

# ICT-recovery in de asset management sector

**In het kort** - Het risico op verstoringen en uitval van ICT neemt toe. Daarom is het belangrijk dat financiële instellingen hun ICT snel en effectief kunnen herstellen. Dit vermogen om systemen, data en processen na een verstoring of uitval weer operationeel te krijgen, wordt ook wel ICT-recovery genoemd. De AFM heeft onderzocht bij vijf grote institutionele asset managers hoe zij hun ICT-recovery hebben ingericht en hoe goed zij zijn voorbereid op het herstellen van ICT na een verstoring of uitval. De AFM vraagt alle asset managers de aandachtspunten in het rapport te bestuderen en daar waar nodig op te pakken.

# Samenvatting

**Financiële instellingen zijn voor hun dienstverlening steeds afhankelijker van ICT. Tegelijkertijd nemen de risico's toe, bijvoorbeeld door cyberaanvallen, geopolitieke spanningen en toepassingen van nieuwe kunstmatige intelligentie (AI).** AI kan bijvoorbeeld worden ingezet om kwetsbaarheden in systemen sneller op te sporen. Om deze risico's in de hele Europese Unie op een uniforme manier aan te pakken, is in januari 2025 de Digital Operational Resilience Act (DORA) volledig van kracht geworden. DORA stelt eisen aan financiële instellingen, waaronder asset managers, om hun digitale weerbaarheid te versterken.

**Digitale weerbaarheid is al jaren een belangrijke prioriteit in het toezicht. Financiële instellingen moeten niet alleen maatregelen nemen om ICT-verstoringen te voorkomen, maar ook hun ICT snel kunnen herstellen als systemen uitvallen.** Het geheel aan processen, maatregelen en voorzieningen om systemen, data en dienstverlening na een verstoring of uitval weer operationeel te krijgen, wordt ook wel ICT-recovery genoemd. Om meer inzicht te krijgen in de inrichting van ICT-recovery is onderzoek gedaan bij een aantal grote institutionele asset managers.

**Uit het onderzoek blijkt dat deze asset managers op hoofdlijnen zijn voorbereid op ICT-uitval. Tegelijkertijd zijn er aandachtspunten die kunnen bijdragen aan een effectievere inrichting van ICT-recovery:**

- Zorg voor een consistente identificatie en classificatie van (kritieke) functies;
- Stel hersteldoelstellingen vast op functies;
- Neem eigen herstellereisten mee in contracten met ICT-dienstverleners;
- Test hersteldoelstellingen aan de hand van verschillende extreme scenario's.

**Asset managers wordt gevraagd deze aandachtspunten te bestuderen en waar nodig verbeteringen door te voeren.**

# Inhoudsopgave

|                                                                                                  |           |
|--------------------------------------------------------------------------------------------------|-----------|
| <b>Samenvatting</b>                                                                              | <b>2</b>  |
| <b>Inhoudsopgave</b>                                                                             | <b>3</b>  |
| <b>1. DORA en onderdelen van ICT-recovery</b>                                                    | <b>4</b>  |
| <b>2. Achtergrond van het verkennend onderzoek</b>                                               | <b>5</b>  |
| <b>3. Aandachtspunten bij ICT-recovery</b>                                                       | <b>6</b>  |
| Aandachtspunt 1: Zorg voor consistente identificatie en classificatie van de (kritieke) functies | 6         |
| Aandachtspunt 2: Definieer hersteldoelstellingen op functies                                     | 6         |
| Aandachtspunt 3: Neem eigen herstelvereisten mee in contracten met ICT-dienstverleners           | 6         |
| Aandachtspunt 4: Test hersteldoelstellingen aan de hand van verschillende extreme scenario's     | 7         |
| <b>4. Conclusie</b>                                                                              | <b>8</b>  |
| <b>Bijlage 1 Belangrijkste bepalingen</b>                                                        | <b>9</b>  |
| <b>Bijlage 2 Definities</b>                                                                      | <b>10</b> |

# 1. DORA en onderdelen van ICT-recovery

**DORA beoogt de digitale weerbaarheid van financiële instellingen te versterken. Het richt zich met name op maatregelen om de risico's rondom verstoringen en uitval van ICT bij financiële instellingen zo veel mogelijk te beperken.** Denk hierbij aan uitval door een cyberaanval, of calamiteit maar ook menselijke fouten. Onderdeel hiervan zijn vereisten gericht op de continuïteit van de bedrijfsvoering, de respons op verstoringen en het herstel van ICT bij verstoringen zoals uitval van ICT (ICT-recovery).

