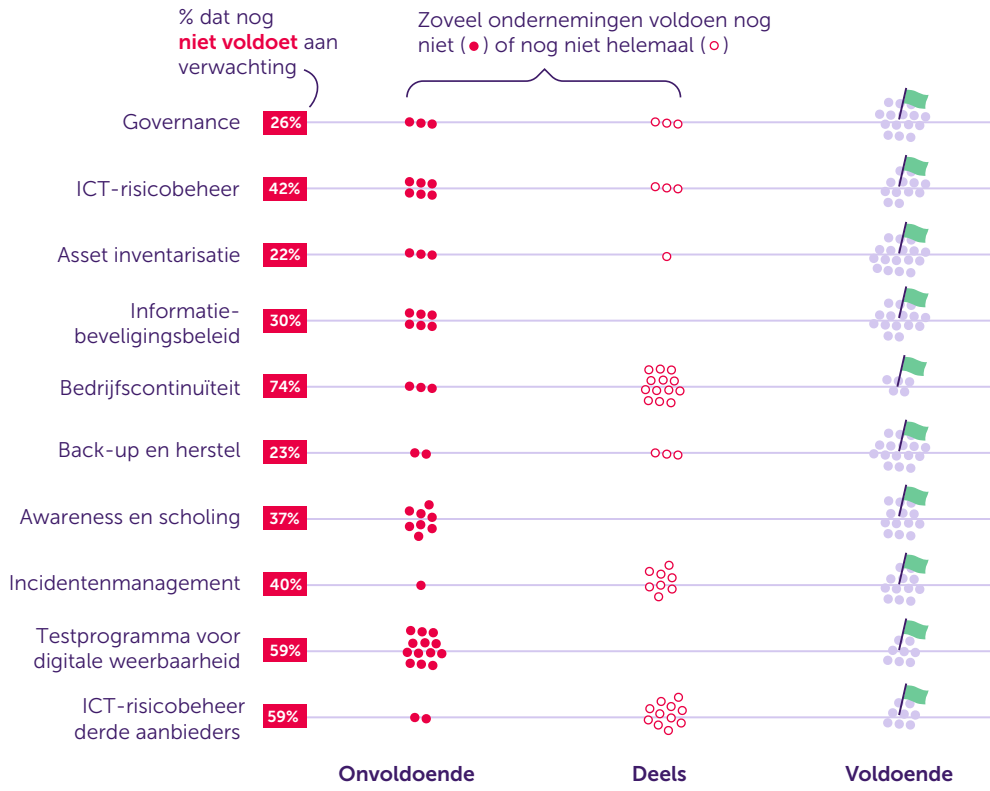
ANALYSE FACTSHEET

Informatiebeveiliging bij beleggingsondernemingen

In het kort Deze factsheet toont de scores van IT-beheersmaatregelen van 212 beleggingsondernemingen. Deze scores zijn tot stand gekomen op basis van de SREP uitvraag uit 2023. De relevante vragen uit dit self-assessment zijn gekoppeld aan tien belangrijke thema's uit DORA. De scores laten zien dat de beheersmaatregelen vaak nog niet op voldoende niveau waren en dat er nog aanzienlijk werk verzet moet worden voor inwerkingtreding van DORA. De AFM roept ondernemingen op haar informatiebeveiliging tegen deze bevindingen te toetsen en waar nodig aan te scherpen. Naast deze verbeterslag dient er ook aandacht te zijn voor de aanvullende vereisten uit DORA die geïmplementeerd moeten worden.



Legenda

Elk datapunt staat voor tien ondernemingen. In totaal hebben 212 ondernemingen de vragenlijst ingevuld.

- Ondernemingen die voldoende scoren
- Ondernemingen die deels voldoende scoren
- Ondernemingen die onvoldoende scoren

Elke stip staat voor tien ondernemingen

Minimale verwachting score

De vragenlijst

De weergegeven scores zijn gebaseerd op de SREP vragenlijst. Deze vragenlijst is in de vorm van een self-assessment afgenomen. De AFM heeft vervolgens de relevante vragen gekoppeld aan de DORA-wetgevings-artikelen. Deze koppeling is onze eigen interpretatie en omvat niet alle vereisten uit DORA.

AFM

Beleggingsondernemingen: klaar voor DORA?

De digitalisering van de financiële sector en het aanbieden van producten en diensten via online platformen zet gestaag door. Hierdoor nemen ook de ICT-risico's toe, zoals cyberaanvallen of andere verstoringen. Deze dreigingen kunnen het verlenen van financiële diensten vertragen of zelfs stilleggen. Het is belangrijk dat financiële dienstverleners voldoende maatregelen treffen om digitaal weerbaar te zijn. Cyberincidenten en mogelijke domino-effecten schaden zowel de continuïteit van, als het vertrouwen in, de financiële sector. De Europese verordening DORA (Digital Operational Resillience Act) stelt eisen ten aanzien van ICT-risicobeheer, ICT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico's bij uitbestedingen aan derden.

