Systemische dimensies van de regulering van ICT-risico's in de Digital Operational Resilience Act (DORA)

mr. dr. J.P. Broekhuizen en mr. L.C. Brederveld[1]

Met de invoering van DORA vervlechten zich bredere doelstellingen van (ICT-)risicobeheer in belangrijke economische sectoren met de doelstellingen van financiële regulering. Hierdoor wordt de nauwe onderlinge verwevenheid tussen de financiële sector en de bredere economie waar het betreft ICT meer uitdrukkelijk gethematiseerd in het financieel recht. Deze systemische perspectieven, die DORA niet alleen meegeeft aan toezichthouders, maar ook aan financiële instellingen en ICT-dienstverleners vraagt mee te nemen in verschillende afwegingen in het kader van het ICT-risicobeheer, staan in dit artikel centraal. We behandelen dit aan de hand van een aantal aspecten van DORA waarin deze perspectieven een rol spelen, zoals bij het bepalen of sprake is van een "kritieke of belangrijke functie" of van een "ICT-concentratierisico", bij de invulling van de testprogramma's waarmee een financiële instelling haar digitale operationele weerbaarheid dient te toetsen, en in de afwegingen die toezichthouders dienen te maken bij het aanwijzen van "kritieke derde aanbieders van ICT-diensten" die met DORA onder rechtstreeks toezicht komen te staan als onderdeel van het oversightkader dat met DORA wordt ingevoerd.

1. Inleiding

ICT is niet meer weg te denken uit de samenleving en onze dagelijkse activiteiten. Het houdt belangrijke sectoren van de economie draaiende, waaronder de financiële sector. Meer digitalisering en onderlinge verwevenheid vergroten echter ook onze afhankelijkheid van ICT, waardoor de samenleving als geheel, en het financiële stelsel in het bijzonder, kwetsbaarder wordt voor cyberdreigingen en ICT-verstoringen.[2] De *Digital Operational Resilience Act* ("**DORA**"[3]) wil deze ICT-risico's (verder) inbakenen. Met deze verordening beoogt de Europese wetgever de digitale weerbaarheid van de financiële sector te verhogen door strengere eisen te stellen aan financiële instellingen in het kader van, onder meer, ICT-risicobeheer en rapportage van ICT-gerelateerde incidenten.

Met dit doel wil DORA het bestaande, over Europese en nationale regelingen versnipperde regelgevend kader op het gebied van (ICT)-risicobeheer[4] harmoniseren en tegelijk ook consolideren en verbeteren, waaronder door inconsistenties in bestaande wet- en regelgeving (bijvoorbeeld in de gebruikte terminologie) op te lossen, helderheid aan te brengen in overlappingen en lacunes te dichten.[5] Daartoe heeft de Europese wetgever de vorm van een verordening

1. Jan Broekhuizen en Laura Brederveld zijn advocaten bij Kennedy Van der Laan te Amsterdam.
2. Overweging 1 DORA (zie volgende voetnoot).
3. Verordening (EU) 2022/2554 van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (PbEU 2022, L 333/1).
4. Waaronder de ICBE-richtlijn (20009/65/EG), de AIFM-richtlijn (2011/61/EU), de CRD-richtlijn (2013/36/EU), MiFID II (2014/65/EU), PSD2 (2015/2366/EU), BRRD (2014/59/EU), de Solvency II Richtlijn (2009/138/EG), Gedelegeerde Verordening Solvency II (EU/2015/35), de ESMA richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten (ESMA50-164-4285 NL), de EBA richtsnoeren inzake interne governance (EBA/GL/2019/02), EBA richtsnoeren inzake ICT en risicobeheer op gebeid van veiligheid (EBA/GL/2019/04), de EBA Richtsnoeren inzake uitbesteding (EBA/GL/2019/02), de EIOPA richtsnoeren voor het governancesysteem (Eiopa-BoS-14/253), de EIOPA richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie (EIOPA-BoS-20/600), de EIOPA richtsnoeren voor uitbesteding aan aanbieders van clouddiensten (EIOPA-BoS-20-002), Wft, Bpr, Bgpr, de Good Practice Informatiebeveiliging 2019/2020 en de Good Practice uitbesteding door verzekeraars van DNB.
5. Zie onder meer overwegingen 10 en 12 DORA. Hier komen ook andere doelstellingen in het spel dan het vergroten van digitale weerbaarheid. Bijvoorbeeld het wegnemen van regulatoire obstakels voor instellingen om grensoverschrijdend diensten te kunnen verlenen en daarmee het faciliteren van de goede werking van de Europese interne markt.

gekozen, en daarmee voor rechtstreeks werkende regels die niet eerst in nationale wetgeving hoeven te worden geïmplementeerd.

DORA maakt daarbij niet alleen onderdeel uit van een bredere Digital Finance Strategy van de Europese Commissie,[6] maar ook van een raamwerk van ICT-regulering met een ruimer bereik dan alleen de financiële sector[7] Zo is DORA bijvoorbeeld een *lex specialis* van de Netwerk en Informatiebeveiligingsrichtlijn[8] ("**NIS 2**"), een horizontaal cybersecurity raamwerk dat geldt voor (inmiddels) een breed scala aan sectoren zoals - naast het bankwezen en de infrastructuur voor financiële markten, de energie-, vervoers-, gezondheidszorg- en levensmiddelensector. In tegenstelling tot de regels uit DORA dienen de bepalingen uit NIS 2 nog wel te worden ingevoegd in nationale wet- en regelgeving. Bovendien strekt DORA, naast dat het strengere vereisten bevat voor de financiële entiteiten die al onder toepassingsbereik van bestaande regelgeving op dit vlak vielen, zich nu ook uit tot ICT-dienstverleners, zoals blijkt uit het feit dat zij deze zelfstandig als addressaat van de verordening worden genoemd,[9] en waarvan enkele – de zogenoemde "kritieke derde aanbieders van ICT-diensten" - met DORA zelfs onder een vorm van rechtstreeks (financieel) toezicht komen te staan.

