ICTRECHT

Cheatcheet

DORA

Lees verder

Scope

Doel van DORA

Zorgen dat de financiële sector
weerbaarder wordt tegen cyberdreigingen.

Voor wie?

01 Financiële entiteiten

DORA is primair van toepassing op organisaties in de financiële sector (“financiële entiteiten”). Kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatiediensten, instellingen voor elektronisch geld, beleggingsondernemingen, aanbieders van cryptoactivadiensten, centrale effectenbewaarinstellingen, centrale tegenpartijen, handelsplatformen, transactieregisters, beheerders van alternatieve beleggingsinstellingen, beheermaatschappijen, aanbieders van datarapporteringsdiensten, verzekerings- en herverzekeringsondernemingen, (her-/neven-) verzekeringstussenpersonen, instellingen voor bedrijfspensioenvoorziening, ratingbureaus, beheerders van kritieke benchmarks, aanbieders van crowdfundingdiensten, securisatieregisters.

02 Leveranciers van kritieke ICT-diensten

Naast financiële entiteiten, is DORA van toepassing op aanbieders van ICT-diensten die leveren aan de financiële entiteiten (met onderscheid tussen leveranciers van kritieke en niet-kritieke ICT-diensten). ICT-leveranciers die van cruciaal belang zijn voor financiële instellingen (kritieke ICT-dienstverleners) krijgen te maken met direct toezicht: dit brengt mee dat zij zich onder meer moeten houden aan specifieke normen voor ICT-risicobeheer en cyberweerbaarheid. Dit vormt een aanzienlijke verschuiving die hen onder een vergelijkbaar toezicht plaatst als de financiële instellingen die zij bedienen.

Vijf pijlers

DORA wordt opgedeeld in vijf pijlers. Elke pijler is van cruciaal belang voor het creëren van een veilige en betrouwbare digitale financiële omgeving.

01 **ICT Risico Management**

Organisaties zijn verplicht te beschikken over een gedegen kader voor het ICT-risicobeheer.

02 **Incident Management**

Organisaties zijn verplicht melding te doen van ernstige ICT-gerelateerde incidenten en, op vrijwillige basis, van significante cyberdreigingen aan de bevoegde autoriteiten.

03 **Weerbaarheids-testen**

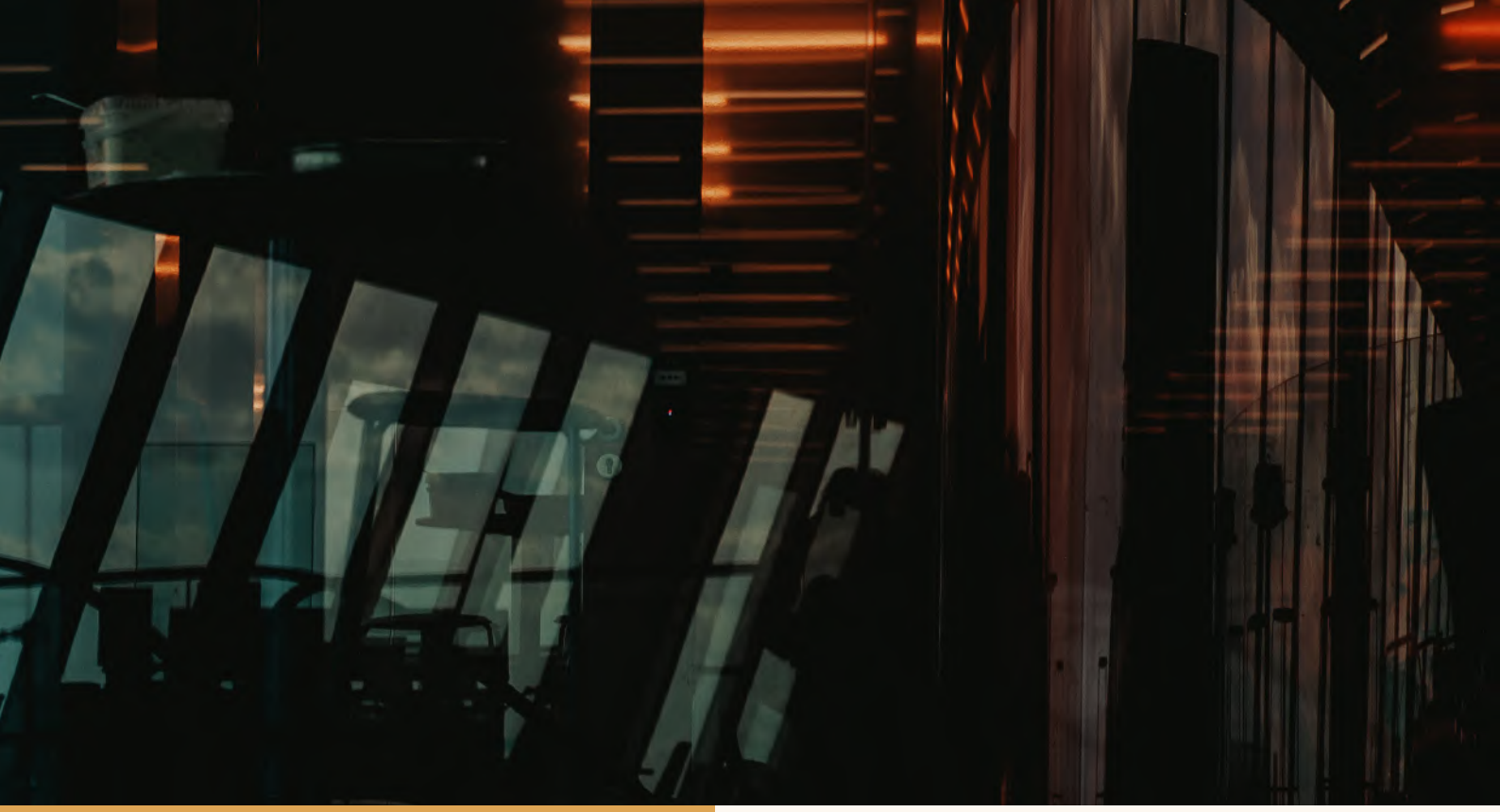
Organisaties zijn verplicht om regelmatig hun digitale operationele weerbaarheid te testen, door middel van onder andere kwetsbaarhedenscans en penetratietesten.

