III

(Voorbereidende handelingen)

EUROPESE CENTRALE BANK

ADVIES VAN DE EUROPESE CENTRALE BANK

van 4 juni 2021

inzake een voorstel voor een Verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector

(CON/2021/20)

(2021/C 343/01)

Inleiding en rechtsgrondslag

Op 22, 23 en 29 december 2020 ontving de Europese Centrale Bank (ECB) van respectievelijk de Raad van de Europese Unie en het Europees Parlement verzoeken om een advies over een voorstel voor een Verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 ([1]) (hierna "de ontwerpverordening" genoemd) en een voorstel voor een Richtlijn tot wijziging van de Richtlijnen 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 ([2]) (hierna "de ontwerpwijzigingsrichtlijn" genoemd, samen met de "ontwerpverordening", de "ontwerphandelingen" genoemd).

De bevoegdheid van de ECB om advies uit te brengen is gebaseerd op artikel 127, lid 4 en artikel 282, lid 5, van het Verdrag betreffende de werking van de Europese Unie, aangezien de voorgestelde handelingen bepalingen bevatten die onder de bevoegdheid van de ECB vallen, met name de bepaling en de uitvoering van het monetair beleid, de bevordering van de goede werking van het betalingsverkeer, de bijdrage aan een goede beleidsvoering van de bevoegde autoriteiten ten aanzien van de stabiliteit van het financiële marktstelsel, en de taken van de ECB ten aanzien van het bedrijfseconomisch toezicht op kredietinstellingen krachtens artikel 127, lid 2,het eerste en vierde streepje, artikel 127, lid 5, en artikel 127, lid 6, VWEU. Overeenkomstig de eerste zin van artikel 17.5 van het reglement van orde van de Europese Centrale Bank heeft de Raad van bestuur dit advies goedgekeurd.

1. Algemene opmerkingen

1.1 De ECB is ingenomen met de ontwerpverordening, die tot doel heeft de cyberveiligheid en de operationele veerkracht van de financiële sector te verbeteren. De ECB is met name ingenomen met het doel van de ontwerpverordening om de belemmeringen voor en de totstandbrenging en werking van de interne markt voor financiële diensten weg te nemen door de regels die van toepassing zijn op het risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), de rapportage, het testen en ICT-risico van derde-aanbieders te harmoniseren. Voorts is de ECB ingenomen met het doel van de ontwerpverordening om alle overlappende regelgevingsvereisten of toezichtverwachtingen waaraan financiële entiteiten momenteel krachtens het Unierecht onderworpen zijn, te stroomlijnen en te harmoniseren.

1.2 De ECB begrijpt dat ten aanzien van financiële entiteiten die als aanbieders van essentiële diensten worden aangemerkt ([3]), de ontwerpverordening in overeenstemming met de betekenis zoals uiteengezet in artikel 1, lid 7, van Directive (EU) 2016/1148, van het Europees Parlement en de Raad ([4]) (hierna de "NIS-richtlijn" genoemd) sectorspecifieke wetgeving (*lex specialis)* vertegenwoordigt, hetgeen inhoudt dat de vereisten in de ontwerpverordening in beginsel over de NIS-richtlijn prevaleren. In de praktijk zouden financiële entiteiten die als aanbieders van essentiële diensten ([5]) worden aangemerkt, onder meer incidenten melden overeenkomstig

([1]) COM(2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Zie artikel 1, lid 2, van de ontwerpverordening.
([4]) 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).
([5]) Zie artikel 5 van de NIS-richtlijn.

de ontwerpverordening in plaats van de NIS-richtlijn. Hoewel de ECB ingenomen is met de vermindering van mogelijke overlappende vereisten voor financiële entiteiten op het gebied van de melding van incidenten, moet verder worden nagedacht over de wisselwerking tussen de ontwerpverordening en de NIS-richtlijn. Zo zou een derde aanbieder van ICT-diensten ([6]) op grond van de ontwerpverordening onderworpen kunnen worden aan aanbevelingen van de leidende toezichthouder ([7]). Tegelijkertijd kan dezelfde derde ICT-dienstverlener op grond van de NIS-richtlijn worden aangemerkt als aanbieder van essentiële diensten en onderworpen worden aan bindende instructies van de bevoegde autoriteit ([8]). In dat geval zou de derde aanbieder van ICT-diensten het voorwerp kunnen zijn van tegenstrijdige aanbevelingen in het kader van de ontwerpverordening en bindende instructies uit hoofde van de NIS-richtlijn. De ECB stelt voor dat de wetgevingsorganen van de Unie zich verder beraden op mogelijke inconsistenties tussen de ontwerpverordening en de NIS-richtlijn die de harmonisatie en vermindering van overlappende en tegenstrijdige vereisten voor financiële entiteiten kunnen belemmeren.

1.3 De ECB begrijpt ook dat krachtens het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot intrekking van Richtlijn (EU) 2016/1148 ([9]) (hierna de "ontwerp-NIS2-richtlijn"), "bijna-ongelukken" ([10]) onderworpen zullen zijn aan rapportageverplichtingen ([11]). Terwijl overweging (39) van de voorgestelde NIS2-richtlijn verwijst naar de betekenis van de term "bijna-ongelukken" is het onduidelijk of het de bedoeling is voor te schrijven dat bijna-ongelukken worden gemeld door de in artikel 2 van de ontwerpverordening genoemde financiële entiteiten. In dit verband, en ook rekening houdend met het feit dat bijna-ongelukken pas als zodanig kunnen worden geïdentificeerd nadat zij zich hebben voorgedaan, zou de ECB graag tijdig in kennis worden gesteld van significante bijna-ongelukken, zoals momenteel het geval is bij cyberincidenten. De ECB stelt voor om de ontwerpverordening en de voorgestelde NIS2-richtlijn beter op elkaar af te stemmen om de precieze reikwijdte te verduidelijken van de rapportage waaraan een bepaalde financiële entiteit onderworpen kan zijn uit hoofde van deze twee afzonderlijke maar onderling verbonden onderdelen van de Uniewetgeving. Tegelijkertijd zouden "bijna-ongelukken" moeten worden gedefinieerd en zouden bepalingen moeten worden ontwikkeld om de betekenis ervan te verduidelijken.

1.4 De ECB is ingenomen met het stimuleren van financiële entiteiten om op vrijwillige basis informatie en inlichtingen over cyberdreiging uit te wisselen om hun cyberweerbaarheid te verbeteren en te versterken. De ECB heeft zelf bijstand verleend bij het *Cyber Intelligence Information Sharing Initiative* (Initiatief tot informatie-uitwisseling over cyber-inlichtingen - CIISI-EU) en de blauwdrukken beschikbaar gesteld aan iedereen om een dergelijk systeem te bouwen en te bevorderen ([12]).

1.5 De ECB ondersteunt de samenwerking tussen de bevoegde autoriteiten voor de toepassing van de ontwerpverordening, de Europese toezichthoudende autoriteiten (ETA's) en de Computer Security Incident Response Teams (CSIRTS) ([13]). Het is van essentieel belang informatie uit te wisselen om de operationele veerkracht van de Unie te waarborgen, aangezien informatie-uitwisseling en samenwerking tussen autoriteiten kunnen bijdragen tot de preventie van cyberaanvallen en kunnen bijdragen tot het verminderen van de verspreiding van ICT-dreigingen. Een gemeenschappelijke interpretatie van ICT-gerelateerde risico's moet worden bevorderd en er moet worden gezorgd voor een consistente beoordeling van dergelijke risico's in de gehele Unie. Het is van het grootste belang dat informatie alleen wordt gedeeld met het centrale contactpunt ([14]) en de nationale CSIRTS door de bevoegde autoriteiten ([15]) wanneer er duidelijke mechanismen voor classificatie en informatie-uitwisseling bestaan in combinatie met passende waarborgen om de vertrouwelijkheid te waarborgen.

