Whitepaper

Digital Operational Resilience Act:

De harmonisering van de digitale weerbaarheid in de financiële sector van de EU

Introductie

De afgelopen jaren heeft de Europese Commissie een aantal vooruitstrevende wetsvoorstellen ontwikkeld, gericht op *"een Europa dat geschikt is voor het digitale tijdperk"*, zoals Commissievoorzitter Ursula von der Leyen het project heeft onthult[1]. Voorstellen als de *Digital Services Act*[2] *en Digital Markets Act*[3] krijgen internationaal de meeste aandacht, maar minder opgemerkte voorstellen lijken alleen de meer gespecialiseerde en sectorale kringen te bereiken.

In september 2020 bracht de Europese Commissie een volledig nieuw regelgevend kader uit, het ontwerp voor de **Digital Operational Resilience Act** (DORA) als onderdeel van *het Digital Finance Package* (DFP)[4]. Het voorstel bouwt voort op reeds bestaande regelgevingsvereisten die door verschillende Europese toezichthouders zijn ingevoerd, en combineert deze in één enkele verordening. De DORA hervormt als het ware de al bestaande sectorale regelgeving van de EU in het licht van de ontwikkelingen in de digitale technologie, en de veranderingen in de sector als gevolg daarvan. Voordat het voorstel in werking treedt, is er eigenlijk nog geen objectieve norm voor ICT-risicobeheer als uniforme aanpak in Europa.

De DORA streeft naar een veel duidelijker fundament te leggen en het zwaartepunt te verleggen van het waarborgen van de financiële veerkracht van ondernemingen, naar het waarborgen dat zij hun activiteiten weerbaar kunnen houden wanneer een ernstige operationele verstoring zich voordoet – zoals bij een cyberaanval.

De urgentie van dit voorstel komt voort uit de grote bezorgdheid die is geuit door het *European Systemic Risk Board*[5], dat adviseerde dat de vereisten voor het beheer van de thirdparty risico's en financiële entiteiten in heel Europa moeten worden gelijkgesteld en aangescherpt. Deze aanbeveling volgt op een verslag over cyberincidenten in de financiële sector, waarin cyberrisico's als een van de grootste risico's werden aangemerkt en waarin werd erkend dat één enkele gebeurtenis een systeemcrisis zou kunnen veroorzaken, waardoor de financiële stabiliteit in heel Europa zou worden bedreigd. Aangezien financiële ondernemingen steeds afhankelijker worden van hun digitale systemen, besloot de EU er bij ondernemingen op aan te dringen hun activiteiten zo weerbaar mogelijk te maken.

Dit gevoel van urgentie en de toenemende behoefte aan betere veerkracht komt voort uit de recente toename van cyberaanvallen, waarbij de financiële sector herhaaldelijk het doelwit is geweest van deze inbraken. Cyberaanvallen kunnen weliswaar niet helemaal worden voorkomen, maar de financiële stabiliteit in Europa – en daarmee de impact op de wereldwijde financiële sector – kan toch worden bereikt als organisaties de gevolgen van cyberdreigingen voor ICT zo veel mogelijk beperken.

De toename van cyberaanvallen werd ook waargenomen tijdens de COVID-19 pandemie, toen het belang van *remote access* voor financiële diensten sterk toenam, en daarmee ook het gebruik en de afhankelijkheid van ICT in de financiële sector. De Europese Commissie verklaarde dat het aantal cyberaanvallen op financiële instellingen sinds het begin van de pandemie met 38% is toegenomen, zonder dat er sprake was van een uniforme manier van beveiliging[6]. Dit impliceert de noodzaak van betere regelgeving, om ervoor te zorgen dat financiële entiteiten bestand zijn tegen potentiële ICT-verstoringen en zo cyberincidenten en -dreigingen aan te pakken.

Wereldwijde scope

De DORA creëert één uniform kader voor de regulering van risicobeheer voor financiële entiteiten die in Europa actief zijn en schrijft een gemeenschappelijke aanpak van cyberbeveiliging voor ICT voor in alle 30 landen van de European Economic Area[7].