**DORA vereist dat financiële instellingen verschillende onderdelen van hun ICT-recovery inrichten en documenteren. Hieronder worden de belangrijkste onderdelen toegelicht:**

- **Business Impact Analyse (BIA):** Er moet een analyse worden gemaakt van de impact die verstoringen van de bedrijfsactiviteiten hebben op de financiële instelling. In de BIA wordt rekening gehouden met de kritieke aard van geïdentificeerde en in kaart gebrachte functies, ondersteuningsprocessen, afhankelijkheden van derden en informatieactiva, en hun onderlinge afhankelijkheden;
- **Hersteldoelstellingen:** Hieronder worden in DORA verstaan de Recovery Time Objective (RTO, ofwel maximaal acceptabele hersteltijd) en de Recovery Point Objective (RPO, ofwel maximaal acceptabel gegevensverlies weergegeven in tijd) van de functies. De financiële instelling stelt deze hersteldoelstellingen per functie vast. Bij deze vaststelling houdt de financiële instelling mede rekening met de gevolgen van verstoringen en de relevante afhankelijkheden die uit de BIA blijken;
- **ICT-respons en -herstelplan (ICT-herstelplan):** Hierin beschrijft een financiële instelling per relevante functie of ICT-asset de maatregelen die nodig zijn voor het herstel van de situatie voor uitval van de ICT. Denk hierbij onder meer aan welke processen moeten worden hersteld, de volgorde van herstel, maatregelen zoals redundante voorzieningen, uitwijklocaties en back-ups en de governance. Het ICT-herstelplan moet zodanig zijn ingericht dat de vastgestelde hersteldoelstellingen kunnen worden behaald;
- **(ICT-)business continuïteitsplan (BCP):** Hierin beschrijft de financiële instelling de maatregelen waardoor de instelling haar bedrijfsvoering kan continueren tijdens verstoringen of uitval van ICT. Denk bijvoorbeeld aan alternatieve werkwijzen;
- **Communicatieplan:** In geval van verstoringen of uitval is het nodig dat er is nagedacht over de communicatie, zowel naar interne als naar externe stakeholders. Dit moet in een plan zijn vastgelegd, inclusief duidelijke rollen, verantwoordelijkheden en procedures en is afhankelijk van de ernst van de verstoring of uitval;
- **Testen:** Regelmatig testen maakt inzichtelijk of de ICT-systemen die functies ondersteunen daadwerkelijk binnen de gestelde hersteldoelstellingen kunnen worden hersteld en of medewerkers hun taken kennen. De uitkomsten van deze tests worden gebruikt om de inrichting van de ICT-recovery verder te verbeteren.

## 2. Achtergrond van het verkennend onderzoek

**Voor dit verkennende onderzoek naar ICT-recovery zijn vijf institutionele asset managers onderzocht. Het onderzoek is gebaseerd op documentonderzoek en gesprekken met deze instellingen.** Het doel was inzicht te krijgen in de manier waarop zij zijn voorbereid op ICT-uitval en het herstel daarvan. Voor een effectieve ICT-recovery is het belangrijk dat instellingen hun functies, informatie-assets en ICT-assets goed in beeld hebben, inclusief de onderlinge afhankelijkheden. Ook moeten hersteldoelstellingen zijn vastgesteld. Deze vormen de basis voor maatregelen die de continuïteit van de dienstverlening ondersteunen en bijdragen aan een snel herstel na ICT-uitval.

**De aandachtspunten in dit rapport zijn grotendeels gebaseerd op algemene uitgangspunten voor ICT-recovery en zijn daarom in beginsel relevant voor alle asset managers.** De mate waarin instellingen deze aandachtspunten moeten uitwerken, hangt af van hun aard, omvang en complexiteit. Op proportionaliteit wordt in dit rapport niet verder ingegaan.

### 3. Aandachtspunten bij ICT-recovery

**De onderzochte asset managers zijn op hoofdlijnen voorbereid op ICT-uitval. Het onderzoek laat tegelijk zien dat verbeteringen mogelijk zijn op een aantal onderdelen van ICT-recovery.** De vier aandachtspunten in dit rapport bieden handvatten voor een verdere versterking van de digitale weerbaarheid. Asset managers wordt gevraagd deze aandachtspunten waar nodig op te pakken.

#### Aandachtspunt 1: Zorg voor consistente identificatie en classificatie van de (kritieke) functies

**Financiële instellingen moeten alle door ICT ondersteunde functies identificeren, classificeren en documenteren.** Hieronder valt ook het indelen van functies in kritieke en niet-kritieke functies. Langdurige uitval van een kritieke functie kan leiden tot onacceptabele schade voor de financiële instelling zelf, tegenpartijen en/of klanten. Om dergelijke schade te voorkomen moeten er voor kritieke functies strenge beheersmaatregelen zijn die in verhouding staan met de hersteldoelstellingen, waaronder ook de beheersmaatregelen voor ICT-bedrijfscontinuïteit. Alle asset managers in het onderzoek beschikten over een overzicht van kritieke functies. Hierbij viel op dat in de door de AFM beoordeelde overzichten de indeling van deze functies niet in alle gevallen overeenkwamen met de indeling die de asset managers hadden gehanteerd bij de uitvraag van het DORA informatieregister in 2026.