Met de invoering van DORA vervlechten zich daarmee bredere doelstellingen van (ICT-)risicobeheer in belangrijke economische sectoren met de doelstellingen van financiële regulering. Hierdoor wordt de nauwe onderlinge verwevenheid tussen de financiële sector en de bredere economie waar het betreft ICT meer uitdrukkelijk gethematiseerd in het financieel recht. Deze systemische perspectieven die DORA, niet alleen aan toezichthouders meegeeft, maar ook aan financiële instellingen en ICT-dienstverleners vraagt mee te nemen in verschillende afwegingen in het kader van ICT-risicobeheer, staan in dit artikel centraal. We behandelen dit aan de hand van een aantal aspecten van DORA waarin deze perspectieven een rol spelen, zoals bij het bepalen of sprake is van een "kritieke of belangrijke functie" (paragraaf 4) of van een "ICT-concentratierisico" (paragaaf 6), bij de invulling van de testprogramma's waarmee een financiële instelling haar digitale operationele weerbaarheid dient te toetsen (paragraaf 5), en in de afwegingen die toezichthouders dienen te maken bij het aanwijzen van "kritieke derde aanbieders van ICT-diensten" die met DORA onder rechtstreeks toezicht komen te staan als onderdeel van het oversightkader dat met DORA wordt ingevoerd (paragraaf 7).

Eerst bespreken we enkele basisbegrippen van DORA: wanneer is er sprake van "ICT-risico" en wat wordt in DORA precies verstaan onder "ICT-diensten" (paragraaf 2). Ook staan we stil bij het evenredigheids- of proportionaliteitsbeginsel in DORA (paragraaf 3).

2. ICT-risico en ICT-diensten

DORA beoogt het ICT-risico van financiële instellingen op individueel niveau en van de financiële sector als geheel in te bakenen door het stellen van uniforme vereisten voor ICT-risicobeheer, rapportage van incidenten, het testen van de operationele weerbaarheid en het monitoren van ICT-risico bij het inschakelen van derde aanbieders van ICT-diensten. Dit is cruciaal voor de financiële stabiliteit en marktintegriteit in het digitale tijdperk en niet minder belangrijk dan bijvoorbeeld gemeenschappelijke prudentiële of marktgedragsnormen, zo is in dit verband te lezen in de overwegingen van deze verordening.[10] De regulering van (risico's verbonden aan) ICT, het gebruik van ICT-systemen en, in bredere zin, netwerk- en informatiesystemen,[11] voegt zich - naast prudentiële normen en gedragsregels - met DORA dan ook meer expliciet als derde-pijler toe aan de fundamenten van het financieel recht.

Onder "ICT-risico" wordt in DORA in dit verband verstaan iedere omstandigheid die zich voordoet bij het gebruik van netwerk- en informatiesystemen die gevaren oplevert voor onder meer de beveiliging van de systemen of de processen van de financiële instelling of van de levering van (financiële) diensten, met schadelijke effecten in hetzij de digitale omgeving, hetzij de fysieke omgeving,[12] met als gevolg dat de samenleving als geheel en het financiële stelsel in het bijzonder kwetsbaarder wordt voor cyberdreigingen en ICT-verstoringen.[13] Dit ICT-risico kan ook ontstaan door gebruik van ICT-diensten van derde aanbieders of hun onderaannemers.

6. European Commissie – Digital Finance Package, 24 september 2020.
7. Waaronder de NIS 2-richtlijn (zie noot hierna), de Cyberbeveiligingsverordening (EU/2019/881), een voorstel voor een *Cyber Resilience Act* (COM/2022/454), een voorstel voor een AI-verordening (COM/2021/206), en de daarbij behorende conceptrichtlijn AI-aansprakelijkheid (COM/2022/496) en het voorstel tot herziening richtlijn productaansprakelijkheid (COM/2022/495).
8. Richtlijn (EU) 2022/2555 van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) 2022/2555/EU.
9. Artikel 2 onder u DORA.
10. Overweging 8 DORA.
11. Gedefinieerd in artikel 6 onder 1 NIS 2 als (i) elektronische communicatienetwerken, (ii) (groepen van onderling verbonden) apparaten die gebruikt worden voor de automatische verwerking van digitale gegevens en (iii) de digitale gegevens als zodanig die daarmee worden verwerkt.
12. Artikel 3 onder 5 DORA.
13. Overweging 1 DORA.

Waar de nadruk in het bestaande regelgevend kader dat ziet op (ICT-)risicobeheer en (ICT-)uitbesteding in de financiële sector vooral op het uitbestedingsbegrip lag,[14] worden in DORA "ICT-risico" en "ICT-diensten" als basisbegrippen gebruikt en gedefinieerd. Het begrip "uitbesteding" wordt – hoewel het in de lopende tekst van DORA wel gebruikt wordt - juist niet meer afzonderlijk gedefinieerd.

"ICT-diensten" wordt in DORA gedefinieerd als doorlopende digitale diensten of gegevensdiensten die via ICT-systemen aan één of meerdere interne of externe gebruikers worden verleend.[15] Daarbij kan bijvoorbeeld gedacht worden aan bepaalde cloudcomputingdiensten (denk aan standaardcloudapplicaties zoals Microsoft 365 en Google Drive, maar ook aan specifiek voor de instelling ontwikkelde of geconfigureerde ICT-toepassingen die door de ICT-leverancier aan de instelling beschikbaar worden gesteld), maar ook aan hardware die als dienst wordt geleverd (zoals servers, computers en printers die beschikbaar worden gesteld via een abonnementsmodel). Overweging 35 van DORA benadrukt dat ICT-diensten in de context van DORA breed moet worden opgevat, zodat DORA betrekking heeft op risico's die voortvloeien uit alle soorten ICT-diensten. Dit om een hoog niveau van digitale operationele weerbaarheid in de hele financiële sector te bereiken en om mee te kunnen bewegen met technologische ontwikkelingen.

Het gebruik van het ICT-dienstenbegrip in DORA ziet daarmee niet uitsluitend op relaties met "derde aanbieders van ICT-diensten" – nog los van de vraag of zo'n relatie onder het bestaande kader als uitbesteding zou kwalificeren - maar wordt ook gebruikt in het kader van het interne ICT-risicobeheer van de financiële instelling. Daaruit kan *a contrario* opgemaakt worden dat (ICT-)uitbesteding slechts een onderdeel vormt van het ICT-risico. Aangezien DORA verschillende aspecten van het ICT-risico beslaat, vormt het daarmee ook een aanvulling op – en niet een vervanging van – het voor uitbestedingen geldende sectorale financiële recht.