DORA's autoriteit zal wereldwijd worden gevoeld, aangezien het aanzienlijke gevolgen zal hebben voor de manier waarop elke ICT-aanbieder of grote financiële organisatie zaken doet in Europa, en voor de manier waarop financiële entiteiten software-as-a-service-technologie gebruiken gedurende de levenscyclus. De verordening is van invloed op alle ICT-aanbieders van financiële diensten, financiële-technologiebedrijven en bedrijven die zijn aangewezen als kritieke leveranciers die in Europa actief zijn, ongeacht of deze leveranciers in Europa of elders in de wereld gevestigd zijn. Zij moeten allemaal voldoen aan de DORA-vereisten, of anders worden zij geconfronteerd met aanzienlijke sancties, aangezien de *European Supervisory Authorities* (ETA's) gemachtigd zullen zijn om rechtstreeks toegang te krijgen tot thirdparty dienstverleners op het gebied van kritieke ICT – en hen zo nodig sancties op te leggen.

Het voorstel bevat echter beperkingen ten aanzien van wie zaken mag doen met financiële entiteiten in de EU. Hoewel de DORA de grensoverschrijdende gegevens overdacht tussen deze entiteiten en derde ICT-aanbieders niet rechtstreeks zou beperken, zouden verschillende van de vermelde bepalingen wel tot dat gevolg kunnen leiden. Het gebruik van aanbieders van buiten de EU en hun diensten zou indirect kunnen worden beperkt indien deze van buiten de EU worden geleverd. Een van de bepalingen (artikel 26, lid 2[8]) zou speciale verplichtingen opleggen aan entiteiten die hun in de EU gevestigde ICT-leverancier toestaan kritieke of belangrijke functies uit te besteden aan een leverancier in een niet in de EU gevestigd land. Technisch gezien zou dit betekenen dat de buitenlandse status van de ICT-sub contractant per definitie hierdoor diskwalificerend kan worden gezien. Niettemin lijkt de bepaling het vermoeden te vestigen dat de keuze van een niet in de EU gevestigde contractant een complicerende factor zou zijn voor een in de EU gevestigde financiële entiteit.

Dit bouwt voort op de volgende bepaling, waarin wordt gesteld dat financiële entiteiten voor hun kritieke ICT-diensten geen beroep mogen doen op ondernemingen zonder zakelijke aanwezigheid in de EU. Hoewel er geen tekstuele reden voor deze beperking wordt gegeven, mag worden aangenomen dat de Commissie de zakelijke aanwezigheid van de derde partij in een EU-lidstaat als juridisch voldoende beschouwt om jurisdictie uit te oefenen en gegevens op te eisen, indien dat nodig wordt geacht. Ook wordt benadrukt dat deze specifieke bepaling geen vereiste is om gegevens te lokaliseren – *"de verordening houdt geen verdere eis in dat de opslag of verwerking van gegevens binnen de Unie moet plaatsvinden"*, zoals artikel 28. Lid 9, van de DORA citeert[9].

Aangezien er kan worden gespeculeerd dat dit om concurrentieredenen is, moet in de voorgestelde DORA-wetgeving beter worden toegelicht hoe de aangedragen beperkingen voor diensten van thirdparty aanbieders buiten het territoriale toepassingsgebied in overeenstemming zijn met de non-discriminatieverplichtingen in het handelsrecht, of kunnen worden gerechtvaardigd door relevante uitzonderingen.

Aangezien een van de belangrijkste redenen achter de verordening de harmonisatie van de regels inzake ICT-risicobeheer is, is het toepassingsgebied van de DORA zeker zeer ruim. DORA bestrijkt alle financiële actoren in de EU, van kredietinstellingen tot AIFMS, betalingsinstellingen, verzekeringsmaatschappijen en *statutory auditors*. De voorschriften zijn dan ook gebaseerd op evenredigheid: hoewel de voorschriften op alle financiële entiteiten van toepassing zijn, hangt de toepasselijkheid af van talrijke variabelen, zoals de omvang, de activiteit en het totale risico waaraan de entiteit is blootgesteld. De toepasselijkheid strekt zich uit tot 20 soorten gereguleerde financiële entiteiten in de EU, zoals banken, effectenbeurzen en *clearinghouses*, maar ook *fintechs*. Buiten het bereik van de DORA blijven betalingssystemen en kaartbetalingsregelingen.

