Rapport

DORA Pilot Handelaren voor Eigen Rekening

Verkennend onderzoek

20 december 2024

Inhoudsopgave

1 Inleiding

Op 14 december 2022 heeft het Europees Parlement nieuwe regelgeving met betrekking tot cybersecurity vastgesteld: de Digital Operations Resilience Act (**DORA**). DORA geeft een regelgevend kader voor financiële instellingen binnen de EU voor de weerbaarheid en veerkracht van ICT-beveiliging en treedt in werking op 17 januari 2025.

De AFM heeft een onderzoek gedaan in de vorm van een pilot bij een beperkt aantal Handelaren voor Eigen Rekening (**HER**). Het doel van het pilot onderzoek was om met een beperkte scope vast te stellen in hoeverre de instellingen voldoen aan de eisen van DORA, dan wel goed op weg zijn om per 17 januari 2025 compliant te zijn. De scope van het onderzoek was gericht op drie gebieden binnen de '*DORA Regulatory Technical Standards (**RTS**) tot vaststelling van tools, methoden, processen en beleidslijnen voor ICT-risicobeheersing'*. Dit betrof specifiek:

1 Beheer ICT-Assets
   - Artikel 4 – Beleid voor het beheer van ICT-assets
   - Artikel 5 – Procedure voor het beheer van ICT-assets

2 ICT-projectmanagement en ICT-wijzigingsbeheer
   - Artikel 17 – ICT-wijzigingsbeheer

3 Toegangscontrole
   - Artikel 20 – Identiteitsbeheer
   - Artikel 21 – Toegangscontrole

Deze drie gebieden en artikelen bestaan uit IT-processen waarvoor reeds in de Wet Financieel Toezicht (**Wft**) en de Markets in Financial Instruments Directive (**MiFiD**) vereisten staan. Bovengenoemde processen waren het focusgebied voor dit pilot onderzoek. Daarnaast heeft de AFM de intra-groepafspraken besproken die binnen de instellingen zijn gemaakt indien deze van toepassing zijn voor de uitvoering van de IT-processen in scope.

De AFM heeft voor deze pilot onderliggende documentatie opgevraagd voor de betreffende IT-processen. In een gesprek met de HER is de documentatie en het onderliggende IT-proces besproken ter verduidelijking. Hiermee heeft de AFM een eerste inzicht gekregen in de huidige opzet van de IT-processen. Daaruit zijn aandachtspunten voortgekomen die mogelijk ook relevant zijn voor andere marktpartijen.

2 Resultaten

2.1 Algemene aandachtspunten

Gebaseerd op de ontvangen documentatie en gesprekken heeft de AFM een aantal algemene aandachtspunten opgesteld. Deze zijn overkoepelend van toepassing op de IT-processen in scope, of komen voort uit gelieerde onderwerpen die zijn besproken, zoals interne uitbesteding. Sommige aandachtspunten vallen hierdoor niet direct in de oorspronkelijke scope van het onderzoek, maar zijn in bredere zin van DORA wel van belang.

1 **Documentatie.** Onderzochte partijen waren niet goed in staat om hun gedocumenteerde IT-beleid en IT-procedures op te leveren, op basis waarvan kan worden vastgesteld dat zij compliant zijn met de vereisten van DORA. Voor partijen die recent beleid hebben opgesteld, signaleert de AFM het risico van een niet-coherente DORA compliance aanpak.

2 **Volledigheid IT-beleid.** Het IT-beleid en IT-procedures van partijen waren niet volledig in lijn met de vereisten, zoals gesteld in de DORA RTS tot vaststelling van tools, methoden, processen en beleidslijnen voor ICT-risicobeheersing. In deze RTS staat specifiek voorgeschreven welke elementen verplicht deel uitmaken van het beleid of procedure. Mocht een element niet direct van toepassing zijn op een financiële entiteit, dan dient dit als zodanig beschreven te worden in het beleid. Als voorbeeld kan een financiële entiteit ervoor kiezen om haar ICT-assets niet bloot te stellen aan externe netwerken (zie artikel 4(2) van de RTS voor ICT-risicobeheersing). Deze keuze dient dan te worden vastgelegd als onderdeel van het beleid op het beheer van ICT-assets.

3 **Bewustheid bij bestuurders**. DORA schrijft voor dat de raad van bestuur aantoonbaar op de hoogte moet zijn van informatiebeveiliging. Het bestuur is verantwoordelijk voor het niveau van informatiebeveiliging voor alle (uitbestede) partners in de volledige end-to-end uitbestedingsketen. Er moet een risico-gebaseerd monitoringsysteem zijn voor al deze informatiebeveiligingsaspecten.

4 **Interne uitbesteding**. In DORA wordt interne uitbesteding in principe gelijkgesteld aan externe uitbesteding. Dit houdt in dat de Nederlandse geregistreerde entiteit uitbestedingsovereenkomsten moet hebben met alle groepsentiteiten die IT-diensten leveren. Bovendien is de Nederlandse entiteit verplicht om een volwaardig Informatieregister te hebben.

5 **Teamprocedures**. Het hanteren van meerdere gedetailleerde procedures met betrekking tot processen zoals wijzigingsbeheer en gebruikerstoegang door verschillende teams binnen een instelling is een aandachtspunt. Deze procedures moeten niet afwijken van het interne beleid om in lijn te zijn met de vereisten van DORA. Het hebben van meerdere procedures is geen risico op zichzelf, maar vraagt wel om meer tijd en aandacht om deze compliant te houden.

6 **Werking beleid en processen**. Naast het in lijn brengen van het beleid en processen met DORA, moeten instellingen ook kunnen aantonen dat zij op die manier werken. Met het aantonen van de werking, naast de opzet, is de instelling compliant met DORA.