1.6 Ten slotte zou de ECB graag zien dat in het kader van de ontwerpverordening regels inzake persoonsgegevens en gegevensbewaring worden ingevoerd. Bij de bepaling van de duur van de bewaringstermijn moet rekening worden gehouden met het onderzoek, de inspectie, het verzoek om informatie, de mededeling, de publicatie, de evaluatie, de verificatie, de beoordeling en de opstelling van oversight- of toezichtplannen die de bevoegde autoriteiten eventueel moeten uitvoeren in het kader van hun respectieve verplichtingen en taken uit hoofde van de ontwerpverordening. In dit verband zou een bewaringstermijn van 15 jaar toereikend zijn. In

([6]) Zie artikel 3, punt 15, van de ontwerpverordening.
([7]) Zie artikel 31, lid 1, onder d) van de ontwerpverordening.
([8]) Zie artikel 15, lid 3, van de NIS-richtlijn.
([9]) COM (2020) 823 final.
([10]) Gebeurtenissen die mogelijk schade hadden kunnen veroorzaken, maar die met succes zijn verhinderd om volledig uit te komen; zie overweging 39 van de NIS2-Richtlijn.
([11]) Zie artikel 11 van de NIS2-richtlijn.
([12]) Initiatief tot informatie-uitwisseling over cyberdreigingen (CIISI-EU), beschikbaar op de website van de ECB www.ecb.europa.eu.
([13]) Zie artikel 42 van de ontwerpverordening
([14]) Zie artikel 8, lid 3, van de NIS-richtlijn.
([15]) Zie eveneens de artikelen 11, 26 en 27 van de NIS2-Richtlijn

specifieke gevallen kan deze bewaringstermijn worden verkort of verlengd. In dit verband stelt de ECB voor dat de wetgevingsorganen van de Unie bij de formulering van de desbetreffende bepaling inzake persoonsgegevens en gegevensbewaring ook rekening houden met het beginsel van minimale gegevensverwerking, alsook met verdere verwerking voor archiveringsdoeleinden in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden ([16]).

2. **Specifieke opmerkingen over oversight en effectenclearing en -afwikkeling**

2.1 *Bevoegdheden op het gebied van oversight van het ESCB en het Eurosysteem*

2.1.1 Nauw verband houdend met de fundamentele taken van het ESCB voorzien het Verdrag en de statuten van het Europees Stelsel van Centrale Banken en van de Europese Centrale Bank (hierna "de ESCB-statuten" genoemd) in het toezicht van het Eurosysteem op clearing- en betalingssystemen. Krachtens artikel 127, lid 2, het vierde streepje, van het Verdrag, zoals overgenomen in artikel 3,1, van de ESCB-statuten is een andere via het Europees Stelsel van Centrale Banken (ESCB) uit te voeren fundamentele taak het bevorderen van de goede werking van het betalingsverkeer. Bij de uitvoering van deze fundamentele taak geldt dat "de ECB en de nationale centrale banken zijn gerechtigd faciliteiten ter beschikking stellen, en de ECB kan verordeningen vaststellen ter verzekering van doelmatige en deugdelijke clearing- en betalingssystemen binnen de Unie en met andere landen" ([17]). Uit hoofde van haar toezichthoudende rol heeft de ECB Verordening (EU) nr. 795/2014 van de Europese Centrale Bank (ECB/2014/28) (hierna de "SIPS-verordening" genoemd) vastgesteld. ([18]) De SIPS-verordening legt de beginselen voor financiële marktinfrastructuren (Principles for financial market infrastructures) ten uitvoer die zijn uitgevaardigd door het Comité betalingen en verrekeningen (Committee on Payment and Settlement Systems) en de International organisatie van effectentoezichthouders (International Organization of Securities Commissions) ([19]), die juridisch bindend zijn en zowel systemen voor grote als systeemrelevante retailbetalingen bestrijken die worden geëxploiteerd door een centrale bank van het Eurosysteem of een particuliere entiteit. Het oversightbeleidskader ([20]) van het Eurosysteem identificeert betaalinstrumenten als een "integraal onderdeel van betalingssystemen" en omvat derhalve deze instrumenten binnen het toepassingsgebied van het oversight ervan. Het oversightkader voor betaalinstrumenten wordt momenteel herzien ([21]). Binnen dat kader wordt een betaalinstrument (bv. een kaart, overmaking, automatische afschrijving, e-geldovermaking en digitale betaaltoken ([22])) gedefinieerd als een gepersonaliseerd instrument (of een reeks apparaten) en/of een reeks procedures die zijn overeengekomen tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder die worden gebruikt om een waardeoverdracht te initiëren ([23]).

2.1.2 In het licht van het bovenstaande is de ECB ingenomen met de uitsluiting van systeembeheerders als gedefinieerd in artikel 2, punt p), van Richtlijn 98/26/EG van het Europees Parlement en de Raad ([24]), betalingssystemen (met inbegrip van door centrale banken geëxploiteerde systemen), betalingsschema's en betalingsregelingen met het oog op de toepassing van de hierboven genoemde oversightkaders van het toepassingsgebied

([16]) Zie artikel 4, punt b), en artikel 13 van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

([17]) Zie artikel 22 van de ESCB-statuten.

([18]) Verordening van de Europese Centrale Bank (EU) nr. 795/2014 van 3 juli 2014 met betrekking tot oversightvereisten voor systeemrelevante betalingssystemen (ECB/2014/28) (PB L 217 van 23.7.2014, blz. 16).

([19]) Beschikbaar op de website van de Bank voor Internationale Betalingen onder www.bis.org.

([20]) Eurosystem oversight policy framework, herziene versie (juli 2016), beschikbaar in het Engels op de website van de ECB onder www.ecb.europa.eu..

([21]) Zie de herziene en geconsolideerde versie van het *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (PISA framework)'" beschikbaar op de ECB-website onder: www.ecb.europa.eu.

([22]) Een digitale betaaltoken is een digitale weergave van waarde die wordt gedekt door vorderingen of activa die elders zijn geregistreerd en die de waardeoverdracht tussen eindgebruikers mogelijk maakt. Afhankelijk van het onderliggende ontwerp kunnen digitale betaaltokens voorzien in een overdracht van waarde zonder dat er noodzakelijkerwijs een centrale derde partij bij betrokken is en/of gebruik wordt gemaakt van betaalrekeningen.

([23]) "Overdracht van waarde": "de door de betaler of namens de betaler of door de begunstigde geïnitieerde handeling waarbij geldmiddelen of digitale betaaltokens worden overgemaakt of contanten op/van een gebruikersrekening worden geplaatst of opgenomen, ongeacht onderliggende verplichtingen tussen de betaler en de begunstigde. Bij de overmaking kunnen één of meerdere betalingsdienstaanbieders betrokken zijn." De definitie van "overdracht van waarde" in het PISA-kader wijkt af van wat wordt gedefinieerd als een overdracht van "geldovermaking" in de zin van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, tot wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010, en tot intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35). Een "overdacht van waarde" in het kader van een "betaalinstrument" als gedefinieerd in de PSD2 kan alleen betrekking hebben op een overdracht van "geldmiddelen". Uit hoofde van PSD2 omvatten "geldmiddelen" geen digitale betaaltokens, tenzij de tokens als elektronisch geld kunnen worden geclassificeerd (of hypothetisch gezien als giraal geld).

([24]) 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).

van de ontwerpverordening. Om deze redenen moeten de bevoegdheden van het ESCB uit hoofde van het Verdrag en de bevoegdheden van het Eurosysteem uit hoofde van de SIPS-verordening duidelijk worden omschreven in de overwegingen van de ontwerpverordening.

2.1.3 Evenzo is de ECB ingenomen met de uitsluiting van de toepassing van het oversightkader zoals uiteengezet in de ontwerpverordening van 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 genoemde taken ([25]). In dit verband wenst de ECB te benadrukken dat centrale banken van het ESCB die in hun monetaire hoedanigheid ([26]) optreden en het Eurosysteem bij het verrichten van diensten via TARGET2, TARGET2-Securites (T2S) ([27]) en TARGET Instant Payment Settlement (TIPS) ([28]) niet onder het artikel betreffende het toepassingsgebied van de ontwerpverordening vallen, en evenmin kunnen worden beschouwd als derde aanbieders van ICT-diensten en dus potentieel geclassificeerd kunnen worden als cruciale derde aanbieders van ICT-diensten in de zin van de ontwerpverordening. Het Eurosysteem houdt toezicht op T2S in samenhang met zijn opdracht om te zorgen voor efficiënte en deugdelijke clearing- en betalingssystemen. Voorts heeft ESMA verduidelijkt dat T2S geen aanbieder van kritieke diensten ([29]) is in de zin van Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad ([30]) (hierna "CSD-verordening" genoemd). Bijgevolg worden de organisatorische en operationele veiligheid, efficiëntie en veerkracht van T2S gewaarborgd door middel van het toepasselijke juridische, regelgevende en operationele kader en overeengekomen governanceregelingen van T2S, in tegenstelling tot de CSD-verordening.