Om de lat op een niveau te leggen dat nieuwkomers op de financiële markten niet in het gedrang komen, zorgt een *'sliding scale'* van toepassingsdrempels ervoor dat hoe groter het risico van de transactie (of hoe kritischer de dienst voor de financiële markten), hoe strikter de toepassing van de wet.

Opmerkelijk is dat de regering van het Verenigd Koninkrijk heeft laten doorschemeren dat zij wetgeving zal uitvaardigen voor een Brits equivalent van de DORA van de EU. Deze plannen zijn aangekondigd in Her Majesty's Treasury, waarin een voorstel wordt geschetst om ook derden bij financiële diensten en financiële markt infrastructuurbedrijven te reguleren. Net als de DORA wil ook het Britse voorstel toezichthouders in staat stellen rechtstreeks toezicht te houden op de diensten van kritieke derden en streeft het naar een grotere veerkracht.

Overeenkomsten en voortzetting

Aangezien de DORA voortbouwt op bestaande regelgeving, stelt de EU dat de complexiteit van de algemene regelgeving zal worden verminderd en dat de financiële en administratieve lasten als gevolg van de huidige lappendeken van regelgeving zullen afnemen.

Het voorstel is de eerste poging om de vereisten voor ICT-risicobeheer op EU-level te stroomlijnen en te harmoniseren. In het verleden hebben we op het gebied van cyberbeveiliging te maken gehad met minimale interventie van de EU, en met te algemene regels die leiden tot eigen interpretatie door de nationale autoriteiten. In tegenstelling tot andere EU-wetgeving op het gebied van cyberbeveiliging, met name de *General Data Protection Regulation* (GDPR) en *Network and Information Systems Directive* (NIS), is de DORA niet een wetgeving die op beginselen is gebaseerd, maar bevat zij juist gedetailleerde lijsten van vereisten om de operationele- en beveiligingscapaciteiten van de betrokken partijen te verbeteren.

Waar de DORA verschilt van de NIS/NIS2, is op welke sectoren beide van toepassing zijn. NIS is van toepassing op de meeste bedrijven en sectoren, terwijl DORA specifiek van alleen toepassing is op de financiële sector en hun kritieke externe ICT-leveranciers. De mogelijke overlappingen tussen de twee worden aangepakt via een *lex specialis*-uitzondering, wat betekent dat in geval van conflict allereerst de DORA van toepassing is.

Een soortgelijke reeks regels is te vinden in het *Cyber Security Framework* (CSF) als adviesaanbeveling, gepubliceerd door het *National Institute of Standards and Technology* (NIST). Het contrast tussen deze twee is dat, terwijl de CSF-richtlijnen slechts adviserend zijn, DORA naleving juist afdwingt en vereist dat wordt aangetoond dat aan de gestelde voorwaarden wordt voldaan.

Autoriteiten

Voor het toezicht op de betrokken financiële entiteiten en de daarmee verbonden *Critical Third-Party Providers* (CTPPs) om ervoor te zorgen dat de regelgevingsnormen worden nageleefd, zal een van de drie ETA's worden aangewezen:

- The European Banking Authority (EBA)[10]
- The European Insurance and Occupational Pensions Authority (EIOPA)[11]
- The European Securities and Markets Authority (ESMA)[12]

Een van de drie zal worden aangesteld als *'Lead Overseer'* voor elk CTPP. De aanwijzing van elke ETA bij een CTPP wordt gekozen op basis van de totale waarde van de activa van de financiële entiteiten die van de diensten van de CTPP gebruikmaken. Het toezicht op CTPP's wordt gebruikt om een zogeheten domino-effect te voorkomen, waarbij de sterk verweven financiële sector door één enkele gebeurtenis ten val zou kunnen komen.

