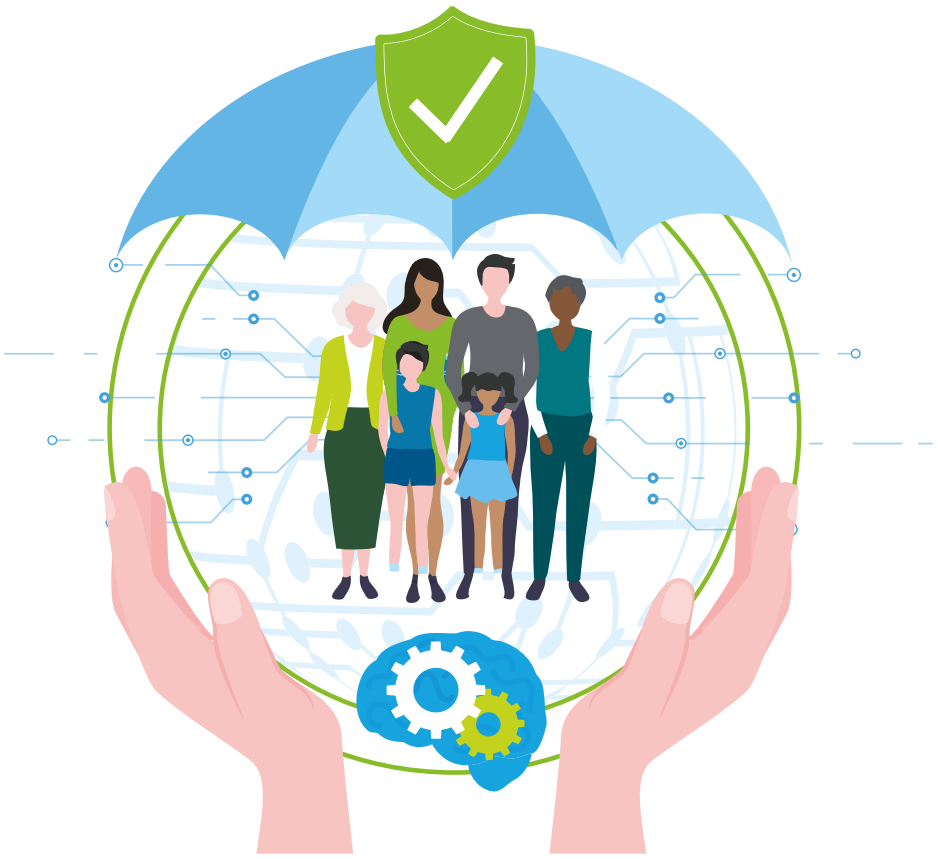
Deloitte.



Actieplan DORA 2024

Beter voorbereid op cyberincidenten

De afgelopen jaren nam het aantal cyberincidenten en -aanvallen fors toe. De Europese Unie (EU) heeft de Digital Operational Resilience Act (DORA) verordening voor het beheersen van IT-risico's vastgesteld. DORA heeft als doel om de digitale operationele veerkracht van financiële instellingen, waaronder verzekeraars, en hun IT-toeleveringsketens te verhogen. DORA is een regelgevend antwoord op de toenemende bedreigingen voor de cyberveiligheid. De vereisten omvatten technische maatregelen, procedures, processen en praktijktesten om verzekeraars te ondersteunen bij het opsporen van afwijkingen, bij het in bedwang houden van en herstel van cyberveiligheidsincidenten.

In het kort

- Uit GAP-assessments blijkt dat aanpassingen van beleid, interne beheersingsmaatregelen en afspraken met derde partijen noodzakelijk zijn.
- Inzicht verkrijgen in kritieke functies is ingewikkeld, maar essentieel om maatregelen te implementeren.
- Niet alle elementen van de regelgeving zijn definitief bekend.
- De rol van tweede en derde lijn richt zich op projectmonitoring en ondersteuning.

Ontwikkeling regelgeving

Het jaar 2023 begon met de bekendmaking van de DORA-wetgeving. Gedurende 2023 heeft de European Securities and Markets Authority (ESMA) twee keer een set met onderliggende regelgeving - de "Regulatory Technical Standards" (RTS) - gepubliceerd ter consultatie. ESMA verwacht de laatste definitieve standaarden in juli 2024 te publiceren. Dat betekent dat verzekeraars nu al moeten anticiperen op DORA.

In 2023 heeft DNB de Good Practice informatiebeveiliging[1] uit 2019/2020 geactualiseerd. Deze nieuwe versie is een stap in de richting van de implementatie van DORA. DNB gebruikt de nieuwe versie voor onderzoeken en uitvragen van 1 juli 2023. DNB benadrukt dat het aan de verzekeraars zelf is om te voldoen aan DORA. In 2024 bepaalt DNB hoe de Good Practice Informatiebeveiliging 2023 zich verhoudt tot de dan uitgewerkte DORA-regelgeving.