2.1.4 Daarnaast heeft het oversightbeleidskader ([31]) van het Eurosysteem betrekking op aanbieders van kritieke diensten zoals de Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is een in België gevestigde coöperatieve vennootschap met beperkte aansprakelijkheid, die internationaal beveiligde berichtendiensten aanbiedt. De Nationale Bank van België treedt op als toezichthouder op SWIFT en oefent op basis van een coöperatieve oversightregeling toezicht uit op SWIFT, in samenwerking met de andere centrale banken van de G10, waaronder de ECB. De toezichthouders van de G10 erkennen dat het operationele risico van SWIFT het voornaamste aandachtspunt van het toezicht is, aangezien dit wordt beschouwd als de primaire risicocategorie via welke SWIFT een systeemrisico voor het financiële stelsel in de Unie zou kunnen vormen. In dit verband heeft de SWIFT-Cooperative Oversight Group een specifieke reeks beginselen en hoge verwachtingen ontwikkeld die van toepassing zijn op SWIFT, zoals het identificeren en beheren van risico's, informatiebeveiliging, betrouwbaarheid en veerkracht, technologische planning en communicatie met gebruikers. De toezichthouders van de G10 verwachten dat SWIFT zich aansluit bij het Comité betalingen en verrekeningen (Committee on Payment and Market Infrastructures - CPMI) en de *Guidance on cyber resilience* ([32]) (Richtsnoeren inzake cyberveerkracht) van de Internationale Organisatie van effectentoezichthouders (International Organization of Securities Commissions – IOSCO) en andere internationale normen inzake ICT-beveiliging die samen de vereisten van de ontwerpverordening overtreffen.

2.1.5 Het is niet zeker dat SWIFT en wellicht andere dienstverleners die onder het oversightbeleidskader van het Eurosysteem vallen, onderworpen zouden kunnen zijn aan de ontwerpverordening als derde aanbieders van ICT-diensten indien zij diensten zouden verlenen die niet onder artikel 127, lid 2, van het Verdrag vallen. De ECB is dan ook zeer verheugd over het feit dat dienstverleners die reeds onder het toezichtbeleidskader van het Eurosysteem vallen, met inbegrip van, maar niet beperkt tot SWIFT, worden uitgesloten van het toepassingsgebied van het toezichtkader dat in de ontwerpverordening is vastgesteld.

([25]) Zie artikel 28, lid 5, van de ontwerpverordening.

([26]) Zie punt 1.3 van het Advies van de Europese Centrale Bank van 19 februari 2021 inzake een voorstel voor een verordening betreffende markten in cryptoactiva en tot wijziging van Richtlijn (EU) 2019/1937 (CON/2021/4). Alle ECB-Adviezen worden gepubliceerd op EUR-Lex.

([27]) Zie bijlage IIa bij Richtsnoer (ECB/2012/27) van 5 december 2012 betreffende een geautomatiseerd trans-Europees realtime-brutovereveningssysteem (TARGET2) (PB L 30 van 30.1.2013, blz. 1) Richtsnoer ECB/2012/13, Richtsnoer van de Europese Centrale Bank van 18 juli 2012 betreffende TARGET2-securities (ECB/2012/13) (PB L 215 van 11.8.2012, blz 19) en Besluit ECB/2011/20 van de Europese Centrale Bank van 16 november 2011 tot vaststelling van gedetailleerde regels en procedures voor de tenuitvoerlegging van de geschiktheidscriteria voor centrale effectenbewaarinstellingen voor toegang tot TARGET2-Securities-diensten (PB L 319 van 2.12.2011, blz. 117). Zie ook de T2S-kaderovereenkomst en de collectieve overeenkomst.

([28]) Zie bijlage IIb bij Richtsnoer ECB/2012/27.

([29]) Zie artikel 30, lid 5, van Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 263/2012 (PB L 257 van 28.8.2014, blz. 1) en artikel 68 van Gedelegeerde Verordening (EU) 2017/392 van de Commissie van 11 november 2016 tot aanvulling van Verordening (EU) nr.. 909/2014 van het Europees Parlement en de Raad met technische reguleringsnormen inzake vergunnings-, toezichts- en operationele vereisten voor centrale effectenbewaarinstellingen (PB L 65 van 10.3.2017, blz. 48).

([30]) Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 263/2012 (PB L 257 van 28.8.2014, blz. 1)

([31]) Eurosystem oversight policy framework, herziene versie (juli 2016), beschikbaar in het Engels op de website van de ECB onder www.ecb.europa.eu.

([32]) Beschikbaar op de website van de Bank voor Internationale Betalingen onder www.bis.org.

2.2 *Bevoegdheden van de ECB op het gebied van effectenafwikkeling*

2.2.1 Centrale effectenbewaarinstellingen (central securities depositories - CSD's) zijn financiëlemarktinfrastructuren (FMI's) die strikt worden gereguleerd door en onder toezicht staan van verschillende autoriteiten overeenkomstig de CSD-verordening, waarin vereisten voor de afwikkeling van financiële instrumenten en regels inzake de organisatie en het gedrag van CSD's zijn vastgelegd. Daarnaast moeten CSD's rekening houden met de CPMI-IOSCO richtsnoeren inzake cyberweerbaarheid, die zijn geoperationaliseerd door de *Cyber resilience oversight expectations for financial market infrastructures* (december 2018) ([33]). Naast de toezichtbevoegdheden die krachtens de CSD-verordening aan de nationale bevoegde autoriteiten (NBA's) zijn toegekend, treden de leden van het ESCB op als "relevante autoriteiten" in hun hoedanigheid van toezichthouders op door CSD's geëxploiteerde effectenafwikkelingssystemen, centrale banken die de meest relevante valuta's uitgeven waarin afwikkeling plaatsvindt, en centrale banken in wier boeken de geldzijde van transacties wordt afgewikkeld ([34]). In dit verband wordt in overweging 8 van de CSD-verordening gesteld dat de verordening van toepassing moet zijn onverminderd de verantwoordelijkheden van de ECB en de nationale centrale banken (NCB's) voor het waarborgen van efficiënte en gezonde clearing- en betalingssystemen. Voorts wordt in overweging 8 gesteld dat de CSD-verordening de leden van het ESCB niet mag beletten de informatie te raadplegen die relevant is voor de uitvoering van hun taken ([35]), met inbegrip van de controle op CSD's en andere FMI's ([36]) .

2.2.2 Daarnaast treden de leden van het ESCB vaak op als afwikkelende instantie voor de geldzijde van effectentransacties en biedt het Eurosysteem afwikkelingsdiensten via T2S aan CSD's aan. Het toezicht van het Eurosysteem op T2S houdt verband met zijn mandaat om te zorgen voor efficiënte en deugdelijke clearing- en betalingssystemen, terwijl bevoegde en relevante autoriteiten van CSD's ernaar streven de soepele werking, de veiligheid en efficiëntie van de afwikkeling en de goede werking van de financiële markten in hun respectieve rechtsgebieden te waarborgen.

2.2.3 Op grond van de ontwerpverordening ([37]) zijn centrale banken niet betrokken bij de ontwikkeling van technische normen met betrekking tot de specificatie van ICT-risico's. Evenzo worden de betrokken autoriteiten op grond van de ontwerpverordening ([38]) niet op de hoogte gebracht van ICT-gerelateerde incidenten. De centrale bank van het ESCB moet hetzelfde niveau van betrokkenheid behouden als momenteel in de CSD-verordening is bepaald, en de relevante autoriteiten moeten in kennis worden gesteld van ICT-gerelateerde incidenten. Het Eurosysteem is de relevante autoriteit voor alle CSD's in het eurogebied en voor verscheidene andere EU-CSD's. Centrale banken van het ESCB zouden moeten worden geïnformeerd over ICT-gerelateerde incidenten die relevant zijn voor de uitvoering van hun taken, met inbegrip van het oversight op CSD's en andere FMI's. De risico's waaraan CSD's zijn blootgesteld, waaronder ICT-risico's, kunnen een bedreiging vormen voor de goede werking van CSD's. Daarom zijn ICT-risico's van belang voor de betrokken autoriteiten, die een volledig en gedetailleerd overzicht van deze risico's moeten krijgen om ze te beoordelen en invloed uit te oefenen op de aanpak van het risicobeheer van de CSD's. De ontwerpverordening mag niet voorzien in minder beperkende vereisten met betrekking tot ICT-risico's in vergelijking met de vereisten waarin de CSD-verordening en de huidige technische reguleringsnormen voorzien.

2.2.4 Daarnaast moeten de wetgevingsorganen van de Unie de wisselwerking tussen de ontwerpverordening ([39]) en de technische reguleringsnormen ter aanvulling van de CSD-verordening verduidelijken. Het is met name niet duidelijk of een CSD moet worden vrijgesteld van de verplichting om over een eigen secundaire locatie te beschikken wanneer haar derde aanbieder van ICT-diensten een dergelijke locatie onderhoudt ([40]). Indien een CSD wordt vrijgesteld van deze verplichting om een secundaire locatie aan te houden, is het onduidelijk wat de

([33]) Beschikbaar op de website van de ECB onder: www.ecb.europa.eu.

([34]) Zie artikel 12 van Verordening (EG) nr. 909/2014.

([35]) Zie ook artikel 13 en artikel 17, lid 4, en artikel 22, lid 6, van Verordening (EU) nr. 909/2014.

