Goed voorbereid op de komst van DORA

Juli 2023

Dit is de eerste editie in een reeks AFM-publicaties over de Digital Operational Resilience Act (DORA). Deze editie is bedoeld voor alle ondernemingen die vanaf 2025 aan deze Europese verordening moeten voldoen. In deze uitgave worden de verschillende onderdelen van DORA toegelicht. Op deze manier kunnen ondernemingen kijken waar ze staan op het gebied van cyberveiligheid en welke stappen eventueel nog moeten worden genomen om aan de verordening te voldoen.

Lees verder

AFM

Inhoud

01 Wat betekent DORA voor de financiële sector?

Sinds januari 2023 is de Digital Operations Resilience Act (DORA) van kracht. DORA is een Europese verordening met als doel dat financiële organisaties IT-risico's beter beheersen en daarmee weerbaarder worden tegen cyberdreigingen. Er is namelijk sprake van scheefgroei tussen de toenemende IT-dreiging en de ontwikkeling van de weerbaarheid. Dit blijkt onder meer uit een recent rapport van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Ook zorgt de verordening voor verdere harmonisatie van IT-vereisten voor de financiële sector.

DORA stelt hiervoor onder meer eisen ten aanzien van IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico's bij uitbesteding aan (kritieke) derden. Daarbij wordt rekening gehouden met de grootte, het risicoprofiel en het systeembelang van individuele organisaties. Zo zijn zogeheten micro-ondernemingen bijvoorbeeld uitgesloten van verschillende onderdelen van de verordening en wordt voor het tweede hoofdstuk van DORA ('ICT-risicobeheer') een versimpeld kader ontwikkeld voor bepaalde vergunningstypes. In de volgende secties wordt dit verder toegelicht.

Daarnaast zijn er nog twee aanvullende effecten die bijdragen aan de weerbaarheid van financiële instellingen. Ten eerste beoogt DORA de ketenveiligheid te verbeteren. De verordening bevat namelijk ook een kader dat van toepassing zal zijn op de meest kritieke ICT-dienstverleners voor de financiële sector. Tenslotte treft de verordening ook een regeling voor informatie-uitwisseling, zodat financiële instellingen onderling informatie en inlichtingen over cyberdreigingen kunnen uitwisselen en risico's daarmee verder kunnen beperken.

Ondernemingen hebben tot januari 2025 de tijd om aan de regelgeving te voldoen. Daarna is DORA officieel van toepassing en zal de AFM toezicht houden op de verordening. Voor een deel van de ondernemingen gelden nu overigens ook al DORA-gerelateerde vereisten vanuit bestaande wet- en regelgeving.

02 Aan de slag voor een verhoogde digitale weerbaarheid

Ondernemingen kunnen al starten met het analyseren van de huidige gap met DORA en het opzetten van daaruit volgende activiteiten. Om in januari 2025 aan DORA te kunnen voldoen, is het raadzaam dat ondernemingen hier zo vroeg mogelijk mee beginnen.

Een deel van de onderwerpen wordt op dit moment door de ESA's (European Supervisory Authorities) in meer detail uitgewerkt in *Regulatory* en *Implementing Technical Standards* (RTS en ITS). Deze thema's zijn wel al op hoofdlijnen beschreven in DORA. De overige onderwerpen uit de verordening zullen niet verder uitgewerkt worden. Ondernemingen kunnen dus al aan de slag met de huidige teksten.

De volgende secties bieden handvatten voor de voorbereiding op DORA langs de vier hoofdonderwerpen van de verordening. Daarnaast lopen de aspecten governance en organisatie als een rode draad door de DORA-hoofdstukken, waardoor deze in de laatste sectie separaat worden behandeld. Per onderwerp is ook opgenomen op welke onderdelen momenteel aanvullende standaarden worden ontwikkeld en op welke momenten deze zullen worden voorgelegd aan de Europese Commissie (EC).

ICT-risicobeheer

Ondernemingen kunnen nu al aan de slag met:

- Het framework voor ICT-risicomanagement, in lijn met het Enterprise Risk Management;
- De inrichting van monitoring, behandeling en follow-up van afwijkende activiteiten, inclusief de inrichting van back-ups;
- Het ICT-bedrijfscontinuïteitsplan dat periodiek wordt getest;
- Awareness-programma's op het gebied van IT, in lijn met het takenpakket van de medewerkers.