**De AFM wijst erop dat consistentie op dit onderdeel belangrijk is.** Inconsistenties bij het definiëren van kritieke functies kunnen leiden tot functies die ten onrechte als niet-kritiek worden gezien. Specifiek voor de ICT-bedrijfscontinuïteit kan dat betekenen dat de getroffen beheersmaatregelen onvoldoende blijken te zijn bij een ernstige verstoring, waardoor er niet voldoende snel hersteld kan worden en of er te veel data verloren gaat.

#### Aandachtspunt 2: Definieer hersteldoelstellingen op functies

**Financiële instellingen moeten hersteldoelstellingen vaststellen.** Hersteldoelstellingen geven aan wanneer en onder welke voorwaarden een functie weer operationeel moet kunnen zijn. De AFM heeft in het onderzoek regelmatig gezien dat er wel hersteldoelstellingen op de individuele ICT-assets worden vastgesteld, maar niet separaat op de functies die door de ICT-assets worden ondersteund.

**Het is belangrijk om hersteldoelstellingen op de functies vast te stellen om meerdere redenen.** In de eerste plaats dienen asset managers zo inzichtelijk te hebben hoe snel functies kunnen worden hersteld na uitval van één of meerdere ICT-assets of ICT-diensten en of dat voldoet aan de hersteldoelstelling van de functie. Daarnaast is het van belang dat duidelijk is welke ICT-assets bijdragen aan kritieke functies. Blinde vlekken in welke ICT-assets kritiek zijn kunnen onvoldoende beheerste risico's met betrekking tot ICT-bedrijfscontinuïteit betekenen.

#### Aandachtspunt 3: Neem eigen herstelvereisten mee in contracten met ICT-dienstverleners

**Financiële instellingen besteden veel ICT-diensten uit.** Denk hierbij bijvoorbeeld aan gespecialiseerde software- en cloudaanbieders. Door deze uitbesteding is er vaak een grote afhankelijkheid van

ICT-dienstverleners. Door de complexiteit van de ICT-organisatie en de toegenomen kans op cyberaanvallen zijn goede afspraken met derden essentieel voor het risk management van de financiële instelling.

**Onderdeel hiervan zijn de vereisten van de instelling voor ICT-recovery.** Bij de selectie en de vastlegging van afspraken met ICT-dienstverleners is het daarom van belang dat financiële instellingen nagaan of de uitbesteding ook past binnen haar de hersteldoelstellingen op de functie of functies die door de uitbestede ICT worden ondersteund. Denk hierbij aan de tijd dat een functie niet beschikbaar kan zijn voor er onacceptabele schade optreedt. Financiële instellingen moeten nagaan of die doelstelling ook kan worden gehaald na de uitbesteding. In het onderzoek heeft de AFM gezien dat asset managers niet in alle gevallen deze hersteldoelstellingen expliciet in een overeenkomst (waaronder ook een service level agreement) vastlegden.

**Het maken en vastleggen van afspraken met ICT-dienstverleners over factoren die van belang zijn om de functies van financiële instellingen te kunnen herstellen binnen de hersteldoelstellingen is belangrijk voor het beheersen van de risico's van herstel.** Zeker in het geval van kritieke functies verwacht de AFM dat financiële instellingen in de overeenkomst met ICT-dienstverleners concrete afspraken vast te leggen die passen bij de hersteldoelstellingen die zij voor de relevante functie(s) heeft vastgesteld.

## Aandachtspunt 4: Test hersteldoelstellingen aan de hand van verschillende extreme scenario's

**Financiële instellingen moeten hersteldoelstellingen vaststellen die ook haalbaar zijn in extreme scenario's.** De hersteldoelstellingen moeten zijn opgenomen in de herstelplannen. Daarnaast moeten in de herstelplannen relevante scenario's worden genoemd die worden meegenomen bij het vaststellen van de maatregelen in de herstelplannen. Hierin moeten financiële instellingen in elk gevalrekening houden met in elk geval negen door DORA voorgeschreven scenario's.

**Het testen van deze herstelplannen moet worden uitgevoerd op basis van testscenario's die potentiële storingen simuleren, met inbegrip van een adequate reeks van zware, maar plausibele scenario's.** De testen bevatten ook scenario's voor de overschakeling van primaire ICT-infrastructuur naar de redundante capaciteit, back-ups en redundante faciliteiten.