([36]) Zie punt 7.3 van het advies van de Europese Centrale Bank van 6 april 2017 inzake de identificatie van kritieke infrastructuren met het oog op de beveiliging van de informatietechnologie (CON/2017/10); punt 7.2 van het Advies van de Europese Centrale Bank van 8 november 2018 inzake de aanwijzing van essentiële diensten en aanbieders van essentiële diensten met het oog op de beveiliging van netwerk- en informatiesystemen (CON/2018/47); punt 3.5.2 van het Advies van de Europese Centrale Bank van 2 mei 2019 inzake de beveiliging van netwerk- en informatiesystemen (CON/2019/17) en punt 3.5.2 van het advies van de Europese Centrale Bank van 11 november 2019 inzake de beveiliging van netwerk- en informatiesystemen (CON/2019/38).

([37]) Zie artikel 54, lid 5, van de ontwerpverordening en artikel 45, lid 7, van Verordening (EG) nr. 909/2014.

([38]) Zie artikel 54, lid 4, van de ontwerpverordening en artikel 45, lid 6, van Verordening (EG) nr. 909/2014.

([39]) Zie artikel 11, lid 5, van de ontwerpverordening.

([40]) Zie artikel 78, lid 3, van Gedelegeerde Verordening (EU) nr. 2017/392 van de Commissie van 11 november 2016 houdende aanvulling van Verordening (EG) nr. 909/2014 van het Europees Parlement en de Raad met technische reguleringsnormen inzake de openbaarmakingsvereisten voor gestructureerde financieringsinstrumenten (PB L 65 van 10.3.2017, blz. 48).

juridische waarde van dit vereiste zou zijn. Evenzo verwijst de ontwerpverordening ([41]) naar een hersteltijddoelstelling en herstelpuntdoelstellingen voor elke functie ([42]), terwijl in de desbetreffende technische reguleringsnorm een onderscheid wordt gemaakt tussen kritieke functies ([43]) en kritieke bedrijfsactiviteiten ([44]) met betrekking tot de hersteltijd die is vastgesteld voor de kritieke activiteiten van CSD's. Verdere verduidelijking en reflectie door de wetgevingsorganen van de Unie is gerechtvaardigd met betrekking tot de wisselwerking tussen de ontwerpverordening en de technische reguleringsnormen ter aanvulling van de CSD-verordening, teneinde het risico van tegenstrijdige vereisten te voorkomen. Tot slot moet worden verduidelijkt dat de vrijstellingen die in het kader van de CSD-verordening worden verleend aan CSD's die door bepaalde publieke entiteiten worden geëxploiteerd ([45]), krachtens de ontwerpverordening worden uitgebreid.

2.3 *Bevoegdheden van het ESCB op het gebied van effectenclearing*

2.3.1 Centrale banken van het ESCB hebben oversightbevoegdheden met betrekking tot centrale tegenpartijen (CTP's). In dit verband werken de nationale centrale banken van het Eurosysteem vaak samen met de relevante nationale bevoegde autoriteiten in de oversight- en toezichthoudende functies van CTP's en nemen zij deel aan het krachtens Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ([46]) (hierna "EMIR" genoemd) opgerichte college van CTP's. De betrokken leden van het Eurosysteem ([47]) nemen als toezichthouder deel aan EMIR-colleges en vertegenwoordigen het Eurosysteem als centrale bank van uitgifte voor CTP's waarbij de euro een van de meest relevante valuta's is voor de geclearde financiële instrumenten (en voor offshore-CTP's die een aanzienlijk deel van de financiële instrumenten in euro clearen). De ECB is de centrale bank van uitgifte voor niet-eurogebied CTP's.

2.3.2 Op grond van de ontwerpverordening ([48]) zijn centrale banken van het ESCB niet betrokken bij de ontwikkeling van technische normen met betrekking tot de specificatie van ICT-risico's. Bovendien wordt in de ontwerpverordening ([49]) nergens verwezen naar de doelstelling van de hersteltijd en de vereisten van de herstelpuntdoelstelling uit hoofde van EMIR ([50]). De voorgestelde regelgeving mag niet voorzien in minder beperkende voorschriften met betrekking tot ICT-risico's dan die welke momenteel bestaan. Daarom is het van cruciaal belang duidelijke hersteltijd- en herstelpuntdoelstellingen vast te stellen met het oog op een degelijk kader voor bedrijfscontinuïteitsbeheer. Het handhaven van specifieke hersteltijd en -puntdoelstellingen maakt ook deel uit van de CPMI-IOSCO-beginselen voor financiëlemarktinfrastructuren (CPMI-IOSCO Principles for Financial Market Infrastructures ([51])). De huidige EMIR-bepaling moet worden gehandhaafd en de ontwerpverordening moet dienovereenkomstig worden aangepast. De centrale banken van het ESCB moeten worden betrokken bij de voorbereiding van wetgeving van secundair niveau en bij verdere verduidelijking en reflectie door de wetgevende organen van de Unie over de wisselwerking tussen de ontwerpverordening en de technische reguleringsnormen ter aanvulling daarvan, teneinde het risico van tegenstrijdige of overlappende vereisten te voorkomen.

3. **Specifieke opmerkingen over aspecten van prudentieel toezicht**

3.1 Verordening (EU) nr.1024/2013 van de Raad ([52]) (hierna de "GTM-verordening" genoemd) kent specifieke taken toe aan de ECB met betrekking tot het prudentieel toezicht op kredietinstellingen binnen het eurogebied en stelt de ECB verantwoordelijk voor de doeltreffende en consistente werking van het gemeenschappelijk toezichtsmechanisme (GTM), waarbinnen specifieke toezichthoudende bevoegdheden worden verdeeld tussen de ECB en de deelnemende NBA's. Met name heeft de ECB tot taak de vergunningen van alle kredietinstellingen te verlenen en in te trekken. De ECB heeft ook onder meer tot taak toe te zien op de naleving van de relevante Uniewetgeving die prudentiële vereisten oplegt aan kredietinstellingen, met inbegrip van het vereiste om te beschikken over robuuste governanceregelingen, zoals deugdelijke risicobeheerprocessen en internecontrolemechanismen ([53]). Te dien einde worden alle

([41]) Zie artikel 11, lid 6, van de ontwerpverordening.
([42]) Zie artikel 3, lid 17, van de ontwerpverordening.
([43]) Zie artikel 76, lid 2, punt d) en e) van Gedelegeerde Verordening (EU) 2017/392 van de Commissie:
([44]) Zie artikel 78, leden 2 en 3, van Gedelegeerde Verordening (EU) 2017/392 van de Commissie: (EU) 2017/392.
([45]) Zie artikel 1, lid 4, van Verordening (EU) nr. 909/2014.
([46]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).
([47]) Zie artikel 18, lid 2, onder g) en h), van EMIR.
([48]) Zie artikel 4 en artikel 5, lid 4, van de ontwerpverordening en artikel 34, lid 3, van de CSD-verordening.
([49]) Zie artikel 53, lid 2, punt a), van de ontwerpverordening.
([50]) Zie artikel 34 van EMIR
([51]) Zie CPMI-IOSCO Principles for Financial Market Infrastructures, beschikbaar op de website van de Bank voor Internationale Betalingen onder www.bis.org.
([52]) Verordening (EU) nr. 1024/2013 van 15 oktober 2013 van de Raad 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).
([53]) Zie artikel 4, lid 1, punt e), en artikel 6, lid 4, van Verordening (EU) nr. 1024/2013.

toezichthoudende bevoegdheden aan de ECB toevertrouwd om te interveniëren in de activiteiten van kredietinstellingen die nodig zijn voor de uitoefening van haar taken. De ECB en de betrokken NBA's zijn derhalve de bevoegde autoriteiten die specifieke bevoegdheden op het gebied van prudentieel toezicht uitoefenen uit hoofde van Verordening 2013/575/EU van het Europees Parlement en de Raad ([54])(hierna de "Verordening kapitaalvereisten" genoemd) en Richtlijn 2013/36/EU van het Europees Parlement en de Raad ([55]) (hierna de "Richtlijn kapitaalvereisten" genoemd).

3.2 In de ontwerpverordening is bepaald dat het gemeenschappelijk rulebook en het toezichtsysteem verder moeten worden ontwikkeld om digitale operationele veerkracht en ICT-beveiliging te bestrijken, door de mandaten van financiële toezichthouders die belast zijn met het monitoren en beschermen van de financiële stabiliteit en de integriteit van de markt uit te breiden ([56]). Het doel is een alomvattend kader voor ICT- of operationele risico's te bevorderen door de harmonisatie van essentiële vereisten inzake digitale operationele veerkracht voor alle financiële entiteiten ([57]). De ontwerpverordening heeft met name tot doel ICT-risicovereisten die tot nu toe afzonderlijk in verschillende wetteksten ([58]) worden behandeld, te consolideren en te verbeteren.

