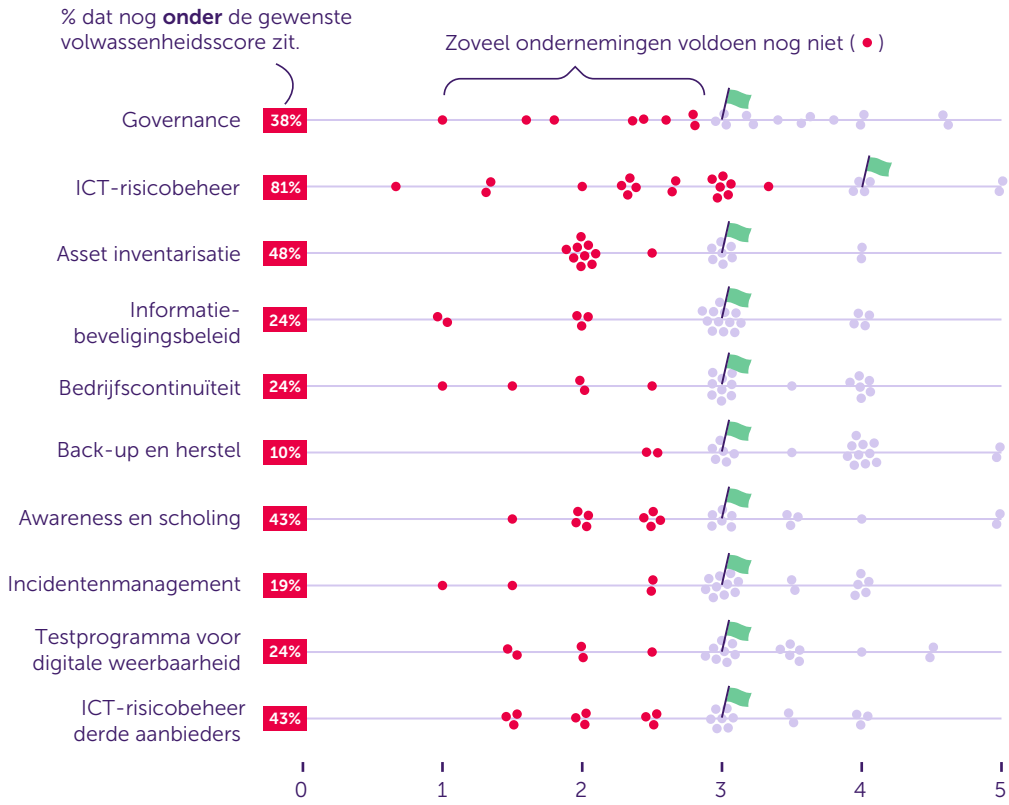
ANALYSE FACTSHEET

Informatiebeveiliging bij financieel dienstverleners

In het kort Deze factsheet toont de volwassenheidsscores van beheersmaatregelen van 21 financiële dienstverleners. Deze scores zijn tot stand gekomen op basis van een self-assessment uit 2023 en zijn gekoppeld aan tien belangrijke thema's uit DORA. Dit laat zien dat in veel gevallen de beheersmaatregelen nog niet op het verwachte volwassenheidsniveau 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 eisen uit DORA die geïmplementeerd moeten worden.



Legenda

Elk datapunt staat voor één onderneming. In totaal hebben 21 ondernemingen de vragenlijst ingevuld.

- Ondernemingen die voldoen aan de volwassenheidsscore
- Ondernemingen die **niet** voldoen aan de volwassenheidsscore

Minimale verwachting volwassenheidsscore

De vragenlijst

De vragenlijst is in de vorm van een self-assessment afgenomen. De ondernemingen hebben zichzelf een volwassenheidscore per control van de DNB IB good practice toegekend. De AFM heeft vervolgens de relevante controls uit de vragenlijst gekoppeld aan de DORA-wetgevingsartikelen. Deze koppeling is onze eigen interpretatie en omvat niet alle vereisten uit DORA.

De gehanteerde antwoordschaal loopt van 0-5:

De beheersmaatregel ...