Regelgeving op hoofdlijnen

DORA kan worden samengevat in vier pilaren. Deze worden weergegeven in figuur *DORA regelgeving op hoofdlijnen*.

Waar staan verzekeraars?

Verzekeraars zijn in 2023 begonnen met het kennisnemen van de nieuwe wet- en regelgeving, het benoemen van een eindverantwoordelijke, het uitvoeren van GAP-assessments en de vertaling daarvan naar het jaarplan 2024 - inclusief de budgettaire vertaling. Uit onderzoek[2] van Deloitte blijkt dat de eindverantwoordelijkheid voor het uitvoeren van de plannen met name ligt bij de CISO (40%) en in mindere mate bij de CRO (16%) en de CIO (16%).

Uit de door Deloitte uitgevoerde GAP-assessments en onderzoek[2] blijkt dat:

- **Beleidskaders, het interne controle framework en procesbeschrijvingen niet op detailniveau aansluiten op de vereisten.** De impact hiervan is afhankelijk van het huidige volwassenheidsniveau. Deze aanpassingen hebben betrekking op alle pilaren. Bijvoorbeeld op het beleid omtrent sub-serviceorganisaties, cryptografie, beleid derde partijen waaronder due diligence, exitplannen en de beveiligingseisen waaraan zij moeten voldoen.

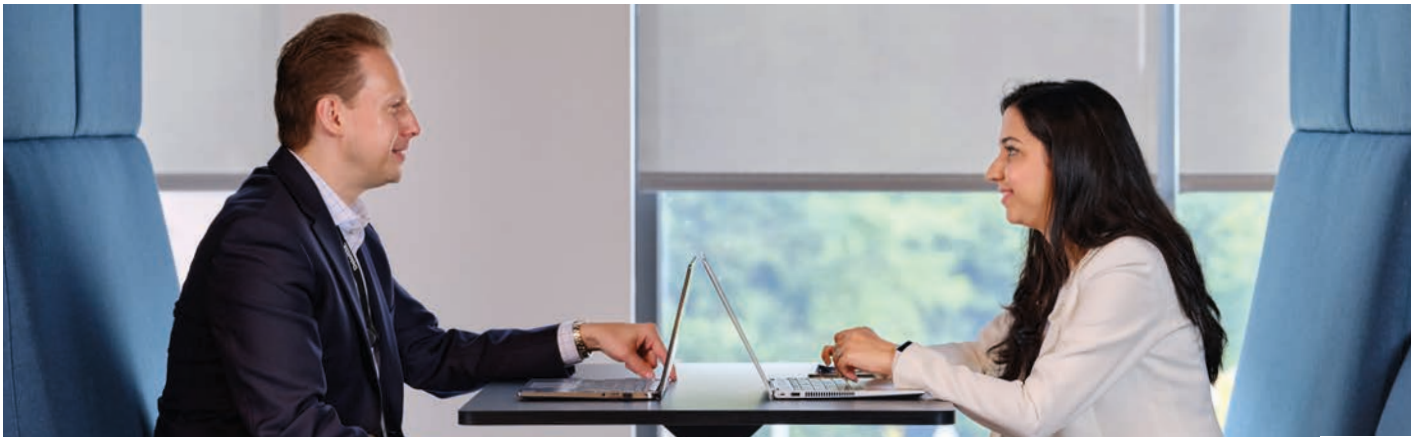
- **Een Digital Operational Resilience Strategie ontbreekt.** Relevante elementen voor de strategie die DORA benoemt, zijn onder andere vulnerability assessment en scans, open source analyses, network security assessments, scenario-gebaseerde tests en end-to-end tests.

- **Kritieke of belangrijke functies nog niet zijn benoemd.** Kritieke functies zijn activiteiten, diensten of bedrijfsactiviteiten waarvan de onderbreking waarschijnlijk leidt tot een verstoring van essentiële diensten aan de reële economie.

- **Nog niet inzichtelijk is welke IT-elementen en derde partijen nodig zijn om de kritieke of belangrijke functies uit te voeren.** Een voorbeeld is de mijn-omgeving. Is inzichtelijk welke IT-componenten waarborgen dat de mijn-omgeving veilig en in continuïteit kan worden uitgevoerd? De kritieke functies hebben invloed op onder andere het melden van incidenten, de weerstandstrategie en de afhankelijkheid en beheersing van derde partijen.