Vijf pilaren van DORA

Zodra de nieuwe verordening eind 2022 in werking treedt, met een verwachte overgangsperiode van twee jaar, wordt van financiële ondernemingen in de EU verwacht dat zij voldoen aan de nieuwe gestelde eisen in de volgende vijf pilaren van de DORA:

Digital Operational Resilience Testing

- Verplichting om een proportioneel en risico gebaseerd testprogramma voor digitale operationele weerbaarheid uit te voeren voor een volledig scala aan passende tests,
- ICT-risicobeheerkaders op regelmatige basis testen,
- Zorgen voor een snelle uitvoering van de juiste maatregelen,
- Kritische ICT-systemen en -toepassingen moeten jaarlijks worden getest.

Om ervoor te zorgen dat de betrouwbaarheid van de ICT-afweer is vastgesteld, moeten financiële entiteiten regelmatig digitale operationele weerbaarheidstests ondergaan, uitgevoerd door interne of externe partijen. Het regelmatig testen bestaat uit een programma voor het testen van de digitale weerbaarheid, waarin de test methodologieën, testprocedures en -instrumenten, de frequentie van de weerbaarheidstesten en prioriteringsstrategie voor het testbeleid zijn opgenomen.

Deze pilaar kan de financiële sector bekend in de oren klinken, aangezien Threat-Led Penetration Testing-kaders momenteel verplicht zijn voor bepaalde financiële markinfrastructuren. De DORA zal de testvereisten uitbreiden tot de hele financiële sector en het aantal entiteiten dat verplicht tests moet uitvoeren, verhogen. Het voorstel gaat uit van een jaarlijkse test voor alle kritieke ICT voor elke financiële entiteit op zijn minst.

De evenredige toepassing van het DORA-voorstel komt het duidelijkst tot uiting in deze pilaar, aangezien basistests verplicht zijn voor alle financiële entiteiten en geavanceerde tests alleen vereist zijn voor financiële entiteiten die door de bevoegde autoriteit als significant worden aangemerkt. Dit is gebaseerd op criteria die in de verordening zijn geschetst en door de ETA's verder zijn uitgewerkt.

ICT Risk Management

- Alomvattend ICT-risicobeheerkader dat richting geeft aan alles wat met ICT-risicobeheer te maken heeft,
- Stroomlijning van de bestaande regels inzake ICT-governance,
- Expliciete verplichting voor het management om hun kennis van ICT-risico's te ontwikkelen en op peil te houden,
- Financiële entiteiten zijn verplicht een internationaal erkend beheersysteem voor informatiebeveiliging in te voeren.

Het ICT-risicobeheer vereist een reeks kernbeginselen die rond specifieke functies draaien (bv. Identificatie, bescherming en preventie, reactie en herstel, leren en evolueren, communicatie). Deze beveiligingsthema's kunnen worden teruggevoerd op de huidige technische normen en de *best practices* van de sector. De entiteiten die onder de DORA vallen, moeten op regelmatige en voortdurende basis nagaan wat alle bronnen van hun ICT-risicoconfiguratie zijn, beschermings- en preventiemaatregelen nemen,

onmiddellijk abnormale en verdachte activiteiten opsporen en een specifiek en alomvattend bedrijfscontinuiteitsbeleid uitwerken, naast disaster en recovery plannen.

De eindverantwoordelijkheid voor het beheer van ICT-risico's wordt overgelaten aan het leidinggevende orgaan van de financiële entiteit. De DORA bevat een lijst van taken en verplichtingen waaraan het management is onderworpen, zoals de expliciete verplichting om hun kennis van ICT-risico's te ontwikkelen en op peil te houden. Verder moeten financiële entiteiten hun ICT-risicolandschap in kaart brengen en beschikken over een volledig en uitgebreid kader voor ICT-risicobeheer, dat richting en sturing geeft aan alle werkzaamheden in verband met ICT-risicobeheer.