IT-risicomanagement is een belangrijk middel om op gestructureerde wijze IT-risico's te detecteren en te beheersen. DORA beschrijft zowel de procesmatige kant van risicobeheer, als de uitwerking in technische maatregelen. Als basis vereist DORA een *governance and control framework*, zodat ondernemingen een controlecyclus inrichten en er continue kan worden geëvalueerd.

Een belangrijk onderdeel is ook de toewijzing van de benodigde rollen op het gebied van IT-beheersing, zoals een onafhankelijke functie voor de beheersing van ICT-risico's en een internal auditor die het framework periodiek beoordeelt.

Naast het governance and control framework schrijft DORA ook een specifiek *ICT risk management framework* (ICT RMF) voor. IT hangt sterk samen met andere bedrijfsprocessen, waardoor dit framework in lijn dient te zijn met het *enterprise risk management* (ERM). Voor een aantal vergunningstypes wordt een RTS ontwikkeld waarin een versimpelde richtlijn voor het inrichten van het *ICT risk management framework* is opgenomen.

Business Continuity Management (BCM) op het gebied van IT is van belang om de stabiliteit van de dienstverlening van een onderneming te kunnen waarborgen. DORA schrijft dan ook voor dat BCM-plannen periodiek worden getest en dat de benodigde crisiscommunicatie is ingericht.

Naast preventie spelen ook reactieve maatregelen een belangrijke rol. Zo vereist DORA dat ondernemingen detectiemechanismen inrichten, evenals processen en technieken voor de afhandeling van gedetecteerde afwijkingen. Belangrijk onderdeel hiervan is ook de inrichting van back-ups, voor het geval dat risico's zich toch manifesteren.

Medewerkers spelen een belangrijke rol in de uitvoer van het IT-beleid. DORA zet daarom ook in op de ontwikkeling van IT-bewustwordingsprogramma's, waarbij rekening moet worden gehouden met de verschillen in werkzaamheden van medewerkers.

Aanvullende uitwerking	Beschrijving	Voorlegging aan de EC
RTS voor artikel 15	Further harmonisation of ICT risk management tools, methods, processes and policies	Uiterlijk 17 januari 2024
RTS voor artikel 16(3)	Simplified ICT risk management framework	Uiterlijk 17 januari 2024

ICT-gerelateerde incidenten

Ondernemingen kunnen nu al aan de slag met:

- Het proces voor het detecteren en afhandelen van incidenten;
- Het bijhouden van een overzicht met voorgedane IT-incidenten.

Het is belangrijk dat IT-incidenten adequaat worden afgehandeld. Voor een effectief incidentmanagement verwacht DORA dat ondernemingen een proces inrichten voor het detecteren en afhandelen van ICT-incidenten en cyberdreigingen.

Daarnaast moeten ondernemingen ook registreren welke incidenten zich voor hebben gedaan. Dit bevordert namelijk een zorgvuldige afhandeling en opvolging van incidenten, en biedt de mogelijkheid voor evaluaties en *root cause* analyses.

DORA schrijft voor dat belangrijke IT-incidenten moeten worden gemeld aan de toezichthouder. Dit is momenteel ook al verplicht. Criteria en templates voor de meldplicht vanuit DORA worden momenteel ontwikkeld. Zie onderstaande tabel voor de bijbehorende tijdslijnen.

Aanvullende uitwerking	Beschrijving	Voorlegging aan de EC
RTS voor artikel 18(3)	Classification of ICT-related incidents and cyber threats	Uiterlijk 17 januari 2024
RTS voor artikel 20(a)	Reporting content and templates	Uiterlijk 17 juli 2024
ITS voor artikel 20(b)	ITS to establish the reporting details for major ICT related incidents	Uiterlijk 17 juli 2024

Testen van digitale operationele weerbaarheid

Ondernemingen kunnen nu al aan de slag met:

- Een risicogebaseerd programma voor het testen van de digitale operationele weerbaarheid.

Door regelmatig te testen krijgt een onderneming inzicht in de feitelijke veiligheid van de IT-omgeving en kunnen gericht verbeteringen worden doorgevoerd. DORA schrijft daarom voor dat ondernemingen een risicogericht programma moeten ontwikkelen voor het testen en verhogen van de digitale weerbaarheid. De inhoud van dit programma is afhankelijk van het vastgestelde risicoprofiel van een onderneming. Er zijn verschillende soorten tests denkbaar, waaronder kwetsbaarhedenscans, pentesten en red teaming.

DORA past onder andere voor dit onderwerp proportionaliteit toe voor zogeheten micro-ondernemingen, waardoor deze uitgezonderd zijn van de betreffende artikelen over dit onderwerp.