3.3 De vereisten in verband met ICT-risico's voor de financiële sector zijn momenteel verspreid over een aantal rechtshandelingen van de Unie, waaronder de Richtlijn kapitaalvereisten en "soft law"-instrumenten (zoals EBA-richtsnoeren), en zijn divers en soms onvolledig. In sommige gevallen is het ICT-risico slechts impliciet aangepakt als onderdeel van het operationele risico, terwijl het in andere geval het helemaal niet is aangepakt. Dit moet worden verholpen door de ontwerpverordening en die handelingen op elkaar af te stemmen. Daartoe wordt in de ontwerpwijzigingsrichtlijn een reeks wijzigingen voorgesteld die noodzakelijk lijken om juridische duidelijkheid en consistentie te creëren met betrekking tot de toepassing van de verschillende vereisten inzake digitale operationele veerkracht. De wijzigingen in de Richtlijn kapitaalvereisten die momenteel in de ontwerpwijzigingsrichtlijn worden voorgesteld ([59]), verwijzen echter alleen naar de bepalingen inzake nood- en bedrijfscontinuïteitsplannen ([60]), aangezien zij naar verluidt impliciet dienen als basis voor ICT-risicobeheer.

3.4 Voorts bepaalt de ontwerpverordening ([61]) dat financiële entiteiten, met inbegrip van kredietinstellingen, beschikken over interne governance- en controlekaders die een doeltreffend en prudent beheer van alle ICT-risico's garanderen. De ontwerpverordening ([62]) voorziet in de toepassing op individueel en geconsolideerd niveau van de daarin vastgestelde vereisten, maar zonder voldoende coördinatie met sectorspecifieke wetgeving waarnaar verwezen wordt. Tot slot wordt in de ontwerpverordening ([63]) bepaald dat, onverminderd de bepalingen inzake het toezichtskader voor cruciale derde aanbieders van ICT-diensten als bedoeld in de ontwerpverordening ([64]), de naleving van de daarin vervatte verplichtingen voor kredietinstellingen wordt gewaarborgd door de bevoegde autoriteit die is aangewezen overeenkomstig artikel 4 van de richtlijn kapitaalvereisten, onverminderd de specifieke taken die bij de GTM-verordening aan de ECB zijn opgedragen.

3.5 In het licht van het voorgaande begrijpt de ECB dat de ontwerpverordening met betrekking tot kredietinstellingen, zulks met uitzondering van de bepalingen van de ontwerpverordening betreffende het toezichtkader voor cruciale derde aanbieders van ICT-diensten ([65]), beoogt een prudentieel intern governancekader voor het beheer van ICT-risico's vast te stellen dat zal worden geïntegreerd in het algemene interne governancekader onder de Richtlijn kapitaalvereisten Bovendien zullen, gezien de prudentiële aard van het voorgestelde kader, de bevoegde autoriteiten die verantwoordelijk zijn voor het toezicht op de naleving van de verplichtingen uit hoofde van het voorgestelde kader, met inbegrip van de ECB, de autoriteiten zijn die verantwoordelijk zijn voor het bankentoezicht overeenkomstig de GTM-verordening.

([54]) 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).

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

([56]) Zie overweging 8 van de ontwerpverordening.

([57]) Zie overweging 11 van de ontwerpverordening.

([58]) Zie overweging 12 van de ontwerpverordening.

([59]) Zie overwegingen 4 en 5 van de ontwerpwijzigingsrichtlijn.

([60]) Zie artikel 85 van de Richtlijn kapitaalvereisten.

([61]) Zie artikel 4, lid 1, van de ontwerpverordening.

([62]) Zie artikel 25, leden 3 en 4, van de ontwerpverordening.

([63]) Zie Artikel 41 van de ontwerpverordening

([64]) Zie hoofdstuk V, afdeling II, van de ontwerpverordening.

([65]) Zie hoofdstuk V, afdeling II, van de ontwerpverordening.

3.6 De wetgevende organen van de Unie kunnen derhalve de volgende suggesties in overweging nemen om de duidelijkheid en de coördinatie tussen de ontwerpverordening en de richtlijn kapitaalvereisten te vergroten. Ten eerste kunnen de vereisten van de ontwerpverordening uitdrukkelijk als prudentieel worden aangemerkt, zoals onder meer in de CSD-verordening ([66]) is gebeurd. Ten tweede zou de formulering van de overwegingen van de ontwerpwijzigingsrichtlijn ([67]) kunnen worden verruimd, aangezien de vereisten van de ontwerpverordening verder gaan dan de enige fase van nood- en bedrijfscontinuïteitsplannen. ICT-risicobeheersmaatregelen vallen in het algemeen onder het meer algemene toepassingsgebied van solide governanceregelingen uit hoofde van artikel 74 van de richtlijn kapitaalvereisten ([68]). Ten derde moet de ontwerpverordening ([69]) worden gewijzigd om in de overwegingen de bevoegdheid van de ECB voor het prudentieel toezicht op kredietinstellingen uit hoofde van het Verdrag en de GTM-verordening in herinnering te brengen. Ten vierde moet de verwijzing naar de toepassing op individueel en geconsolideerd niveau van de daarin opgenomen vereisten ([70]) worden herzien, aangezien de gesubconsolideerde en geconsolideerde niveaus in de ontwerpverordening niet zijn gedefinieerd en bepaalde typen intermediairs niet onderworpen zijn aan geconsolideerd toezicht uit hoofde van de desbetreffende wetgeving (bv. betalingsinstellingen). Bovendien mag het toepassingsniveau van de vereisten in de ontwerpverordening uitsluitend voortvloeien uit de wetgeving die op elk type financiële entiteit van toepassing is. In het geval van kredietinstellingen wordt gezorgd voor een duidelijk verband tussen de richtlijn kapitaalvereisten en de ontwerpverordening, zodat de vereisten van de ontwerpverordening automatisch van toepassing zijn op individueel, gesubconsolideerd of geconsolideerd niveau ([71]), naargelang het geval. Tot slot zouden de wetgevingsorganen van de Unie kunnen overwegen om te voorzien in een overgangsregeling voor het beheer van de periode tussen de inwerkingtreding van de ontwerpverordening en de inwerkingtreding van de in de ontwerpverordening beoogde technische reguleringsnormen, aangezien sommige intermediairs, waaronder kredietinstellingen, reeds onderworpen zijn aan regels inzake ICT-risico's die van toepassing zijn op specifieke sectoren en gedetailleerder zijn dan de algemene bepalingen van de ontwerpverordening.

3.7 De ECB is in het kader van de GTM-verordening belast met de taak ervoor te zorgen dat kredietinstellingen voldoen aan de vereisten van het Unierecht die kredietinstellingen verplichten te beschikken over solide risicobeheerprocessen en interne controlemechanismen ([72]) Dit betekent dat de ECB ervoor moet zorgen dat instellingen beleidslijnen en procedures toepassen om de blootstelling aan operationeel risico, met inbegrip van modelrisico, te beoordelen en te beheren en zelden voorkomende, zeer ernstige gebeurtenissen af te dekken. Kredietinstellingen omschrijven nader wat voor de toepassing van deze beleidslijnen en procedures onder operationeel risico wordt verstaan ([73]).

3.8 In juli 2017 heeft de Raad van bestuur van de Europese Centrale Bank (ECB) op basis van een ontwerpvoorstel van de raad van toezicht overeenkomstig artikel 26, lid 8, en artikel 6, lid 2, van de GTM-verordening en artikel 21, lid 1, van Verordening (EU) nr. 468/2014 van de Europese Centrale Bank (ECB/2014/17) ([74]) het GTM *Cyber Incident Reporting Framework* (cyberincidentrapportagekader, hierna de "kaderregeling" genoemd) vastgesteld. Het kader bestaat uit een bindend verzoek (individuele besluiten gericht aan kredietinstellingen) om informatie en/of rapportage op basis van artikel 10 van de GTM-verordening ([75]). Sommige landen beschikken al over een incidentenmeldingsproces, waarbij kredietinstellingen verplicht worden alle significante cyberincidenten aan hun NBA's te melden. In die landen zullen belangrijke kredietinstellingen incidenten nog steeds rapporteren aan de NBA's, die deze vervolgens zonder onnodige vertraging doorzenden aan de ECB namens de onder toezicht staande