Daarbij dient te worden opgemerkt dat de geldende sectorale vereisten in de uitbestedingsrichtsnoeren van de Europese toezichthouders ESMA[16] en EIOPA[17] specifiek zijn uitgewerkt met oog op het uitbesteden van *clouddiensten*,[18] welk begrip een beperktere omvang kent dan ICT-diensten zoals bedoeld in DORA. Clouddiensten zijn immers een specifiek soort ICT-diensten, waarbij een ICT-oplossing via een netwerk - meestal internet - beschikbaar wordt gesteld en daarmee toegankelijk is vanaf verschillende locaties (denk aan cloudopslag voor bestanden). En dit terwijl artikel 30 van DORA, waarin minimumvereisten worden gesteld aan de inhoud van overeenkomsten tussen een financiële instelling en een ICT-dienstverlener, een codificatie lijkt te zijn van de in deze richtsnoeren vervatte vereisten aan uitbestedingsovereenkomsten. De vraag is dan ook of DORA en deze richtsnoeren naast elkaar zullen blijven bestaan. Met het oog op de met DORA beoogde consolidatie, ligt het in de rede dat deze richtsnoeren zullen worden ingetrokken of tenminste aangepast om consistentie te bereiken met DORA en de in DORA gebruikte terminologie.

Om te kwalificeren als ICT-diensten onder DORA moet het verder gaan om diensten die doorlopend worden geleverd, zoals blijkt uit de definitie. Wanneer sprake is van dit doorlopende karakter (bijvoorbeeld over welke (minimum)periode de diensten moeten worden geleverd) wordt daarbij in het midden gelaten, maar eenmalige leveringen of diensten, zoals eenmalige installatie of configuratie, zijn hierdoor in ieder geval uitgesloten van het toepassingsbereik van DORA.

Het vereiste van doorlopendheid is ook terug te vinden in het bestaande regelgevend kader. Zo moeten financiële instellingen die onder het toepassingsbereik van de uitbestedingsrichtsnoeren van EBA[19] vallen, bij hun beoordeling of sprake is van uitbesteding, meewegen of de uitbestede functie periodiek of doorlopend door de dienstverlener wordt verricht.[20] De uitbestedingsrichtsnoeren van EIOPA, die van toepassing zijn bij uitbesteding door verzekerings- of herverzekeringsondernemingen, bevatten een vergelijkbaar vereiste. In hun beoordeling of een overeenkomst met een aanbieder van clouddiensten als uitbesteding kwalificeert, moet worden onderzocht of de uitbestede operationele functie of activiteit (of een deel daarvan) herhaaldelijk of doorlopend wordt uitgevoerd.[21] Wat hieraan opvalt is dat het toepassingsbereik van het bestaande regelgevende kader

14. Zie ook paragraaf 4 hierna en de bijdrage van P. van Vliet in dit tijdschrift.
15. Artikel 3 onder 21 DORA.
16. ESMA richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten (ESMA50-164-4285 NL), ("**ESMA uitbestedingsrichtsnoeren**").
17. EIOPA richtsnoeren voor uitbesteding aan aanbieders van clouddiensten (EIOPA-BoS-20-002) ("**EIOPA uitbestedingsrichtsnoeren**").
18. Zoals van toepassing op onder meer vermogensbeheerders en beleggingsinstellingen in geval van ESMA en (her)verzekeraars in geval van EIOPA. De voorloper van de uitbestedingsrichtsnoeren van EBA (zie volgende noot) voor financiële instellingen zoals banken kende initieel ook een nadruk op cloudsourcing, maar in de huidige versie van de EBA-richtsnoeren voor uitbesteding is deze nadruk op clouddiensten losgelaten.
19. EBA Richtsnoeren inzake uitbesteding (EBA/GL/2019/02) ("**EBA uitbestedingsrichtsnoeren**").
20. Randnummer 26 EBA uitbestedingrichtsnoeren.
21. Randnummer 14 onder a EIOPA uitbestedingrichtsnoeren.

voor uitbesteding in dit opzicht juist een ruimer bereik van diensten kan omvatten (en DORA *a contrario* een beperkter bereik), aangezien ook het periodiek of herhaaldelijk (laten) uitvoeren van een functie of activiteit onder het toepassingsbereik van uitbesteding valt terwijl DORA alleen ziet op ICT-diensten die doorlopend geleverd worden.

DORA impliceert daarmee dat het moet gaan om diensten die onafgebroken worden geleverd. Dat is op zich ook niet gek bezien tegen de bredere, systemische doelstellingen van DORA, waartoe immers beoogd wordt de operationele integriteit en betrouwbaarheid van financiële instellingen op te bouwen, te waarborgen en te evalueren, door te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die de *permanente* verlening van financiële diensten en de kwaliteit ervan ondersteunen, ook tijdens (ICT-)storingen. In DORA wordt dit ook wel "digitale operationele weerbaarheid" genoemd.[22]

3. Evenredigheid en *level playing field*

Financiële instellingen moeten in hun aanpak van ICT-risico in principe steeds dezelfde benadering en regels volgen. Consistentie draagt immers bij tot een groter vertrouwen in het financiële stelsel en tot het behoud van de stabiliteit ervan, met name in tijden van grote afhankelijkheid van ICT-systemen, -platforms en -infrastructuren, waardoor het digitale risico stijgt, aldus DORA.[23] Tegelijk verklaren deze systemische doelen van stabiliteit en vertrouwen in het stelsel niet al de regels van DORA van toepassing hoeven te zijn op alle instellingen actief in de financiële sector, en dat de wel van toepassing zijnde regels door de betreffende instelling ook proportioneel mogen worden toegepast.[24] Dit is ook in lijn met het in het Unierecht in algemene zin van toepassing zijnde proportionaliteitsbeginsel, dat meebrengt dat regulering in zijn algemeenheid niet verder moet gaan dan nodig om de daarmee gestelde doelen te bereiken. Dit in zichzelf betekent dat de hiervoor bedoelde consistentie altijd gepaard moet gaan met een zeker maatwerk in regulering en toezicht.[25]

In de context van prudentiële regels heeft DNB in het verleden wel gesteld dat het proportionaliteitsbeginsel meebrengt dat regelgeving en toezicht dienen te zijn afgestemd op de omvang, de complexiteit en, bovenal, de risico's van financiële instellingen.[26] Een evenredige of proportionele aanpak kan vaak eenvoudigere regels betekenen voor kleine en minder complexe instellingen, en omgekeerd om extra regelgeving voor grote en complexere instellingen, die een groter risico voor de financiële stabiliteit vormen. Dankzij proportionaliteit kan naleving door kleine en minder complexe of minder risicovolle instellingen worden vereenvoudigd. Maar ook kan proportionaliteit inhouden dat betrekkelijk grote instellingen mogelijk een tamelijk eenvoudig bedrijfsmodel met lage risico's hanteren en om die reden aan een versimpeld regime kunnen voldoen. Het vormgeven van proportionaliteit dient dus niet alleen te worden gedreven door de omvang, maar ook door de complexiteit en bovenal - volgens DNB - de risico's die een instelling loopt.