0 ... is **niet aanwezig.**
1 ... is (gedeeltelijk) aanwezig, maar wordt **niet consistent** uitgevoerd.
2 ... is aanwezig, maar wordt **niet aantoonbaar effectief** uitgevoerd.
3 ... is **aantoonbaar effectief** en wordt getoetst.
4 ... is **aantoonbaar effectief** en wordt **periodiek geëvalueerd** in samenhang met het gehele stelsel van beheersmaatregelen.
5 ... is **aantoonbaar effectief** en wordt **continu verbeterd.**

AFM

ANALYSE FACTSHEET

Financieel dienstverleners 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 financiele 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. DORA geldt voor financieel dienstverleners met meer dan 250 FTE in dienst of meer dan 50 miljoen euro omzet.

Volwassenheidsscores informatiebeveiliging Financieel Dienstverleners

De Autoriteit Financiële Markten (AFM) monitort doorlopend de kwaliteit van informatiebeveiliging binnen de financiële sector. Deze factsheet toont de volwassenheidsscores van beheersmaatregelen van 21 financiële dienstverleners die gekoppeld zijn aan tien belangrijke thema's uit DORA. De scores zijn tot stand gekomen op basis van een self-assessment onderzoek uit 2023 naar informatiebeveiliging op basis van de DNB IB Good Practices. De AFM heeft voor de factsheet een koppeling gemaakt tussen de uitgevraagde beheersmaatregelen en de DORA-thema's. Deze koppeling is onze eigen interpretatie en omvat niet alle vereisten uit DORA.

Voor **ICT-risicobeheer** voldeden veel ondernemingen (81%) 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[1] 15 is dit verder in detail uitgewerkt en in concept RTS 16(3) is het vereenvoudigd kader voor ICT-risicobeheer beschreven dat geldt voor een aantal uitgezonderde ondernemingen.

Ook voor de **governance** rondom ICT-risicobeheer kunnen verschillende ondernemingen (38%) zich nog verbeteren. DORA bevat o.a. eisen voor een risico gestuurde en periodieke evaluatie van het ICT-risicobeheer door het leidinggevend orgaan. Naast deze controlecyclus, dienen ook duidelijke taken en verantwoordelijkheden voor ICT-risicobeheer toegewezen te worden, zoals een onafhankelijke functie voor de beheersing van ICT-risico's en een interne auditfunctie.

Verder bleek dat bijna de helft van de ondernemingen (48%) geen of geen volledige **ICT-asset inventaris** hebben. Deze inventaris is noodzakelijk voor het identificeren en onderhouden van de ICT-assets die kritische of belangrijke bedrijfsfuncties ondersteunen. Mogelijke wijzigingen en kwetsbaarheden van ICT-assets kunnen anders niet adequaat gemonitord worden.

Voor het **ICT-risicobeheer** van derde aanbieders gaf bijna de helft (43%) zichzelf een onvoldoende. Belangrijke bedrijfsfuncties worden steeds meer uitbesteed aan derde partijen waardoor ketenrisico's kunnen toenemen. Daarbij blijven ondernemingen zelf verantwoordelijk voor het beheersen van deze ketenrisico's. Ondernemingen dienen de risico's te analyseren, geaccordeerde afspraken te maken over de dienstverlening en dit te monitoren. De verschillende eisen voor de beheersing van ICT-risico's bij uitbestede diensten zijn uitgewerkt in concept RTS 28(1) en 30(5). In concept ITS 28(9) zijn de vereisten voor het opstellen van een uitbestedingenregister toegelicht.

Om de stabiliteit van de dienstverlening van een onderneming te kunnen waarborgen, is het belangrijk dat er procedures zijn ingericht en geïmplementeerd voor bedrijfscontinuïteit. Een essentieel onderdeel hiervan is het inrichten van **back-up en herstelmogelijkheden** als verstoringen zich toch manifesteren. De meeste ondernemingen scoorden hier voldoende (90%), maar let op dat er onder DORA aanvullende en gedetailleerde vereisten zijn.

1 Regulatory Technical Standards

De AFM verwacht dat ondernemingen hun informatiebeveiliging op basis van deze bevindingen evalueren en waar nodig aanscherpen. Naast deze verbeterslag dient er ook aandacht te zijn voor de aanvullende 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 concrete activiteiten 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