**De AFM constateert dat alle asset managers in het onderzoek een testprogramma hebben waarin diverse scenario's worden getest.** Wel ziet de AFM verschillen in de reikwijdte en diepgang van de uitgevoerde testen. Zo werd in alle gevallen het overzetten van het primaire naar het secundaire datacentrum getest. Bij de overige testen lag bij sommige asset managers de nadruk op de uitval van een bepaald systeem, waarbij deze test periodiek werd herhaald. Bij andere asset managers werden meerdere scenario's getest waarin verschillende systemen niet beschikbaar waren.

**De AFM verwacht dat financiële instellingen herstelplannen, waaronder de hersteldoelstellingen, door de jaren heen testen aan de hand van voldoende verschillende scenario's.** Daarbij is het van belang dat financiële instellingen rekening houden met de scenario's die zijn betrokken bij de opzet van het herstelplan en met de uitkomsten van de risicoanalyse. Het testprogramma moet voldoende inzicht geven in de vraag of kritieke of belangrijke functies binnen de vastgestelde hersteldoelstellingen kunnen worden hersteld. Het is daarom van belang om niet alleen te testen of verschillende functies kunnen herstellen na een cyberaanval, maar ook of herstel mogelijk is bij andere relevante oorzaken van verstoringen.

## 4. Conclusie

**DORA richt zich op de digitale operationele weerbaarheid van financiële instellingen.** Door technologische en maatschappelijke ontwikkelingen nemen de digitale dreigingen verder toe. De AFM vindt het van groot belang om beter zicht te krijgen op hoe instellingen met zo min mogelijk schade hun ICT kunnen herstellen nadat deze uitvalt. Daarom heeft de AFM naast een onderzoek naar ICT-risk management nu ook een verkennend onderzoek naar ICT-recovery gedaan<sup>1</sup>.

**Belangrijke aandachtspunten zijn:**

- Zorg voor consistente identificatie en classificatie van de (kritieke) functies binnen de instelling
- Definieer hersteldoelstellingen op functies
- Neem ook eigen herstelvereisten mee in contracten met ICT-dienstverleners
- Hou bij het testen van hersteldoelstellingen rekening met verschillende extreme scenario's.

De AFM acht deze punten ook relevant voor andere asset managers en deelt deze daarom in dit rapport. De aandachtspunten kunnen ook relevant zijn voor andere financiële ondernemingen.

**De AFM vraagt asset managers de aandachtspunten in het rapport te bestuderen en daar waar nodig op te pakken.**

---

<sup>1</sup> Zie [Handelssystemen vragen om scherpere ICT-risicobeheersing onder DORA](#), gericht op handelssystemen maar met aanbevelingen die ook voor andere financiële instellingen van belang kunnen zijn.

# Bijlage 1 Belangrijkste bepalingen

| Onderwerp                                   | DORA                       | Gedelegeerde Verordening Risk Management                                       |
|---------------------------------------------|----------------------------|--------------------------------------------------------------------------------|
| Definities                                  | Artikel 3                  | -                                                                              |
| Consistente identificatie en classificatie  | Artikel 8, lid 1,3, 4 en 6 | Artikel 4, lid 2, sub b                                                        |
| Hersteldoelstellingen op functie            | Artikel 12, lid 6          | Artikel 24, lid 1, sub b, onderdeel ii, punt 2                                 |
| Vereisten herstel in contracten derden      | Artikel 30, lid 3 sub c    | -                                                                              |
| Testen met verschillende extreme scenario's | Artikel 11, lid 6          | Artikel 24, lid 2, sub b (iv)<br>Artikel 25, lid 2, sub a<br>Artikel 26, lid 2 |

## Bijlage 2 Definities

**Wat is een kritieke of belangrijke functie (kritieke functie)?** Een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële instelling of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële instelling van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten.

**Wat zijn hersteldoelstellingen?** Deze bestaan in DORA uit een RTO (Recovery Time Objective) en RPO (Recovery Point Objective).

**Wat is een RTO?** De maximale tijdsduur waarbinnen een systeem, proces of dienst hersteld moet zijn na een verstoring, voordat onacceptabele gevolgen voor de organisatie optreden.

**Wat is een RPO?** Het punt in de tijd tot waar gegevens na een verstoring moeten kunnen worden hersteld; oftewel de maximaal acceptabele hoeveelheid gegevensverlies, uitgedrukt in tijd.

**Wat is een ICT-dienstverlener?** Een onderneming die ICT-diensten verleent.

**Wat is een ICT-dienst?** Een digitale- en gegevensdienst die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers wordt verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten. Verschillende types ICT-diensten zijn opgenomen in bijlage III van Gedelegeerde Verordening (EU) 2024/2956 over het Informatieregister.