Ook in DORA staat het beginsel van proportionaliteit (in de Nederlandse tekst van DORA: het evenredigheidsbeginsel) centraal. Zo dienen bijvoorbeeld de regels in het kader van ICT-risicobeheer uitdrukkelijk toegepast te worden overeenkomstig dit beginsel.[27] Dat resulteert erin dat financiële instellingen de vereisten in het kader van hun ICT-risicobeheer, zoals die met betrekking tot hun governance en controlekader, moeten toepassen rekening houdend met hun omvang, algehele risicoprofiel en de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen. Dat betekent ook dat zolang de belangrijkste door financiële instellingen gecreëerde capaciteiten de uiteenlopende functies in het ICT-risicobeheer (identificatie, bescherming en voorkoming, detectie, respons en herstel, scholing en ontwikkeling en communicatie) ten goede komen, het de financiële instellingen vrij zou moeten staan om anders opgezette of gecategoriseerde modellen voor ICT-risicobeheer te gebruiken.[28] Op operationeel vlak zou dit bijvoorbeeld kunnen inhouden dat de in het kader van het ICT-risicobeheer aangewezen *(chief) technology officer*, *information security officer*, of andere medewerker of commissie niet bij iedere financiële instelling dezelfde senioriteit hoeft te hebben. Uiteraard blijft de financiële instelling en daarmee het bestuur wel de eindverantwoordelijkheid houden voor het door haar gevoerde ICT-risicobeheer.

22. Artikel 3 onder 1 DORA.
23. Overweging 13 DORA.
24. DORA is van toepassing op een breed scala aan financiële instellingen, zie artikel 2 lid 1 DORA. Tegelijk sluit DORA bepaalde, waaronder kleinere, instellingen uit van toepasselijkheid van regels in een andere expressie van het evenredigheidsbeginsel. Artikel 2 lid 3 bepaalt bijvoorbeeld dat de verordening in het geheel niet van toepassing is op bepaalde instellingen, bijvoorbeeld kleinere verzekeringstussenpersonen en artikel 16 DORA schrijft voor bepaalde instellingen een vereenvoudigd kader voor ICT-risicobeheer voor en verklaart daartoe bepaalde regels van DORA buiten toepassing. Interessant is dat de AFM meent dat DORA kan dienen als raamwerk voor alle ondernemingen, ook die strikt genomen niet onder het toepassingsbereik van DORA vallen. Zie Rapport AFM, 'Keuzes maken blijft essentieel in de markt van financiële dienstverleners', Marktindrukken 2022, p. 4 en 14.
25. Artikel 5 lid 4 van het Verdrag betreffende de Europese Unie.
26. DNB studie Proportioneel en effectief toezicht, 2019.
27. Artikel 4 lid 1 DORA. Zie over het evenredigheidsbeginsel bijvoorbeeld ook EIOPA's 2019 Report on best practices on licencing requirements, peer-to-peer insurance and the principle of proportionality in an InsurTech context.
28. Overweging 47 DORA.

En ook het beheer van het ICT-risico dat kan ontstaan door het inschakelen van derde aanbieders moet door financiële instellingen worden uitgevoerd aan de hand van het evenredigheidsbeginsel, rekening houdend met de aard, de schaal, de complexiteit en het belang van ICT-gerelateerde afhankelijkheden, en de risico's die voortvloeien uit contractuele overeenkomsten met derde aanbieders inzake het gebruik van ICT-diensten, rekening houdend met het kritieke karakter of het belang van de respectieve diensten, processen of functies en met de potentiële gevolgen voor de continuïteit en de beschikbaarheid van financiële diensten en activiteiten, op individueel en groepsniveau.[29] Deze laatste toepassing van het evenredigheids- of proportionaliteitsbeginsel wordt door DORA genoemd naast het beginsel dat de instelling te allen tijde volledig verantwoordelijk blijft voor de naleving van haar in DORA vervatte verplichtingen.

Het evenredigheidsbeginsel zoals geëxpliciteerd in DORA erkent daarmee ook een andere, onderliggende doelstelling van Europese regulering, te weten het bevorderen van een gelijk speelveld en daarmee ook de ordelijke werking van de financiële markten. Een proportionele aanpak bevordert juist eerlijke concurrentie en kan tegelijk ook de verscheidenheid tussen en binnen verschillende financiële sectoren ten goede komen. Een *level playing field* in termen van regulering vergt immers niet altijd dezelfde regels maar soms ook *asymmetrische* regels voor financiële instellingen in bepaalde situaties of sectoren of, als alternatief, de proportionele toepassing van dezelfde regels en een proportioneel toezicht op de naleving van die regels.[30] De consistentie en de consistente toepassing zit dan juist in het maatwerk.

4. Kritieke of belangrijke functies

ICT-diensten en ICT-dienstverleners ondersteunen, zoals in paragraaf 2 uiteengezet, doorlopend interne of externe gebruikers van de financiële instelling en daarmee per definitie ook de functies van de financiële instelling. Onder deze functies kunnen ook kritieke functies van de financiële instelling vallen, oftewel een "kritieke of belangrijke functie" in de betekenis van DORA: een functie waarvan de verstoring wezenlijk afbreuk zou doen (i) aan de financiële prestaties van de instelling, (ii) aan de soliditeit of de continuïteit van haar diensten en activiteiten, of (iii),waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door de instelling van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten. [31] Dit zijn zaken waar het natuurlijk met name om gaat waar het digitale operationele weerbaarheid betreft.

