE KOSTEN				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[70] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

De toezichtactiviteiten worden volledig gefinancierd door vergoedingen die van de onder toezicht staande aanbieders worden gevraagd:

EBA

	2022	2023	2024	2025	2026	2027	Totaal
De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[71].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAAL medegefinancierde kredieten	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Totaal
De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[72].	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAAL medegefinancierde kredieten	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Totaal

[71] 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

[72] 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

De kosten worden voor 100 % gedekt door vergoedingen die van de onder toezicht staande entiteiten worden gevraagd[73].	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAAL medegefinancierde kredieten	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPECIFIEKE INFORMATIE

Bevoegdheden op het gebied van rechtstreeks toezicht

Om te beginnen dient eraan te worden herinnerd dat onder rechtstreeks toezicht van de ESMA staande entiteiten vergoedingen aan de ESMA moeten betalen (eenmalige kosten voor registratie en vaste kosten voor continu toezicht). Dit is het geval voor ratingbureaus (zie Gedelegeerde Verordening (EU) nr. 272/2012 van de Commissie) en transactieregisters (Gedelegeerde Verordening (EU) nr. 1003/2013 van de Commissie).

Volgens dit wetgevingsvoorstel zullen de ETA's worden belast met nieuwe taken die gericht zijn op het bevorderen van convergentie in de aanpak van het toezicht op ICT-risico's van derde aanbieders in de financiële sector door cruciale aanbieders van ICT-diensten aan een kader voor Unietoezicht te onderwerpen.

Het in dit voorstel naar voren geschoven toezichtkader bouwt voort op de bestaande institutionele architectuur op het gebied van financiële diensten, waarbij het Gemengd Comité van de ETA's in overeenstemming met zijn taken inzake cyberveiligheid de sectoroverschrijdende coördinatie met betrekking tot alle aangelegenheden op het gebied van ICT-risico's garandeert. Daarvoor krijgt het de steun van het bevoegde subcomité (toezichtforum) dat voorbereidende werkzaamheden verricht voor individuele besluiten en collectieve aanbevelingen die gericht zijn tot cruciale derde aanbieders van ICT-diensten.

Via dit kader krijgen de ETA's die voor elke cruciale derde aanbieder van ICT-diensten als leidende toezichthouder zijn aangewezen, bevoegdheden om ervoor te zorgen dat aanbieders van technologiediensten die een cruciale rol vervullen voor het functioneren van de financiële sector, op pan-Europese schaal passend worden gemonitord. De toezichttaken zijn in het voorstel uiteengezet en worden in het financieel memorandum verder verduidelijkt. Het gaat onder meer om het recht om alle relevante informatie en documentatie op te vragen in het kader van algemene onderzoeken en inspecties, om aanbevelingen te doen en vervolgens verslagen in te dienen over de genomen maatregelen of de uitgevoerde corrigerende maatregelen waarmee gevolg wordt gegeven aan die aanbevelingen.

Voor de uitvoering van de nieuwe taken waarin dit voorstel voorziet, moeten de ETA's dan ook extra personeel in dienst nemen dat gespecialiseerd is in ICT-risico's en zich toelegt op de beoordeling van de mate van afhankelijkheid van derden.

De behoefte aan personele middelen kan worden geraamd op 6 vte voor elke autoriteit (5AD's en 1 AST ter ondersteuning van de AD's). De ETA's zullen ook te maken krijgen met extra

[73] 100% van de totale geraamde kosten plus de volledige pensioenbijdragen van de werkgever

IT-kosten, geraamd op 500 000 EUR (eenmalige kosten) en op 50 000 EUR per jaar voor onderhoudskosten voor elk van de drie ETA's. Eén belangrijk onderdeel van de nieuwe uit te voeren taken zijn de missies om inspecties en audits ter plaatse te verrichten; deze worden geraamd op 200 000 EUR per jaar voor elke ETA. De vertaalkosten voor de verschillende documenten die cruciale aanbieders van ICT-diensten aan ETA's bezorgen, zijn eveneens opgenomen in de rij voor de operationele kosten en bedragen 350 000 EUR per jaar.

Alle genoemde administratieve kosten zullen volledig worden gefinancierd met de jaarlijkse vergoedingen die de ETA's aan de onder toezicht staande derde aanbieders van ICT-diensten in rekening brengen (geen gevolgen voor de EU-begroting).