Volwassenheidsscores informatiebeveiliging beleggingsondernemingen

De Autoriteit Financiële Markten (AFM) monitort doorlopend de kwaliteit van informatiebeveiliging binnen de financiële sector. Deze factsheet toont de scores van IT-beheersmaatregelen van 212 beleggingsondernemingen[1] en zijn gekoppeld aan tien belangrijke thema's uit DORA. De scores zijn tot stand gekomen op basis van de SREP (Supervisory Review and Evaluation Process) uitvraag uit 2023. De AFM heeft voor de factsheet een koppeling gemaakt tussen de relevante SREP-vragen en de DORA-thema's. Deze koppeling is onze eigen interpretatie en omvat niet alle vereisten uit DORA.

Voor **ICT-risicobeheer** voldeden veel ondernemingen (42%) niet aan het verwachte niveau. DORA heeft als doel dat financiële ondernemingen ICT-risico's beter beheersen en daarmee weerbaarder worden tegen cyberdreigingen en ICT-verstoringen. Goed ICT-risicobeheer stelt een onderneming in staat om risico's tijdig en effectief te detecteren en te beheersen. DORA bevat vereisten voor zowel de procesmatige inrichting van risicobeheer, als de uitwerking in technische maatregelen. In concept RTS[2] ICT Risk Management Framework is dit verder in detail uitgewerkt. Ook is daarin is het vereenvoudigd kader voor ICT-risicobeheer beschreven dat o.a. geldt voor een bepaalde beleggingsondernemingen (zgn. klasse 3).

Voor het **ICT-risicobeheer van derde aanbieders** gaf meer dan de helft van de ondernemingen (59%) zichzelf geen voldoende. Steeds meer ondernemingen besteden belangrijke bedrijfsfuncties uit aan derde partijen waardoor ketenrisico's kunnen toenemen. Daarbij blijven ondernemingen zelf verantwoordelijk voor het beheersen van deze ketenrisico's. Daarbij dienen ondernemingen o.a. de ICT-risico's te analyseren, contractuele afspraken te maken over de dienstverlening en dit te monitoren. Onder DORA zijn de verschillende vereisten voor de beheersing van ICT risico's bij uitbestede diensten zijn verder uitgewerkt in concept RTS 28(1) en 30(5). In concept ITS[3] 28(9) zijn de eisen voor het opstellen van een uitbestedingenregister toegelicht.

De meeste ondernemingen (74%) kunnen hun **bedrijfscontinuïteit** nog verbeteren. Bedrijfscontinuïteit 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.

Ook voor het **testprogramma voor digitale weerbaarheid** scoorde het merendeel van de ondernemingen (59%) geen voldoende. Door regelmatig te testen krijgt een onderneming inzicht in de feitelijke veiligheid van hun IT-omgeving en kunnen gericht verbeteringen worden doorgevoerd. DORA schrijft daarom voor dat ondernemingen een risicogericht programma ontwikkelen voor het testen en verhogen van de digitale weerbaarheid. De inhoud van dit programma is afhankelijk van het vastgestelde risicoprofiel van een onderneming.

Om de stabiliteit van de dienstverlening van een onderneming te kunnen waarborgen, is het belangrijk dat een onderneming procedures heeft ingericht en geïmplementeerd voor hun bedrijfscontinuïteit.

1 Dit is inclusief beheerders met een MiFID top-up

2 Regulatory Technical Standards

3 Implementing Technical Standards

Een essentieel onderdeel hiervan is het inrichten van **back-up en herstelmogelijkheden** als verstoringen zich toch manifesteren. De meeste ondernemingen scoren hier voldoende (77%), maar let op dat er onder DORA aanvullende en gedetailleerde vereisten zijn.

De AFM verwacht dat organisaties hun informatiebeveiliging op basis van deze bevindingen evalueren en waar nodig aanscherpen. Naast deze verbeterslag dient er ook aandacht te zijn voor de andere eisen uit DORA die geïmplementeerd moeten worden.

Bereid je voor op DORA

Financiële ondernemingen moeten vanaf 17 januari 2025 voldoen aan DORA. Ter voorbereiding dienen ondernemingen tijdig helder te krijgen waar ze staan op het gebied van digitale weerbaarheid en welke stappen nog moeten worden genomen om aan de eisen uit de verordening te voldoen. Voor een dergelijke gap-analyse kunnen ondernemingen onder andere de DORA-checklist gebruiken als startpunt. Vervolgens dient de geïdentificeerde gap omgezet te worden naar een activiteitenplan waarmee een onderneming de inrichting van informatiebeveiliging verbetert en zich voorbereidt op de vereisten uit DORA. Dit betekent o.a. het aanpassen van intern beleid en procedures, het aanscherpen van beheersmaatregelen en de evaluatie van de contracten met derde aanbieders.

De DORA-checklist is een handige tool voor ondernemingen om op een aantal punten helder te krijgen wat er qua beleid en procedures nodig is om te voldoen aan de vereisten uit DORA. De checklist moet hierbij worden gezien als een beginpunt- voor ondernemingen om een beeld te krijgen wat belangrijke aanknopingspunten zijn om een volledige gap-analyse mee uit te voeren. Vanwege de omvang van DORA is de checklist niet volledig. Voor de volledige vereisten verwijst de AFM naar de verordening en bijbehorende RTS en ITS.
Meer informatie hierover staat op onze website