Deze definitie van kritieke of belangrijke functies lijkt veel op de "kritieke of belangrijke operationele functies of werkzaamheden" genoemd in artikel 49 van de Solvency II Richtlijn, zoals van toepassing bij uitbesteding door verzekeraars.[32] Hierin wordt het begrip overigens gebruikt in de context van functies waarvan de uitvoering aan een derde, externe partij, worden overgelaten, of in de uitvoering waarvan een derde betrokken wordt, en dus sprake is van uitbesteding, terwijl het begrip kritieke of belangrijke functies in DORA ruimer gebruikt wordt.[33]

In de Wft komt het kritieke – en het daarmee voor toezicht met name relevante – aspect van uitbestedingen tot uitdrukking in de definitie van uitbesteding zelf. De Wft definieert "uitbesteding" als het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden: (i) die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten, of (ii) die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan. Met de term "wezenlijke" is tot uitdrukking gebracht dat de regels voor uitbesteding niet voor elke werkzaamheid van belang zijn.

Deze materialiteitsdrempel wordt in de verschillende regelingen met verschillende termen aangeduid.[34] Het komt echter telkens op hetzelfde neer: een beperking van de reikwijdte van de uitbestedingsregels tot de voor het toezicht relevante werkzaamheden. In artikel 49 van de Solvency II Richtlijn worden die wezenlijke werkzaamheden bijvoorbeeld omschreven in termen van de gevolgen waartoe ze niet mogen leiden. Die gevolgen zijn: (i) wezenlijke afbreuk aan de kwaliteit van het governancesysteem, (ii) onnodige toename van het operationele risico, (iii) afbreuk aan het vermogen van de toezichthouder om te controleren of de onderneming haar verplichtingen nakomt, en (iv) ondermijning

29. Artikel 28 DORA.
30. Over het evenredigheidsbeginsel, zie bijvoorbeeld Andrea Enria, Regulation, proportionality and the sustainability of banking. Enria writes: "So evidently, we cannot have a "one size fits all" approach. For the sake of fairness and for a level playing field, rules must indeed be proportional", of Kerstin af Jochnick, Striking a balance: proportionality in European banking regulation and supervision. Introductory statement by Kerstin af Jochnick, Member of the Supervisory Board of the ECB, at the panel discussion on "A proportionate implementation of Basel III" at the European Commission's DG Financial Stability, Financial Services and Capital Markets Union conference on the implementation of Basel III, Brussels, 12 November 2019.
31. Artikel 3 onder 22.
32. 2009/148/EU. Zie ook art. 274 van de Solvency II Gedelegeerde Verordening (2015/35/EU).
33. Zie bijvoorbeeld artikel 9 lid 2, waarin het belang van implementatie van ICT-beveiligingsbeleid en -procedures in algemene zin wordt benadrukt, met name waar het gaat om ICT-systemen die gebruikt worden ten behoeve van kritieke of belangrijke functies, zonder daarbij expliciet te verwijzen naar een betrokken ICT-leverancier.
34. Zie P. Laaper, Uitbesteding in de financiële sector (O&R nr. 88) 2015/2.5.5 en 2.5.5.3.

van de continuïteit of toereikendheid van de dienstverlening aan de cliënten.

DORA legt andere en nieuwe accenten ten opzichte van dit bestaande begrip van wezenlijkheid. Niet alleen omdat het bij de kritieke functies uit het hiervoor genoemde Solvency II-regime per definitie gaat om functies die door derden voor de instelling worden verricht, waar dat onder DORA niet het geval hoeft te zijn zoals hiervoor toegelicht. Maar ook omdat het begrip kritieke of belangrijke functies in DORA een bredere betekenis heeft, en ook de "kritieke functies" omvat als bedoeld in artikel 2, lid 1, punt 35 van de Richtlijn herstel en afwikkeling van banken en beleggingsondernemingen (ook bekend als de *Bank Recovery and Resolution Directive* of "**BRRD**").[35] In het bestaande regelgevend kader is dat niet het geval, en wordt in de EBA uitbestedingsrichtsnoeren zelfs expliciet benadrukt dat het gebruik van "kritieke of belangrijke functies" daarin moet worden onderscheiden van de definitie uit de BRRD en daarmee geen verband houdt.[36]

Hierdoor wordt van financiële instellingen vanaf het moment dat DORA van toepassing is meer uitdrukkelijk een instellingsoverschrijdend en zelfs systemisch perspectief verwacht, aangezien de BRRD onder kritieke functies ook die activiteiten, diensten of bedrijfsactiviteiten vangt waarvan de onderbreking naar alle waarschijnlijkheid in één of meer lidstaten tot een verstoring van essentiële diensten aan de reële economie zal leiden of, wegens de omvang of het marktaandeel van een instelling of groep, haar verwevenheid met entiteiten binnen en buiten een groep, haar complexiteit of haar grensoverschrijdende activiteiten, de financiële stabiliteit zal verstoren, vooral wat de vervangbaarheid van de functie betreft.

Met de hierin opgenomen verwijzing naar financiële stabiliteit gaat het om een systeemperspectief dat gewoonlijk aan externe, publieke toezichthouders is voorbehouden. Maar ook de verwijzing naar de verstoring van essentiële diensten aan de reële economie veronderstelt een bredere "blik naar buiten" van de financiële instelling. DORA vraagt instellingen om deze blik in afwegingen die - zeker waar het dienstverlening die betrekking heeft op kritieke of belangrijke functies betreft - al complex zijn en die zowel ICT-dienstverleningsrelaties binnen de financiële instelling zelf kunnen betreffen, bijvoorbeeld tussen afdelingen of tussen (bij)kantoren, als relaties met derde partijen.