ICT Incident Reporting

- Implementeren van ICT-gerelateerde incident management processen en het ontwikkelen van capaciteiten om incidenten te monitoren, te behandelen en een follow-up aan te geven,
- Indiening van initiële, tussentijdse en eindrapporten over ICT-gerelateerde incidenten bij de relevante bevoegde autoriteit, overeenkomstig het in et voorstel uiteengezette proces,
- Indeling van incidenten volgens de in het voorstel genoemde factoren, bv. geografische spreiding, hoe kritisch de getroffen diensten zouden zijn en duur van het incident.

De DORA vermeldt ook de meldingsplicht van entiteiten, naast de invoering en implementatie van een beheersproces, bedoeld om ICT-gerelateerde incidenten te monitoren en te loggen. Deze incidenten worden vervolgens geclassificeerd op basis van criteria die in het voorstel zijn opgenomen en door de ETA's zijn ontwikkeld. Wanneer het incident als ernstig wordt geclassificeerd, moet het aan de relevante bevoegde autoriteit worden gemeld en in een gemeenschappelijk model worden geformatteerd, zodat de procedure zo geharmoniseerd is als de ETA's voor ogen hebben. Als een incident zich voordoet, moeten financiële entiteiten een initieel, tussentijds en eindrapport indienen. Daarnaast moeten cliënten en gebruikers worden geïnformeerd wanneer het incident gevolgen heeft of kan hebben voor hun financiële belangen.

Bovendien zal de DORA een meer gestroomlijnd meldingskanaal voor ICT-gerelateerde incidenten creëren, wat een welkome verbetering is ten opzichte van de huidige meervoudige meldingsvereisten. Het aantal triggers voor meldingen moet worden verminderd en het formaat voor meldingen zal worden geharmoniseerd. Dit volledig gestroomlijnde meldingskanaal leidt naar één EU-hub, in plaats van naar meerdere *National Competent Authorities* (NCA's).

Deze EU-hub zal alle meldingen van grote ICT-incidenten die gevolgen hebben voor financiële entiteiten verzamelen, waarbij de verzamelde gegevens gemeenschappelijke kwetsbaarheden en trends in de financiële sector aan het licht zullen brengen. Volgens de nieuwe EU-rapportageregels moeten alle financiële ondernemingen binnen een maand na een groot ICT-incident een rapport over de oorzaak van het incident indienen. Om de tijdige indiening van dergelijke rapporten te ondersteunen, zullen financiële entiteiten betrouwbare indicatoren voor vroegtijdige waarschuwing van ICT-verstoringen moeten implementeren.

Information & Intelligence Sharing

- Bewustmaking van nieuwe cyberdreigingen, betrouwbare oplossingen voor gegevensbescherming en tactieken voor operationele weerbaarheid,
- Informatie delen binnen vertrouwde gemeenschappen en uitvoering hiervan in overeenstemming met de toepasselijke wetgeving (bv. Gegevensbescherming, handelsgeheimen en mededinging).

Naast de rapportageverplichtingen wordt in het voorstel ook de nadruk gelegd op de functie van leren en ontwikkelen bij het delen en het uitwisselen van informatie over cyberdreigingen, tussen entiteiten binnen vertrouwde financiële gemeenschappen. Het doel van een dergelijke informatie-uitwisseling is het vergroten van het bewustzijn van nieuwe cyberdreigingen, betrouwbare oplossingen voor gegevensbescherming en tactieken voor operationele weerbaarheid.

ICT Third-party Risks

- Vaststellen van een kader voor kritieke ICT-risico's van thirdparty aanbieders,
- Vaststellen en regelmatig herzien van een strategie voor ICT-risico's met thirdparty aanbieders,
- Bijhouden van een register van informatie, controle outsourcing contracten en regelingen,
- ICT-concentratierisicobeoordeling en uitvoeren alvorens nieuwe contractuele regelingen aan te gaan.

Een van de meest opmerkelijke aspecten van de DORA is de aandacht die het besteedt aan thirdparty risico's. Hoewel de financiële sector steeds meer een beroep doet op ICT-bedrijven, lijkt er een gebrek te zijn aan specifieke bevoegdheden om ICT-risico's aan te pakken die voortvloeien uit deze derden partijen. De wet zou dienstverleners van kritieke thirdparty aanbieders binnen het bereik van de regelgevers brengen en hen aan een toezichtkader op EU-niveau onderwerpen.