([66]) Zie titel van hoofdstuk II, afdeling 4, "Prudentiële vereisten" van de CSD-verordening.
([67]) Zie overweging 4 van de ontwerpwijzigingsrichtlijn.
([68]) Artikel 85 van Richtlijn 2013/36/EU is slechts een specificatie. Zie in dit verband ook de bladzijden 4, 11 en 37 van de richtsnoeren van de Europese Bankautoriteit van 29 november 2019 (hierna de "EBA-richtsnoeren" genoemd), waarin artikel 74 van Richtlijn 2013/36/EU als uitdrukkelijke rechtsgrondslag worden genoemd.
([69]) Zie artikel 41, lid 1, van de ontwerpverordening.
([70]) Zie Artikel 25, leden 3 en 4 van de ontwerpverordening
([71]) Zie ook artikel 109 van de Richtlijn kapitaalvereisten.
([72]) Zie artikel 4, lid 1, punt e), van de GTM-verordening.
([73]) Zie artikel 85 van de Richtlijn kapitaalvereisten.
([74]) Verordening (EU) nr. 468/2014 van de Europese Centrale Bank van 16 april 2014 tot vaststelling van een kader voor samenwerking binnen het Gemeenschappelijk Toezichtsmechanisme tussen de Europese Centrale Bank en nationale bevoegde autoriteiten en met nationale aangewezen autoriteiten (GTM-kaderverordening)(ECB/2014/17) (PB L 141 van 14.5.2014, blz. 1).
([75]) In het bijzonder moet een cyberincident (een vastgestelde mogelijke inbreuk op de informatiebeveiliging, of het nu kwaadwillig of accidenteel is) aan de ECB worden gemeld indien aan ten minste een van de volgende voorwaarden is voldaan: 1) er is een potentiële financiële impact van 5 miljoen EUR of 0,1 % van het tier 1-kernkapitaal; 2) het incident wordt openbaar gemeld of veroorzaakt reputatieschade; 3) het incident is buiten de reguliere rapportage naar de Chief Information Officer geëscaleerd; 4) de bank heeft het incident gemeld aan het CERT/CSIRT, een beveiligingsinstantie of de politie; 5) procedures voor herstel na een ramp of bedrijfscontinuïteitsprocedures in gang zijn gezet of een aanvraag voor een cyberverzekering is ingediend; 6) er is sprake van een inbreuk op wettelijke of bestuursrechtelijke voorschriften; of 7) de bank maakt gebruik van interne criteria en het oordeel van deskundigen (met inbegrip van een mogelijk systeemeffect) en besluit de ECB te informeren.

entiteiten. Daarom zijn de bovengenoemde besluiten ook gericht tot deze nationale bevoegde autoriteiten om deze informatie op basis van het kader aan de ECB door te zenden. De ECB steunt de inspanningen van de wetgevingsorganen van de Unie om harmonisatie en stroomlijning te bevorderen, onder meer met betrekking tot de reeks regels en verplichtingen die van toepassing zijn op kredietinstellingen inzake incidentenmelding. In het licht hiervan is de ECB bereid om het kader waar nodig in het licht van de uiteindelijke vaststelling van de ontwerpverordening te wijzigen (en eventueel in te trekken).

4. **Specifieke opmerkingen over ICT-risicobeheer, melding van incidenten, testen van operationele veerkracht en ICT-risico van**

4.1 *ICT-risicobeheer*

4.1.1 De ECB is ingenomen met de invoering in de ontwerpverordening van een solide en alomvattend kader voor ICT-risicobeheer dat de CPMI-IOSCO Richtsnoeren inzake cyberveerkracht omvat en nauw aansluit bij de beste praktijken, waaronder de Verwachtingen inzake cyberveerkracht voor FMI's van het Eurosysteem (*Eurosystem Cyber Resilience Oversight Expectations for FMI's)*.

4.1.2 De ECB steunt de notie dat financiële entiteiten risicobeoordelingen moeten uitvoeren bij elke "grote verandering" in de infrastructuur van het netwerk en het informatiesysteem ([76]). Dit gezegd zijnde, bevat de ontwerpverordening geen definitie van "grote verandering", waardoor onwelkome ruimte ontstaat voor uiteenlopende interpretaties door financiële entiteiten, hetgeen uiteindelijk de harmonisatiedoelstellingen van de ontwerpverordening zou kunnen belemmeren. Met het oog op de rechtszekerheid kunnen de wetgevingsorganen van de Unie overwegen een definitie van "grote verandering" in de ontwerpverordening op te nemen.

4.1.3 De ECB steunt in het algemeen het idee dat andere financiële entiteiten dan micro-ondernemingen relevante kosten en verliezen als gevolg van ICT-verstoringen en ICT-gerelateerde incidenten rapporteren aan de bevoegde autoriteiten ([77]). Om de algehele doeltreffendheid van het systeem te waarborgen en om te voorkomen dat de bevoegde autoriteiten en de financiële entiteiten worden overstelpt met een buitensporig aantal rapporten, zou de invoering van relevante drempels, mogelijk van kwantitatieve aard, door de wetgevingsorganen van de Unie nuttig kunnen worden onderzocht.

4.1.4 De ECB erkent de mogelijkheid dat financiële entiteiten, na goedkeuring door de bevoegde autoriteiten, aan intragroep- of externe ondernemingen de taak delegeren om te controleren of aan de vereisten inzake ICT-risicobeheer wordt voldaan ([78]). Tegelijkertijd is het belangrijk dat de wetgevingsorganen van de Unie verduidelijken hoe de goedkeuring door de bevoegde autoriteiten zou worden verleend in de gevallen waarin een financiële entiteit aan meerdere bevoegde autoriteiten is onderworpen. Dit kan het geval zijn wanneer een financiële entiteit een kredietinstelling, een aanbieder van cryptoactivadiensten en/of een betalingsdienstaanbieder is. Met betrekking tot de door financiële entiteiten uit hoofde van de ontwerpverordening uit te voeren identificatie en classificatie zou de ECB het met het oog op de classificatie van activa prudent achten dat de ontwerpverordening ([79]) ook zou voorschrijven dat financiële entiteiten rekening houden met het cruciale karakter van dergelijke activa (d.w.z. of zij cruciale functies ondersteunen).

4.2 *Melding van incidenten*

4.2.1 De ECB is ingenomen met de in de ontwerpverordening geschetste inspanningen om het landschap voor de melding van ICT-incidenten binnen de Unie te harmoniseren en te streven naar een gecentraliseerde melding van ernstige ICT-gerelateerde incidenten ([80]). De invoering van een geharmoniseerd kader voor de melding van ernstige ICT-gerelateerde incidenten ([81]) aan de betrokken bevoegde autoriteiten zou in beginsel de rapportagelast van financiële entiteiten, met inbegrip van kredietinstellingen, stroomlijnen en harmoniseren. De bevoegde autoriteiten zouden baat hebben bij het bredere scala van bestreken incidenten, dat verder gaat dan cybergerelateerde incidenten die momenteel onder de huidige kaders ([82]) vallen. De toekomstige vaststelling van de ontwerpverordening vereist een herziening en mogelijke intrekking van bestaande kaders, met inbegrip van het GTM *Cyber Incident Reporting Framework*. Dat gezegd hebbend is het met het oog op een echte stroomlijning en volledige afstemming tussen alle kaders van cruciaal belang om ervoor te zorgen dat het toepassingsgebied van de bepalingen inzake incidentenmelding in het kader van de ontwerpverordening, met inbegrip van alle relevante definities, drempels en

([76]) Zie artikel 7, lid 3, van de ontwerpverordening.
([77]) Zie artikel 10, lid 9, van de ontwerpverordening.
([78]) Zie artikel 5, lid 10, van de ontwerpverordening.
([79]) Zie Artikel 7 van de ontwerpverordening.
([80]) Zie Artikel 19 van de ontwerpverordening.
([81]) Zie artikel 3, lid 7 en de artikelen 17 en 18 van de ontwerpverordening.
([82]) Zie bijvoorbeeld de kaderregeling.

rapportageparameters, volledig wordt afgestemd op de relevante kaders. Het is met name van het grootste belang te zorgen voor afstemming tussen enerzijds de ontwerpverordening en anderzijds Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad ([83]) (hierna "PSD2" genoemd) en de EBA-richtsnoeren voor de melding van grote incidenten (hierna de "EBA-richtsnoeren" genoemd). De ontwerpwijzigingsrichtlijn ([84]) bevat wijzigingen van de PSD2 met betrekking tot de afbakening van de melding van incidenten tussen de ontwerpverordening en de PSD2, die voornamelijk gevolgen zou hebben voor betalingsdienstaanbieders, die ook een vergunninghoudende kredietinstelling zijn, en voor de bevoegde autoriteiten. Er is onduidelijkheid over de procedure voor de melding van incidenten en er is een mogelijke overlapping tussen sommige incidenten die moeten worden gemeld uit hoofde van zowel de ontwerpverordening als de EBA-richtsnoeren.