Aanvullende uitwerking	Beschrijving	Voorlegging aan de EC
RTS voor artikel 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Uiterlijk 17 juli 2024

Beheer van ICT-risico van derde aanbieders

Ondernemingen kunnen nu al aan de slag met:

- Een strategie en de inrichting van risicomanagement op het gebied van ICT-uitbestedingen;

DORA besteedt veel aandacht aan *third party risk* om op deze wijze ketenrisico's zo veel mogelijk te beperken. Van ondernemingen wordt vereist dat ze *third party risk* expliciet opnemen in het *ICT risk management framework* en een strategie ontwikkelen voor (IT-)uitbestedingen.

De verordening schrijft ook voor welke onderdelen belangrijk zijn om rekening mee te houden bij een uitbesteding. Zo moet een onderneming altijd wederzijds geaccordeerde afspraken met de dienstleverancier vastleggen over de *service levels* (bijv. in Service Level Agreements). Voor kritieke uitbestedingen moet altijd een exit-strategie beschikbaar zijn. Daarnaast zijn er enkele vaste elementen die de onderneming op moet nemen in een overeenkomst. Een voorbeeld hiervan is de bevoegdheid om een inspectie of audit uit te voeren, zij het door de instelling, een daartoe aangestelde derde partij of de bevoegde toezichtautoriteit.

Ook moet een onderneming een register bijhouden van bestaande uitbestedingen, inclusief relevante kenmerken.

Aanvullende uitwerking	Beschrijving	Voorlegging aan de EC
RTS voor artikel 28(1)	General principles for a sound management of ICT third-party risk	Uiterlijk 17 januari 2024
ITS voor artikel 28(9)	Register of information	Uiterlijk 17 jan 2024
RTS voor artikel 30(5)	Key contractual provisions	Uiterlijk 17 juli 2024
Input for advice on criticality criteria t.b.v. artikel 31(6)	n.v.t.	Uiterlijk 17 juli 2024
Selectie van kritieke IT-dienstverleners t.b.v. artikel 31	n.v.t.	Geen tijdslijn gecommuniceerd

Rode draden governance en organisatie

Ondernemingen kunnen nu al aan de slag met:

- De toewijzing van de benodigde, voldoende onafhankelijke IT-rollen in lijn met het Three Lines model;
- Continue evaluatie van de IT-inrichting en -beheersing.

De onderwerpen governance en organisatie spelen een belangrijke rol in DORA en komen in alle onderdelen naar voren. Zo is voor veel van de processen die de verordening voorschrijft, opgenomen dat ondernemingen de bijbehorende rollen en verantwoordelijkheden duidelijk moeten toewijzen.

Daarnaast legt DORA ook veel nadruk op de inrichting van het Three Lines model. Hierbij wordt verwacht dat ondernemingen zowel een controle- als auditfunctie benoemen, en deze voldoende onafhankelijk positioneren binnen de organisatie. Ook wordt voor een deel van de beschreven processen vereist dat deze continue worden geëvalueerd en dat dit procesmatig geborgd is.

Onderdeel van de verordening is ook dat bestuurders hun kennis op peil dienen te houden door het volgen trainingen en opleidingen.

03 **Vooruitblik**

De komende tijd worden de RTS'en en ITS'en verder ontwikkeld volgens de overzichten die in de vorige secties zijn opgenomen. De ESA's zullen deze via publieke consultatie ook voorleggen aan ondernemingen in de financiële sector, waarbij er op de stukken gereageerd kan worden.

De AFM bereidt zich in de tussentijd voor op het uitvoeren van DORA-toezicht. In de volgende publicaties uit deze reeks zal dieper worden ingegaan op deelonderwerpen uit de verordening. De volgende editie zal in het derde kwartaal van 2023 worden gepubliceerd.

Voor meer informatie over de scope van DORA kunnen onder andere de volgende onderdelen uit de verordening worden geraadpleegd:

- Het toepassingsgebied is beschreven in artikel 2;
- Definities (zoals 'micro-onderneming') zijn uitgewerkt in artikel 3.

Verdere vragen? Neem contact op met het ondernemersloket van de AFM.

Heeft u vragen of opmerkingen over deze publicatie?

Stuur een e-mail naar: redactie@afm.nl

Autoriteit Financiële Markten
Postbus 11723 | 1001 GS Amsterdam

Telefoon
020 797 2000

www.afm.nl

Volg ons: →

De AFM maakt zich sterk voor eerlijke en transparante financiële markten. Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.