Dit is waarschijnlijk de meest uitdagende pilaar van de DORA. Aanbieders, zoals clouddiensten, zullen gedwongen worden zich aan de toezichthouders te houden als zij als 'kritiek' worden aangemerkt. Enkele factoren die een dienstverlener van derden als kritiek zou classificeren, zijn:

- *Mate van vervangbaarheid* – CTPP's zijn moeilijker te vervangen in het geval van een operationele verstoring (die zich intern of in de omgeving van de verkoper voordoet)
- Het *aantal* financiële entiteiten dat voor de operationele continuïteit op de CTPP's vertrouwt

Zodra een third party aanbieder als kritiek is aangemerkt, zal het toezicht op die thirdparty worden uitgeoefend door een van de ETA's, die inspecties on-site en off-site zal kunnen uitvoeren, aanbevelingen zal kunnen doen en boetes zal kunnen opleggen die kunnen oplopen tot 1% van de dagelijkse wereldwijde omzet, en dit voor een periode van maximaal 6 maanden in geval van niet-naleving[13].

Hoe kunnen wij helpen?

Hoewel de DORA nog slechts een voorstel is, worden financiële entiteiten aangeraden nu al te beginnen met de naleving van de gestelde eisen.

De DORA is een zeer welkome katalysator voor de inspanningen om de digitale interne markt voor financiële diensten tot stand te brengen, aangezien de huidige omstandigheden vragen om de invoering van een geharmoniseerd kader op EU-niveau. Hoewel sommige verplichtingen naar verwachting geen grote veranderingen en gevolgen zullen hebben voor de huidige werkwijzen en bestaande frameworks, kunnen andere verplichting een stuk meer inspanning en tijd vergen. Naarmate de DORA haar definitieve vorm aanneemt, moeten ondernemingen zich bewust zijn van de omvang van de uitdaging die de tenuitvoerlegging met zich zal brengen. Een implementatieperiode van twee jaar is een vrij kort tijdsbestek om alles goed te regelen. Daarom kunnen bedrijven het zich simpelweg niet veroorloven te wachten tot het politieke proces is afgerond, en moeten zij nu al nagaan wat een succesvolle implementatie van hen vraagt.

Aangezien het een tijdrovende aangelegenheid kan zijn om zich vertrouwd te maken met deze voorschriften – zowel juridisch als op technisch niveau – en ervoor te zorgen dat deze worden nageleefd, mogen de ontwikkelingen naar aanleiding van dit voorstel niet aan de aandacht ontsnappen. Onze professionals kunnen u helpen de nieuwe verplichtingen te begrijpen en u ondersteunen bij de transformatie. Inzicht in de eisen en het herkennen van hiaten is de sleutel tot optimale ontwikkelingen en groei. Bekijk onze speciale diensten om u te helpen aan alle noodzakelijk vereisten te voldoen en ervoor te zorgen dat u volledig bent voorbereid op wat komen gaat.

Referenties:

1. A Europe fit for the digital age
2. The Digital Services Act: ensuring a safe and accountable online environment
3. The Digital Markets Act: ensuring fair and open digital markets
4. Digital finance package
5. Systemic cyber risk
6. A digital finance strategy for Europe
7. EUR-Lex - 52020PC0595 - EN - EUR-Lex
8. EUR-Lex - 52020PC0595 - EN - EUR-Lex
9. EUR-Lex - 52020PC0595 - EN - EUR-Lex
10. The European Banking Authority
11. The European Insurance and Occupational Pensions Authority
12. The European Securities and Markets Authority
13. EUR-Lex - 52020PC0595 - EN - EUR-Lex

Over CGI

CGI, opgericht in 1976, behoort tot de grootste IT- en business consultancy bedrijven ter wereld. CGI is actief op honderden locaties over de hele wereld en levert end-to-end diensten en oplossingen, waaronder strategisch IT- en business consultancy, systeem-integratie, managed IT en diensten op het gebied van bedrijfsprocessen.

cgi.com/nl