02 **Derde ICT-aan-bieders Risico Management**

Organisaties zijn verplicht een gedegen kader vast te stellen voor het beheer van risico's van (kritieke) externe ICT-dienstverleners.

03 **Informatie uitwisseling**

Organisaties worden aangemoedigd informatie en kennis met betrekking tot cyberdreigingen en -kwetsbaarheden te delen binnen vertrouwde financiële gemeenschappen. Daar moeten echter wel goede afspraken over worden gemaakt.



Sancties

Er zijn aanzienlijke boetes voor de niet-naleving van de verplichtingen die uit DORA voortkomen. Financiële instellingen die de verplichtingen niet nakomen kunnen te maken krijgen met verschillende administratieve strafmaatregelen en corrigerende maatregelen.

Zo kan De Nederlandsche Bank (“DNB”) onder meer:

- Toegang verkrijgen tot documenten en gegevens (bijvoorbeeld middels inspecties of onderzoeken)
- Eisen dat financiële instellingen bepaalde gedragingen tijdelijk of definitief staken;
- Openbare meldingen of mededelingen doen over de inbreuk, inclusief identiteit van de organisatie die de inbreuk heeft gemaakt
- Financiële instellingen boetes opleggen; en
- Eisen dat bepaalde overzichten van dataverkeer worden overgelegd door telecommunicatiediensten.

Een EU-lidstaat kan tevens besluiten strafrechtelijke maatregelen op te leggen voor inbreuken waarop in het nationale recht strafrechtelijke maatregelen staan.

Kritieke IT-dienstverleners die zich niet aan de regels houden kunnen boetes in de vorm van een dwangsom krijgen tot wel 1% van de wereldwijde gemiddelde dagomzet. Deze boetes kunnen dagelijks aan bedrijven worden opgelegd, totdat zij compliant zijn. Als gevolg van reputatieschade en verlies van vertrouwen bij klanten kan niet-naleving nog schadelijker zijn.

Vanaf wanneer?

17 januari 2023:	DORA is in werking getreden
17 januari 2024:	De eerste reeks van gewenste Regulatory Technical Standards worden uitgegeven
17 juli 2024:	De tweede en laatste reeks van Regulatory Technical Standards worden uitgegeven
17 januari 2025:	Volledige compliance met DORA en Regulatory Technical Standards vereist

ICTRECHT

Wil je meer weten over de DORA?

Bezoek onze website voor het laatste nieuws, onze diensten en trainingen.

Vragen?

- www.ictrecht.nl/dora
- 020 - 663 1941