4.2.2 De procedures voor het melden van ernstige incidenten in het kader van respectievelijk de ontwerpverordening ([85]), de PSD2 en de overeenkomstige EBA-richtsnoeren zouden betalingsdienstaanbieders ertoe verplichten een incidentenmelding in te dienen bij hun respectieve bevoegde autoriteit zodra het incident is geclassificeerd. In eerste verslagen wordt immers niet ingegaan op de essentie, de oorzaak of het functionele gebied waarop het incident betrekking heeft, en kunnen betalingsdienstaanbieders pas in een later stadium een dergelijk onderscheid maken, wanneer meer gedetailleerde informatie over het incident beschikbaar komt. Als gevolg daarvan kunnen initiële incidentverslagen worden ingediend in het kader van zowel de ontwerpverordening als de EBA-richtsnoeren, of kunnen betalingsdienstaanbieders besluiten tot één enkel rapportagekader en de indiening ervan op een latere datum corrigeren. Dezelfde onzekerheid (bijvoorbeeld met betrekking tot de onderliggende oorzaak van een incident) kan ook tot uiting komen in tussentijdse en eindverslagen. Dit zou de mogelijkheid van parallelle indiening van verslagen bij de bevoegde autoriteiten in het kader van de ontwerpverordening en de PSD2 opnieuw vergroten.

4.2.3 Sommige incidenten die als ICT-gerelateerde incidenten kunnen worden aangemerkt, kunnen ook gevolgen hebben voor andere gebieden en moeten bijgevolg worden gemeld uit hoofde van de EBA-richtsnoeren. Dit kan het geval zijn wanneer een incident gevolgen heeft vanuit ICT-oogpunt, maar tegelijkertijd ook van invloed is geweest op het aanbieden van betalingsdiensten en/of andere niet-ICT-functionele gebieden of kanalen. Bovendien kunnen er gevallen zijn waarin het niet mogelijk is een onderscheid te maken tussen operationele en ICT-gerelateerde incidenten. Bovendien zou dezelfde entiteit, wanneer dezelfde financiële entiteit een belangrijke kredietinstelling en een betalingsdienstaanbieder is, op grond van de ontwerpverordening tweemaal het ICT-gerelateerde incident moeten melden en onderworpen zijn aan de twee bevoegde autoriteiten. In het licht van het voorgaande moet in de ontwerpverordening duidelijker worden aangegeven hoe de wisselwerking tussen PSD2 en de EBA-richtsnoeren in de praktijk moet werken. Belangrijker is dat het met het oog op de harmonisatie en stroomlijning van de rapportageverplichtingen van belang is dat de wetgevingsorganen van de Unie nadenken over resterende kwesties van dubbele rapportage, en dat wordt verduidelijkt of de ontwerpverordening, enerzijds, en de PSD2 en de EBA-richtsnoeren, anderzijds, naast elkaar zouden bestaan, dan wel of er één reeks vereisten voor incidentrapportage moet worden vastgesteld.

4.2.4. De ontwerpverordening verplicht de bevoegde autoriteiten ([86]) om na ontvangst van een melding de ontvangst ervan te bevestigen en de financiële entiteit zo snel mogelijk alle nodige feedback of richtsnoeren te verstrekken, met name om oplossingen op het niveau van de entiteit te bespreken of manieren te bespreken om de negatieve impact op alle sectoren tot een minimum te beperken. Dit zou betekenen dat de bevoegde autoriteiten actief moeten bijdragen aan het beheersen en verhelpen van incidenten en tegelijkertijd ook de reactie van een onder toezicht staande entiteit op kritieke incidenten moeten beoordelen. De ECB benadrukt dat de verantwoordelijkheid en verantwoording voor het herstel en de gevolgen van een incident uitsluitend en duidelijk bij de betrokken financiële entiteit moeten blijven. Daarom stelt de ECB voor om de feedback en richtsnoeren te beperken tot prudentiële feedback en richtsnoeren op hoog niveau. Als de feedback breder zou zijn, zou dit gespecialiseerde beroepsbeoefenaren met zeer aanzienlijke technische kennis vereisten die doorgaans niet beschikbaar is in de talentenpool waarover prudentiële autoriteiten beschikken.

4.3 *Testen van de digitale operationele veerkracht*

4.3.1 De ECB is ingenomen met de vereisten van de ontwerpverordening ([87]) betreffende het testen van digitale operationele veerkracht tussen financiële entiteiten en met de noodzaak van een eigen testprogramma voor elke instelling. In de ontwerpverordening ([88]) worden verschillende soorten tests beschreven als indicatie voor financiële entiteiten. De soorten tests zijn niet erg duidelijk en sommige tests, zoals compatibiliteitstests, vragenlijsten of

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

([84]) Zie artikel 7, lid 9, van de ontwerpwijzigingsrichtlijn.

([85]) Zie artikel 17, lid 3, van de ontwerpverordening.

([86]) Zie Artikel 20 van de ontwerpverordening

([87]) Zie de artikelen 21 en 22 van de ontwerpverordening.

([88]) Zie artikel 22, lid 1, van de ontwerpverordening.

scenariogebaseerde tests, zijn vatbaar voor interpretatie door ESA's, bevoegde autoriteiten of financiële entiteiten. Bovendien zijn er ook geen richtsnoeren voor de frequentie van elke test. Een mogelijke aanpak zou erin kunnen bestaan dat in de ontwerpverordening algemene testvoorschriften worden vastgesteld, met een nauwkeuriger beschrijving van de soorten tests die in technische regulerings- en uitvoeringsnormen uiteen worden gezet.

4.3.2 Dreigingsgestuurde penetratietests (*Threat-Led penetration testing* TLPT) zijn een krachtig instrument om beveiligingsbescherming en paraatheid te testen. Daarom moedigt de ECB TLPT door financiële entiteiten aan. Met dit instrument worden niet alleen technische maatregelen getest, maar ook personeel en processen. De resultaten van deze tests kunnen het beveiligingsbewustzijn van het hoger management binnen de geteste entiteiten aanzienlijk vergroten. Het Europees kader voor ethisch hacken op basis van infornatie over bedreigingen (*Threat Intelligence Based Ethical Red-teaming* - TIBER-EU) ([89]) en andere reeds beschikbare TLPT-instrumenten buiten de Unie zijn primaire instrumenten voor entiteiten om zelf hun houding en verdediging op het gebied van cyberveerkracht te beoordelen, te testen, uit te oefenen en te verbeteren.

4.3.3 In de meeste lidstaten waar TIBER-EU is geïmplementeerd, spelen toezichthouders geen actieve rol bij de tenuitvoerlegging van een lokaal TIBER-XX programma en bevindt het TIBER Cyberteam zich in bijna alle gevallen onafhankelijk van deze functies. Daarom moeten geavanceerde tests in het kader van de ontwerpverordening ([90]) door middel van TLPT worden uitgevoerd als instrument om het financiële ecosysteem te versterken en de financiële stabiliteit te vergroten in plaats van een louter toezichtsinstrument. Bovendien is er geen behoefte aan de ontwikkeling van een nieuw geavanceerd kader voor het testen van de cyberweerbaarheid, aangezien de lidstaten reeds op grote schaal TIBER-EU hebben aangenomen, het enige kader dat momenteel in de EU bestaat.

4.3.4 Eisen voor testers mogen niet worden opgenomen in het dispositief van de ontwerpverordening, aangezien de TLPT-gerelateerde sector zich nog steeds ontwikkelt en innovatie kan worden belemmerd door het opleggen van specifieke eisen. Niettemin is de ECB van mening dat, om een hoge mate van onafhankelijkheid bij het uitvoeren van tests te waarborgen, financiële entiteiten geen testers in dienst mogen nemen of aan mogen stellen die door financiële entiteiten in hun eigen groep in dienst zijn of aangesteld worden of anderszins in het bezit zijn van en/of onder zeggenschap staan van de te testen financiële entiteiten.

4.3.5 Om het risico op fragmentatie te beperken en harmonisatie te verzekeren, moet de ontwerpverordening één TLPT-kader opleggen dat van toepassing is op de financiële sector in de gehele Unie. Fragmentatie kan leiden tot hogere kosten en technische, operationele en financiële behoeften voor zowel bevoegde autoriteiten als financiële instellingen. Deze hogere kosten en vereisten kunnen uiteindelijk een negatief effect hebben op de wederzijdse erkenning van tests. Dit gebrek aan harmonisatie en de daaruit voortvloeiende problemen met wederzijdse erkenning zijn met name van cruciaal belang voor financiële entiteiten, die meerdere vergunningen kunnen hebben en/of actief kunnen zijn in meerdere rechtsgebieden in de gehele Unie. De technische regulerings- en uitvoeringsnormen, die in het kader van de ontwerpverordening voor TLPT moeten worden opgesteld, moeten in overeenstemming zijn met TIBER-EU. Voorts verwelkomt de ECB de mogelijkheid om in samenwerking met de ETA's te worden betrokken bij de voorbereiding van deze technische regulerings- en uitvoeringsnormen.