Die complexiteit volgt bijvoorbeeld uit de afwegingen die de financiële instelling moet maken indien ICT-dienstverleningsovereenkomsten die kritieke of belangrijke functies ondersteunen bijvoorbeeld de mogelijkheid inhouden dat de ICT-leverancier de ICT-diensten verder (onder)uitbesteedt.[37] In dat geval moet de instelling in het DORA-regime de baten en risico's afwegen die uit een dergelijke uitbesteding kunnen voortkomen, met name in het geval van een in een derde land gevestigde subcontractant. Daarbij moet het zowel het lokale insolventierecht expliciet worden meegewogen, als de naleving van de gegevensbeschermingsregels van de Unie en de doeltreffende handhaving van de wet in dat derde land. Financiële instellingen moeten ook 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.[38]

5. Testen van digitale operationele weerbaarheid

Grotendeels[39] nieuw in DORA is de verplichting voor de financiële instelling om haar digitale operationele weerbaarheid periodiek te testen en in dit kader testprogramma's in te richten.[40] Zo'n testprogramma dient passende tests te bevatten die worden uitgevoerd op de ICT-systemen en -toepassingen van de financiële instelling, zoals kwetsbaarheidsbeoordelingen en -scans, open source analyses, beoordeling van netwerkbeveiliging, broncodereviews en pentests.[41] Daarbij geldt dat de testverplichtingen strenger zullen zijn wanneer het gaat om grote,

35. Richtlijn 2014/59/EU van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen. Zie overweging 70 DORA.
36. Zie Background nr. 20 en voetnoot 28 van de Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 February 2019.
37. Complexiteit volgt ook uit het feit dat, bijvoorbeeld, het ene bijkantoor van een financiële instelling functies verlenen aan het andere bijkantoor van die instelling. Dan is er strikt genomen geen sprake van uitbesteding, aangezien bij uitbesteding diensten worden verricht door een andere rechtspersoon dan de financiële instelling zelf en dat bij intragroepdienstverlening niet het geval is. Maar ook in geval van dergelijke quasi uitbesteding dienen soortgelijke risico's als bij uitbesteding onder ogen gezien worden. Dit wordt onder meer benadrukt in een recente *supervisory statement* van EIOPA, dat gaat over (interne) governance afspraken tussen verzekeraars of verzekeringstussenpersonen en hun eigen bijkantoren in derde landen: "*Although these governance arrangements do not qualify as outsourcing, similar risks need to be addressed and therefore supervisory actions aimed at addressing concerns related to outsourcing might also be considered as relevant and appropriate*", aldus EIOPA. Zie EIOPA-22/362 3 februari 2023.
38. Artikel 29 lid 2 DORA.
39. De richtsnoeren van EBA bevatten wel een verplichting tot een uitvoeren van periodieke pentests (randnummer 94 EBA-richtsnoeren, en randnummer 55 (h) onder (iv) EBA-richtsnoeren inzake de beoordeling van het ICT-risico in het kader van SREP), maar dit betreft een veel beperktere (en niet gecodificeerde) verplichting dan de uitgebreide testprogramma's zoals die in DORA zijn vormgegeven.
40. Hoofdstuk IV, artikel 24 t/m 27, DORA.
41. Artikel 25 lid 1 DORA.

systemische en in ICT-opzicht ontwikkelde financiële instellingen.[42] Hier speelt het in het evenredigheidsbeginsel, zoals we dat al bespraken in paragraaf 3, een rol: de uitvoering van de testverplichtingen uit Hoofdstuk IV DORA dient namelijk in verhouding te staan tot de omvang, het algehele risicoprofiel van de financiële instelling, en de aard, schaal en complexiteit van hun diensten en activiteiten.[43]

Bij het uitvoeren van het testprogramma dient de financiële instelling volgens DORA bovendien een risicogebaseerde benadering te volgen in een (ons) opvallende samensmelting van het evenredigheidsbeginsel en het principe van risico-georiënteerde compliance. Er moet bij de uitvoering en die benadering volgens DORA namelijk niet alleen rekening worden gehouden met de hiervoor genoemde proportionaliteitscriteria van artikel 4 lid 2 DORA, maar ook met het veranderende landschap van het ICT-risico, eventuele specifieke risico's waaraan de financiële instelling wordt of kan worden blootgesteld, de kritieke aard van informatieactiva en verleende diensten, en alle andere factoren die de instelling passend acht.[44] Hoewel de kaders van de beoordeling daarmee wel worden meegegeven, wordt de invulling van de verplichte testprogramma's vooralsnog vooral overgelaten aan de financiële instelling zelf. Dit betekent ook dat er veel onduidelijkheid bij financiële instellingen kan bestaan met betrekking tot de vraag of zij aan haar verplichtingen in dit kader heeft voldaan en of zij dus compliant is.

Naast deze algemene tests voor de beoordeling of voldaan is aan de basisvereisten om ICT-risico te voorkomen en beperken dienen bepaalde, specifiek door de toezichthouder daartoe aangemerkte, financiële instellingen minimaal eens per drie jaar geavanceerde tests uit te voeren in de vorm van dreigingsgestuurde penetratietests ("*threat led penetration testing*" of "**TLPT**"). Bij TLPT worden de tactiek, technieken en procedures die voorkomen bij cyberdreigingen nagebootst en uitgevoerd op de productiesystemen van de financiële instelling door middel van een gecontroleerde (zogeheten *red team*) test.[45] De toezichthouder zal deze verplichting alleen opleggen aan instellingen die actief zijn in subsectoren van de belangrijkste financiële diensten en die een systemische rol hebben.[46]

Indien een financiële instelling verplicht wordt tot uitvoering van TLPT, is het vervolgens wederom aan de instelling zelf om het exacte toepassingsbereik van de TLPT te bepalen en vrijelijk aan te geven voor welke en hoeveel kritieke of belangrijke functies TLPT moet worden verricht.[47] Het resultaat van deze beoordeling dient nog wel te worden gevalideerd door toezichthouder, maar dat lijkt uitsluitend een formaliteit te betreffen. Ook in dit kader wordt de nadere invulling van deze verplichting dus uiteindelijk overgelaten aan de financiële instelling zelf.

6. ICT-concentratierisico

Nieuw is ook dat DORA de bredere systeemrisico's aan de orde stelt die kunnen voortvloeien aan blootstelling van de financiële sector aan een beperkt aantal kritieke derde aanbieders van ICT-diensten.[48] Als onderdeel van haar ICT-risicobeheer in het DORA-regime dient een financiële instelling vooruitlopend op het inschakelen van een derde aanbieder, bij het identificeren en beoordelen van alle relevante risico's daarvan, mee te wegen of het inschakelen van deze derde kan leiden tot versterking van wat DORA het "ICT-concentratierisico" noemt.[49]

Van een ICT-concentratierisico is sprake indien de financiële instelling door inschakeling van die derde wordt blootgesteld aan individuele of aan meerdere onderling verbonden kritieke derde aanbieders van ICT-diensten, waardoor een bepaalde mate van afhankelijkheid ten aanzien van deze aanbieders ontstaat, zodat de onbeschikbaarheid, het falen of een ander soort tekortkoming van deze aanbieder het vermogen van een financiële entiteit om kritieke of belangrijke functies te vervullen in gevaar kan brengen, ertoe kan leiden dat zij andere soorten nadelige effecten, waaronder grote verliezen, ondervindt, of de financiële stabiliteit van de Unie in haar geheel in gevaar kan brengen.[50]

In hun beoordeling van dit ICT-concentratierisico dienen financiële instellingen onder meer rekening te houden met de vraag of het inschakelen van de derde mogelijk kan leiden tot een zogenoemde *vendor lock-in* waarbij de aanbieder niet eenvoudig te vervangen is, en of de financiële instelling al meerdere overeenkomsten heeft gesloten met dezelfde kritieke aanbieder waardoor mogelijk een te grote afhankelijkheid van de betreffende aanbieder ontstaat.[51] Daarbij dienen instellingen een kosten-batenafweging van alternatieve oplossingen mee te nemen.