2.2 Aandachtspunten voor beheer ICT-assets, ICT-wijzigingsbeheer, identiteitsbeheer en toegangscontrole

Naast de algemene aandachtspunten heeft de AFM ook een aantal meer specifieke aandachtspunten voor de gebieden waar de pilot zich hoofdzakelijk op gefocust heeft: beheer ICT-assets, ICT-wijzigingsbeheer, identiteitsbeheer en toegangscontrole. De gegeven aandachtspunten komen vooral voort uit de specifieke vereisten van de RTS tot vaststelling van tools, methoden, processen en beleidslijnen voor ICT-risicobeheersing.

1 **Classificeren van informatie en systemen**. In artikel 5 van de DORA RTS over ICT-risicobeheer wordt beschreven dat de classificatie van informatie (data) en systemen gebaseerd moet zijn op de criteria beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid. De classificatie van informatie en systemen zijn vervolgens in lijn met de classificatie van ICT-ondersteunde bedrijfsfuncties zoals beschreven in artikel 8, lid 1, van de DORA verordening.

2 **Audit trail wijzigingsbeheer**. Er moet een volledige audit trail aanwezig zijn, waarbij de scheiding van taken aangetoond wordt. Het is belangrijk om IT-wijzigingen en de goedkeuringen van deze wijzigingen te documenteren. Dit is vooral van toepassing als de goedkeuring van wijzigingen wordt gegeven in vergaderingen of als er meerdere systemen worden gebruikt voor het wijzigingsbeheer, zoals een pipeline en servicemanagementsysteem.

3 **Verbanden en onderlinge afhankelijkheden ICT-assets**. In artikel 4, lid 2 van de RTS voor ICT-risicobeheersing staat dat de financiële entiteit in haar beleid voor het beheer van ICT-assets vastlegt hoe wordt omgegaan met de verbanden en onderlinge afhankelijkheden tussen ICT-assets en de bedrijfsfuncties die van deze ICT-asset gebruikmaken. Dit vereist extra aandacht van entiteiten die gebruikmaken van meerdere vastleggingen en overzichten voor hun ICT-assets, om dit verband en onderlinge afhankelijkheden goed te documenteren en te bewaken.

4 **ICT-assets definitie.** Het beleid voor het beheer van ICT-assets en vastlegging in overzichten is vooral gefocust op hardware. Terwijl de definitie van ICT-assets, zoals gegeven in artikel 3(7) van de DORA verordening, zowel hardware als software omvat. Extra aandacht is nodig om ook de softwarecomponenten in voldoende mate te vangen in het beleid en de procedure voor het beheer van ICT-assets.

5 **ICT user-access**. Binnen een aantal onderzochte instellingen heeft de AFM niet kunnen vaststellen dat er een gedocumenteerde werkwijze is ten aanzien van user-access. Password beveiliging is meestal goed georganiseerd, maar een systematiek voor user-profielen en daaraan gekoppeld de user-ID's ontbraken.

3 Conclusie en aanbevelingen

Op basis van de documentatie en gesprekken met een beperkt aantal HER is de conclusie dat de mate waarin instellingen klaar zijn voor DORA per 17 januari 2025 in grote mate verschilt. Een aantal partijen is kortgeleden gestart met de implementatie van de DORA-eisen binnen hun organisatie en het lijkt onwaarschijnlijk dat zij per 17 januari 2025 DORA compliant zullen zijn. Bij andere partijen is het de vraag of zij volledig compliant zijn met alle specifieke vereisten van DORA.

Gebaseerd op de gegeven aandachtspunten heeft de AFM de volgende aanbevelingen:

- Voer een gap analyse uit om na te gaan of alle vereiste elementen uit DORA ingebed zijn in de beleidsstukken en procedures. Hiervoor kan hulp worden ingeschakeld van een externe adviseur of tweedelijnsfunctie (compliance, riskmanagement). Zodra het beleid en procedures in lijn met DORA is geïmplementeerd kan een interne- of externe audit worden uitgevoerd om assurance te verkrijgen voor opzet, bestaan en werking.

- Partijen die afhankelijk zijn van een groepsentiteit voor het uitvoeren van hun IT-processen, moeten er zorg voor dragen dat hun intragroep uitbestedingsovereenkomst de ontvangen diensten volledig dekt. Daarbij wordt onder DORA interne uitbesteding in principe beschouwd als externe uitbesteding, waardoor in beginsel dezelfde eisen van toepassing zijn. Een review van de intragroep uitbestedingsovereenkomst wordt aangeraden om na te gaan of deze voldoet aan de eisen van DORA.

- Voor een geïntegreerde benadering van ICT-risicobeheer is het van belang om alle informatiebeveiligingscriteria (beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit) mee te wegen in het classificeren van alle ICT-ondersteunende bedrijfsfuncties en de informatie- en ICT-assets. Deze classificatie moet indien nodig en ten minste eenmaal per jaar worden geëvalueerd. Het wordt daarom aangeraden om dit vooruit te plannen aangezien het veel tijd kost om alle ICT-ondersteunde bedrijfsfuncties en de informatie- en ICT-assets te classificeren. Ook hier geldt dat er sprake moet zijn van een aantoonbaar en vastgelegd proces.

Los van het uitgevoerde onderzoek vraagt de AFM nog aandacht voor het informatieregister. Nadat DORA in werking treedt op 17 januari 2025 wordt het informatieregister als eerste opgevraagd bij de marktpartijen. De AFM dient deze registers aan te leveren bij de EBA op 30 april 2025. De AFM is voornemens om hiertoe in februari 2025 een informatieverzoek te versturen naar alle ondernemingen met een AFM-vergunning die onder DORA vallen.