4.3.6 De actieve betrokkenheid van de bevoegde autoriteiten bij de tests kan leiden tot een mogelijk belangenconflict met de andere functie die zij vervullen, namelijk het beoordelen van het testkader van de financiële entiteit. Tegen deze achtergrond stelt de ECB voor om elke verplichting voor bevoegde autoriteiten met betrekking tot de validering van documenten en de afgifte van een attest voor een TLPT-test uit de ontwerpverordening te schrappen.

4.4 ICT-risico van derde-aanbieders

4.4.1 De ECB is ingenomen met de invoering van een uitgebreide reeks kernbeginselen en een solide toezichtkader voor het identificeren en beheren van ICT-risico's die voortkomen uit derde aanbieders van ICT-diensten, ongeacht of deze tot dezelfde groep van financiële entiteiten behoren. Niettemin is het met het oog op een doeltreffende identificatie en beheer van ICT-risico's van belang dat onder meer cruciale derde aanbieders van ICT-diensten correct worden geïdentificeerd en geclassificeerd. Hoewel de invoering van gedelegeerde handelingen ([91]) ter aanvulling van de criteria voor classificatiedoeleinden wordt toegejuicht ([92]), dient de ECB voorafgaand aan de vaststelling van dergelijke gedelegeerde handelingen te worden geraadpleegd.

([89]) Beschikbaar op de ECB-website onder www.ecb.europa.eu.
([90]) Artikelen 23 en 24 van de ontwerpverordening.
([91]) Zie artikel 28, lid 3, van de ontwerpverordening.
([92]) Zie artikel 28, lid 2, van de ontwerpverordening.

4.4.2 Wat de structuur van het toezichtkader ([93]) betreft, moet de rol van het Gemengd Comité verder worden verduidelijkt. Tegelijkertijd is de ECB ingenomen met haar opname als waarnemer in het toezichtforum (*Oversight Forum*), aangezien deze rol de ECB dezelfde toegang tot documentatie en informatie zal bieden als stemgerechtigde leden ([94]). De ECB vestigt de aandacht van de wetgevende organen van de Unie op het feit dat de ECB in haar hoedanigheid van waarnemer zou willen bijdragen aan de werkzaamheden van het toezichtforum, zowel vanuit haar rol als centrale bank van uitgifte, welke verantwoordelijk is voor het toezicht op de marktinfrastructuren, als prudentiële toezichthouder op kredietinstellingen. Daarnaast merkt de ECB op dat de ECB niet alleen waarnemer is in het toezichtforum maar ook als bevoegde autoriteit deel zou uitmaken van het gezamenlijke onderzoeksteam. In dit verband zou door de wetgevingsorganen van de Unie verder kunnen worden nagedacht over de samenstelling van de gezamenlijke onderzoeksteams ([95]) om te zorgen voor een passende betrokkenheid van de relevante bevoegde autoriteiten. Evenzo is de ECB van mening dat het maximumaantal deelnemers aan de gezamenlijke onderzoeksteams moet worden verhoogd, rekening houdend met het kritieke belang, de complexiteit en de reikwijdte van derde aanbieders van ICT-diensten.

4.4.3 De ECB merkt op dat volgens de ontwerpverordening de leidende toezichthouder kan verhinderen dat cruciale derde aanbieders van ICT-diensten verdere uitbestedingsregelingen treffen wanneer i) de beoogde onderaannemer een in een derde land gevestigde aanbieder van ICT-diensten of een ICT-subcontractant is en ii) de uitbesteding een cruciale of belangrijke functie van de financiële entiteit betreft. De ECB wenst te benadrukken dat deze bevoegdheden alleen door de hoofdautoriteit kunnen worden uitgeoefend in het kader van onderaannemingsovereenkomsten waarbij een cruciale derde aanbieder van ICT-diensten een cruciale of belangrijke functie uitbesteedt aan een afzonderlijke juridische entiteit die in een derde land is gevestigd. De ECB begrijpt dat de leidende toezichthouder geen vergelijkbare bevoegdheden kan uitoefenen om te voorkomen dat een cruciale derde aanbieder van ICT-diensten cruciale of belangrijke functies van de financiële entiteit uitbesteedt aan faciliteiten van die dienstverlener die zich in een derde land bevinden. Het kan bijvoorbeeld zo zijn dat vanuit operationeel oogpunt cruciale gegevens en/of informatie kunnen worden opgeslagen of verwerkt door buiten de Europese Economische Ruimte (EER) gelegen faciliteiten. In een dergelijk geval kunnen de bevoegdheden van de leidende toezichthouder de bevoegde autoriteiten niet voldoende machtigen om toegang te krijgen tot alle informatie, gebouwen, infrastructuur en personeel die relevant zijn voor de uitvoering van alle cruciale of belangrijke functies van de financiële entiteit. Om ervoor te zorgen dat de bevoegde autoriteiten hun taken ongehinderd kunnen uitvoeren, stelt de ECB voor dat aan de leidende toezichthouder de bevoegdheid moet worden toegekend om ook het gebruik van buiten de EER gevestigde derde aanbieders van ICT-diensten te beperken. Deze bevoegdheid kan worden uitgeoefend in specifieke gevallen waarin er geen administratieve regelingen zijn getroffen met de betrokken autoriteiten van derde landen, zoals bepaald in de ontwerpverordening ([96]), of wanneer de vertegenwoordigers van de cruciale derde aanbieders van ICT-diensten in het kader van het betrokken derde land onvoldoende waarborgen bieden met betrekking tot de toegang tot de informatie, gebouwen, infrastructuur en personeel die nodig zijn om oversight- of toezichtstaken uit te voeren.

4.4.4 Tot slot zou de verplichting van de bevoegde autoriteiten om gevolg te geven aan de aanbevelingen van de leidende toezichthouder ([97]) ondoeltreffend kunnen blijken, aangezien de bevoegde autoriteiten mogelijk geen holistische kijk hebben op de risico's die worden gegenereerd door elke cruciale derde aanbieder van ICT-diensten. Daarnaast kan van de bevoegde autoriteiten worden verlangd dat zij maatregelen nemen tegen onder hun toezicht staande financiële entiteiten wanneer de aanbevelingen niet worden opgevolgd door de cruciale derde aanbieders van diensten. Op grond van de ontwerpverordening ([98]) kunnen de bevoegde autoriteiten van hun onder toezicht staande financiële entiteiten verlangen dat zij de cruciale dienst van een derde aanbieder tijdelijk opschorten of uitstaande contracten met derde aanbieders van kritieke diensten beëindigen. Het is moeilijk om het beoogde follow-upproces te vertalen in concrete acties. Het is met name niet duidelijk of een onder toezicht staande financiële entiteit in staat zal zijn een contract met een cruciale derde aanbieder van diensten op te schorten of te beëindigen. De reden hiervoor is dat cruciale derde aanbieder van ICT-diensten een belangrijke aanbieder voor die financiële entiteit zou kunnen zijn, of vanwege de kosten en schade, contractueel of anderszins, die de financiële entiteit kan lijden als gevolg van een dergelijke opschorting of beëindiging. Bovendien ondersteunt deze benadering de convergentie van het toezicht niet, aangezien de bevoegde autoriteiten dezelfde aanbeveling op uiteenlopende wijze kunnen interpreteren. Dit zou uiteindelijk een belemmering kunnen vormen voor de beoogde harmonisatie en consistente aanpak bij de monitoring van kritieke ICT-risico's van derde aanbieders op het niveau van de Unie. In het licht van het voorgaande kunnen de wetgevingsorganen van de Unie overwegen om de juridische toezichthouders specifieke handhavingsbevoegdheden toe te kennen ten aanzien van cruciale derde aanbieders van ICT-diensten, rekening houdend met de beperkingen die door de *Meroni*-doctrine zijn opgelegd, zoals gedeeltelijk door het Hof van Justitie in zijn arrest in de ESMA-zaak is afgezwakt ([99]).

([93]) Zie Artikel 29 van de ontwerpverordening.
([94]) Zie artikel 29, lid 3, van de ontwerpverordening.
([95]) Zie Artikel 35 van de ontwerpverordening
([96]) Zie artikel 39, lid 1, van de ontwerpverordening.
([97]) Zie Artikel 29, lid 4 en artikel 37 van de ontwerpverordening
([98]) Zie artikel 37, lid 3, van de ontwerpverordening.
([99]) Zie het arrest van het Hof (grote kamer) van 22 januari 2014, Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland/Raad van de Europese Unie, Europees Parlement inzake Verordening (EU) nr 236/2012 - zaak C-270/12.

Wanneer de ECB wijzigingen van het voorstel aanbeveelt, worden daartoe in een apart technisch werkdocument specifiek onderbouwde formuleringsvoorstellen opgenomen. Het technische werkdocument is in de Engelse taal beschikbaar op EUR-Lex.

Gedaan te Frankfurt am Main, 4 juni 2021.

De president van de ECB
Christine LAGARDE