Deze vereisten, die artikel 29 DORA aan de financiële instelling oplegt, zijn op zichzelf overigens niet nieuw. Zo vereisen zowel de uitbestedingsrichtsnoeren van de EBA als die van de EIOPA dat de financiële instelling in haar *pre-outsourcing analysis* nagaat in hoeverre er sprake is van (geaggregeerde) blootstelling is aan dezelfde ICT-dienstverlener[52] en

42. Overweging 56 DORA.
43. Artikel 4 lid 2 DORA.
44. Artikel 24 lid 3 DORA.
45. Artikel 3 onder 17 DORA.
46. Overweging 56 en artikel 26 lid 8 DORA.
47. Artikel 26 lid 2 DORA.
48. Overweging 30 DORA.
49. Artikel 28 lid 4 sub c DORA.
50. Artikel 3 onder 29 DORA.
51. Artikel 29 DORA.
52. 31 onder e EBA uitbestedingsrichtsnoeren, 29 onder c EIOPA uitbestedingsrichtsnoeren.

of de ICT-leverancier vervangbaar is.[53] De uitbestedingsrichtsnoeren van de ESMA gaan zelfs verder en vereisen naast een beoordeling van mogelijke concentratie binnen de financiële instelling (of groep waarvan zij onderdeel uitmaakt) door het aangaan van meerdere uitbestedingsovereenkomsten met dezelfde cloud service provider, ook een instellingsoverschrijdende toets waarin de instelling nagaat of sprake is van mogelijke concentratie binnen de financiële sector van de EU doordat meerdere ondernemingen gebruikmaken van dezelfde leverancier.[54]

Opvallend is ook hier dat de beoordeling of sprake is van een ICT-concentratierisico in DORA wordt neergelegd bij de financiële instelling zelf. Het ICT-concentratierisicobegrip wordt vooral in artikel 29 gebruikt, welk artikel uitsluitend verplichtingen voor de financiële instelling zelf bevat, zoals hiervoor al omschreven.[55] Dit wringt enigszins aangezien in de definitie van ICT-concentratierisico zelf de systemische implicaties van deze concentratierisico's wordt erkend. Bovendien wordt in DORA erkend dat de impact van kritieke derde aanbieders van ICT-diensten op de financiële sector in de Unie en de mogelijke problemen als gevolg van het daaraan verbonden ICT-concentratierisico vragen om een gezamenlijke aanpak op het niveau van de Unie.[56] Een betere greep krijgen op deze systemische dimensie is één van de redenen voor het eveneens door DORA ingevoerde systeemtoezicht op derde dienstverleners, in de vorm van het oversightkader dat we in de volgende paragraaf bespreken. De definitie van ICT-concentratierisico verwijst in dit verband reeds naar de in dat oversightkader door de ESA's als cruciaal aangewezen kritieke derde aanbieders van ICT-diensten.

Gezien de invulling van de vereisten met betrekking tot het ICT-concentratierisico die worden gesteld aan de financiële instelling zoals neergelegd in artikel 29, lijkt de toetsing die zij in de praktijk zullen (moeten) doen vooral te zien op de vragen (i) of zij een contract sluiten met een derde aanbieder van ICT-diensten die niet gemakkelijk substitueerbaar is, danwel (ii) of zij beschikken over meerdere contractuele overeenkomsten inzake de verlening van ICT-diensten die kritieke of belangrijke functies ondersteunen, met dezelfde derde aanbieder van ICT-diensten of met nauw verbonden derde aanbieders van ICT-diensten. Evenwel kleurt ook hier via de definitie van "kritieke of belangrijke functies" (paragraaf 4) het systemische perspectief het antwoord op deze vragen ook voor de individuele financiële instelling wel degelijk mede in.

7. Oversight Framework en het perspectief van de ICT-dienstverlener

DORA betrekt niet alleen financiële instellingen in haar regulering en toezicht, maar ook de ICT-dienstverleners die een rol spelen bij de levering van financiële diensten of zelfs zijn geïntegreerd in de waardeketen van die diensten. Met DORA komen bepaalde dienstverleners onder een rechtstreekse vorm van toezicht te vallen, namelijk die dienstverleners die als kritiek (ook wel: cruciaal) worden aangemerkt. Ook dat is nieuw in zowel financiële als ICT-regulering. ICT-storingen en cyberincidenten kunnen bij uitstek impact hebben op het gehele financiële stelsel, sector- en grensoverschrijdend, en zich daarin in een aanzienlijk sneller tempo verspreiden dan andere soorten risico's die in de financiële sector worden gemonitord. Dergelijke incidenten kunnen uitgroeien tot een systemische crisis, aldus DORA, waarin het vertrouwen in het financiële stelsel wordt uitgehold door de verstoring van functies die de reële economie ondersteunen, of door aanzienlijke financiële verliezen die een niveau kunnen bereiken waar het financiële stelsel niet tegen bestand is of waarvoor zware maatregelen ter schokabsorptie moeten worden genomen.[57]

