DORA en DNB Good Practice Informatie Beveiliging 2019 en 2023

DORA en actualisatie Good Practice Informatiebeveiliging

Een van de grootste veranderingen op het gebied van wetgeving rondom IT is de Digital Operational Resilience Act (DORA). Deze nieuwe regelgeving is vastgesteld door de Europese Commissie voor de gehele Europese financiële sector en richt zich op het uniformeren van regels voor het beheer van ICT-risico's waaronder de beveiliging van informatietechnologie. DORA stelt eisen aan financiële ondernemingen ten aanzien van IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico's bij uitbesteding aan IT-dienstverleners. Daarnaast zijn er regelingen uitgewerkt voor het uitwisselen van informatie over cyberdreigingen. Met het oog op DORA, en andere ontwikkelingen op het gebied van IT beheersmaatregelen heeft DNB een actualisatie gemaakt van Good Practice Informatiebeveiliging (GPIB). Deze is eind 2023 gepubliceerd.

Good Practice Informatie Beveiliging (GPIB)

In 2019 publiceerde DNB de eerste Good Practice Informatie Beveiliging (GPIB). Met behulp van de GPIB draagt DNB haar opvattingen uit over de geconstateerde of verwachte gedragingen die een goede toepassing inhouden voor informatiebeveiliging en cybersecurity. Dit gebeurt op basis van een risicoanalyse als onderdeel van de Risk Management Cycle. De beheersmaatregelen gaan over technologische oplossingen, maar betreffen ook menselijk handelen, het inrichten van processen, en faciliteiten. De GPIB is aan de hand van deze thema's opgebouwd met onder andere de hoofdstukken 'Technology', 'People', 'Processes', en 'Facilities'.

De GPIB is inmiddels een bekend fenomeen in de Nederlandse financiële sector en pensioenfondsen, verzekeraars en banken hebben hun informatiebeveiliging de afgelopen jaren materieel verbeterd op basis van GPIB van DNB.

Belangrijkste wijzigingen in GPIB 2023

De GPIB 2023 kent dezelfde indeling als de GPIB 2019/2020. Volgens DNB is het een verdere verdieping en aanscherping die past bij toenemende en veranderende cyberbedreigingen.

De belangrijkste wijzigingen zijn:

1. Aandacht voor de digitale operationele weerbaarheidsstrategie op korte, midden en lange termijn als onderdeel van het Risk Management Framework. Belangrijk is dat de regie op derde partijen hier ook onder valt.
2. Aandacht voor een risico-gebaseerde invulling per control. Instellingen kunnen hierdoor verdergaand maatwerk toepassen op de inrichting en implementatie van hun controls.
3. Aandacht aan het uitvoeren van een business impact analyse vormt de basis voor continuïteitsborging om gevoeligheden voor ernstige bedrijfsonderbrekingen te beoordelen.
4. Ook wordt de gewenste rol van het bestuur bij het onderwerp informatiebeveiliging beter uitgediept. Bij sommige controls is deze rol expliciet benoemd. Zo wordt gesteld dat het bestuur

actief op de hoogte moet zijn van de belangrijkste technologische ontwikkelingen en dreigingen. En wordt nu ook verwacht dat het bestuur het belang van informatiebeveiliging zichtbaar en actief uitdraagt. Het ontwikkelen en bijhouden van kennis van het dagelijks bestuur, RvC, RvT, en sleutelfunctiehouders krijgt nu ook aandacht in de nieuwe versie van GPIB. Dit wordt gedaan door het aantoonbaar volgen van toegespitste trainingen op het gebied van IT- en cyberrisico.

5. Het invullen van een onafhankelijke en objectieve informatiebeveiligingsfunctie met een vastomlijnd takenpakket die rechtstreeks rapporteert aan het bestuur.
6. Ten slotte komt er ook aandacht voor kansen en risico's die samenhangen met technologische ontwikkelingen. Voorbeelden hiervan zijn quantum computing en AI.

De actualisatie dient er voornamelijk voor dat instellingen stappen gaan maken naar een implementatie van DORA per 17 januari 2025. De reeds gepubliceerde en nog te publiceren Regulatory Technical Standards (RTS) zijn niet verwerkt in de nieuwe GPIB. De GPIB moet daarom worden gezien als aanvulling op de ontwikkeling rond DORA. DNB onderzoeken, uitvragen en andere toezichtactiviteiten gaan nu nog uit van de GPIB 2019/2020. Na het tweede kwartaal van 2024 zal de GPIB 2023 het uitgangspunt zijn voor alle DNB activiteiten. Ter voorbereiding op DORA is het aan te raden om te beginnen met de implementatie van de veranderingen van GPIB en de ontwikkelingen van de RTS in de gaten te houden. Wij informeren u over updates rondom de GPIB en de DORA RTS.

Voor hulp om compliant te worden met de aangepaste Good Practice van DNB en DORA kunt u contact opnemen met Edward Roozenburg.