- **De keten van IT-service-organisaties onvoldoende inzichtelijk is en dat afhankelijkheden onvoldoende zijn getest.** EIOPA verwacht dat financiële instellingen de keten van IT-service-organisaties beheersen. Dit betekent dat financiële instellingen afspraken moeten maken met IT-service-organisaties over de keuze en beheersing van hun leveranciers. Een voorbeeld is als de IT-service-organisatie, die online een applicatie ontwikkelt en host, wilt wisselen van leverancier van de IT-infrastructuur.

- **De afspraken met derde partijen** over tijdige incidentrapportage niet toereikend zijn om aan de meldplicht te voldoen.



1. DNB Governance,, Q&A Informatiebeveiliging
2. Deloitte, Survey on Digital Operational Resilience Act, februari 2023

DORA regelgeving op hoofdlijnen

ICT-risicomanagement

- Implementeren van ICT governance, inclusief een centrale en actieve rol voor het bestuursorgaan.
- Invoering van een kader voor ICT risicobeheer (georganiseerd rond identificatie, bescher-ming en preventie, opsporing, respons en herstel, opleiding en ontwikkeling en communicatie).

Beheer van ICT-incidenten

- Stroomlijn de rapportage van ICT incidenten door het loggen en classificeren van ICT incidenten
- Meld ernstige incidenten aan de bevoegde autoriteiten met behulp van gemeenschappelijke modellen en procedures
- Rapportage is gebaseerd op kritieke functies, de zogenaamde Critical or Important Functions (CIF's).

Testen van digitale operationele veerkracht

- Voer ten minste jaarlijks digitale operationele basistests uit voor alle verzekeraars.
- Voer ten minste om de drie jaar een geavanceerde thread led penetratietest uit voor 'significante' verzekeraars.

Beheer van ICT-risico's van derden

- Toezicht houden op contractuele regelingen van derden in alle stadia (contractering, beeindiging en postcontractuele fase)
- Europese toezichthoudende autoriteiten (ETA's) in staat stellen toezicht te houden op derde aanbieders van ICT diensten die als "kritiek" worden beschouwd, met duidelijke vereisten en sancties.

Bron: Deloitte

Actieplan 2024

Verzekeraars moeten in 2024 stappen zetten om de DORA-vereisten te implementeren. Een deel van de implementatie kan worden uitgevoerd als onderdeel van bestaande processen. Maar het vormen van projecten, inclusief het aanstellen van projectmanagement, is noodzakelijk omdat de implementatie door meerdere afdelingen moet worden uitgevoerd. De compliance officer, de risk officer en internal audit zijn bij de implementatie betrokken om vast te stellen dat de projecten adequaat zijn opgezet, voldoende invulling geven aan de vereisten en tijdig zijn geïmplementeerd. De Good Practice Informatiebeveiliging 2023 kan als leidraad worden gebruikt.

Een succesvolle implementatie in 2024 vraagt om drie acties.

1. Ten eerste hebben verzekeraars een digitale operationele strategie nodig om de resilience te verhogen. Dit kan een nieuwe strategie zijn of een aanvulling op bestaande strategieën en plannen. De strategie moet in 2024 afgerond zijn, zodat de uitvoering in 2025 kan beginnen. Het is verstandig om een koppeling te leggen met de kritieke functies en de strategie te bepalen vanuit risicoanalyse.
2. Ten tweede zijn verzekeraars in 2023 begonnen met het **bepalen van de kritieke functies en het inzichtelijk maken van het IT-landschap,** inclusief de afhankelijkheid van derde partijen. Deze actie moet in 2024 worden afgerond en een proces moet worden ingericht om het te kunnen bijstellen. Bijvoorbeeld als onderdeel van het wijzigingsbeheer.
3. Ten derde: om na te gaan of alle relevante ketenpartijen voldoende inzichtelijk zijn en worden meegenomen in de tests, is **actie nodig op het gebied van business continuity**. Dit hangt samen met de actie om de beheersing van de derde partijen verder te verbeteren. Verzekeraars moeten beleidskeuzes maken voor de beheersing van derde partijen. Wanneer moet een due diligence worden uitgevoerd? Hoe moeten exitplannen eruitzien? Hoe kunnen deze worden vertaald in contractuele bepalingen? En hoe wordt gewaarborgd dat incidenten tijdig worden gemeld en geëvalueerd?

Op naar een veiliger wereld!

Omarming door de sector van DORA is essentieel. Het zorgt ervoor dat verzekeraars beter zijn voorbereid en draagt bij aan het inperken van de hoeveelheid en de impact van cyberincidenten. Op naar een veiligere wereld!

Deloitte.

Designed and produced by CoRe Creative Services RITM1619240