Om dit soort scenario's te voorkomen, wil DORA de praktijken inzake toezicht op ICT-risico's meer op één lijn te brengen, en introduceert daartoe nieuwe regels die oversight van de Unie op derde aanbieders van ICT-diensten mogelijk zullen maken. Het bedoelde oversight vertegenwoordigt als zodanig zelf een systeemperspectief en plaatst de dienstverleners en de financiële instellingen die van hun diensten gebruik maken, daarmee expliciet in dit kader. Daartoe kunnen ESA's onder DORA derde aanbieders van ICT-diensten aanwijzen die cruciaal zijn voor financiële entiteiten en voor dergelijke "kritieke derde aanbieders van ICT-diensten" een *lead overseer* benoemen. Deze aanwijzingen doen de ESA's via het Gemengd Comité en op aanbeveling van een nieuw aan te stellen subcommissie daarvan: het oversightforum. Hun beoordeling houdt rekening met diverse systemische invalshoeken ten aanzien van de door de dienstverlener geleverde ICT-diensten, zoals:

i. de systemische effecten op de stabiliteit, continuïteit of kwaliteit van de verlening van financiële diensten ingeval de betrokken ICT-leverancier te maken zou krijgen met een grootschalige operationele verstoring van de dienstverlening, waarbij rekening dient te worden gehouden met het aantal financiële entiteiten en de totale waarde van de activa van de financiële entiteiten waaraan de betreffende leverancier diensten verleent,
ii. het systemische karakter of belang van de financiële instellingen die afhankelijk zijn van de ICT-leverancier, en

53. 31 onder h EBA uitbestedingsrichtsnoeren, 29 onder e EIOPA uitbestedingsrichtsnoeren.
54. 21 (a) onder (vii) ESMA uitbestedingsrichtsnoeren.
55. Zie echter ook art. 32 lid 2 en 35 lid 1 d(ii) DORA.
56. Overweging 88 DORA.
57. Overweging 79 DORA.

iii. de afhankelijkheid van financiële instellingen ten aanzien van de diensten die door de ICT-leverancier worden verleend met betrekking tot kritieke of belangrijke functies van financiële instellingen waarbij uiteindelijk dezelfde ICT-leverancier betrokken is.

Ook de vraag hoe makkelijk de ICT-leverancier substitueerbaar is, speelt een rol bij de beoordeling van diens cruciale status.

Lead overseers krijgen de nodige bevoegdheden binnen een nieuwe vorm van systeemtoezicht om onderzoeken te verrichten, inspecties ter plaatse en daarbuiten uit te voeren in de gebouwen en op de locaties van de derde aanbieders, en volledige en actuele informatie te verkrijgen. Die bevoegdheden moeten de lead overseer in staat stellen een gedegen inzicht te krijgen in het soort, de omvang en de impact van het ICT-risico van derden voor financiële instellingen en, uiteindelijk, voor het financiële stelsel van de Unie.[58] De lead overseer kan als onderdeel van zijn bevoegdheden aanbevelingen uitvaardigen aan ICT-leveranciers over hun eigen uitbestedingsarrangementen of de leverancier zelfs instrueren om deze, onder omstandigheden, stop te zetten.

Interessant is dat de derde aanbieders van ICT-diensten ook zelf via de ESA's kunnen verzoeken om door het Gemengd Comité als cruciaal te worden aangewezen, om daarmee onder het oversightkader te komen vallen. Wij kunnen ons voorstellen dat er redenen zijn voor ICT-dienstverleners om hier vrijwillig voor te opteren. Zo verkrijgen zij immers een eigenstandige positie vis-a-vis de toezichthouder en zijn niet afhankelijk, waar het toezichtsvereisten betreft, van de (informatie van of via) financiële instellingen waaraan zij diensten verlenen. Zij kunnen op deze manier onzekerheid wegnemen, zowel voor zichzelf als voor de instellingen waarvoor zij diensten verrichten, over hun eigen cruciale status. Daarnaast zal het deelnemen aan de systeemdialoog binnen het Europese oversightkader ongetwijfeld ook een kwaliteitskenmerk worden en een markering van het belang van de dienstverlener.

DORA aarzelt overigens niet om te benadrukken dat het oversightkader niet in de plaats mag komen van het vereiste voor financiële instellingen om zelf de risico's te beheren die voortvloeien uit het inschakelen van ICT-leveranciers, waaronder hun verplichting om overeenkomsten met kritieke aanbieders permanent te monitoren.[59] In die zin wordt de verantwoordelijkheid voor (toezicht op) digitale *resilience* uitdrukkelijk niet een gedeelde verantwoordelijkheid.

8. Tot slot: vertrouwensgemeenschappen tussen financiële instellingen

DORA laat evident lastige, op beginselen en risico's gebaseerde afwegingen bij de financiële instellingen zelf. Dit lijkt ook een bewuste keuze van de Europese wetgever, nu regels die te gedetailleerde voorschriften bevatten al snel achterhaald worden naarmate de toepassingen van ICT in de financiële sector verder innoveren en cyber- en ICT-risico's evolueren. Hier tonen zich ook grenzen van wat in de macht ligt van nationale en Europese financiële toezichthouders met betrekking tot de aard en verspreiding van cyberrisico's in het kader van hun toezicht.

Volgens DORA moet niet alleen het gemeenschappelijk rulebook en het publieke toezichtsysteem op digitale operationele weerbaarheid worden ontwikkeld, maar zouden ook instellingen zelf in hun onderlinge verhoudingen beter op cyberdreigingen en –kwetsbaarheden moeten anticiperen.[60] Financiële instellingen kunnen elkaar in dit opzicht op verschillende manieren bijstaan. Bijvoorbeeld door elkaar bewust te maken van cyberdreigingen of de mogelijkheden tot verdere verspreiding van cyberdreigingen beperken. Zij kunnen ook technieken voor dreigingsdetectie delen of steunen. Deze uitwisseling moet geschieden binnen wat DORA "vertrouwensgemeenschappen van financiële entiteiten" noemt.

In dit kader dient een regeling voor informatie-uitwisseling te worden getroffen ter bescherming van de potentieel gevoelige aard van de gedeelde informatie, en er moeten gedragsregels gelden waarin de vertrouwelijkheid van bedrijfsinformatie, de bescherming van persoonsgegevens overeenkomstig de Algemene Verordening Gegevensbescherming[61] en de richtsnoeren inzake mededingingsbeleid volledig worden gerespecteerd. Daarin zijn overigens gelijk ook evident de beperkingen van die vertrouwensgemeenschap en de mogelijkheden tot informatie-uitwisseling gelegen. In deze vooruitblik naar regulatoire vertrouwensgemeenschappen worden preventieve mechanismen voor informatie-uitwisseling tussen financiële instellingen deel van de regulatoire context die de systemische dimensies van ICT-risico's wil borgen.

58. Overweging 88 DORA.
59. Overweging 92 DORA.
60. Artikel 45 DORA.
61. Verordening (EU) 2016/679 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).