De evolutie van cyberweerbaarheid:

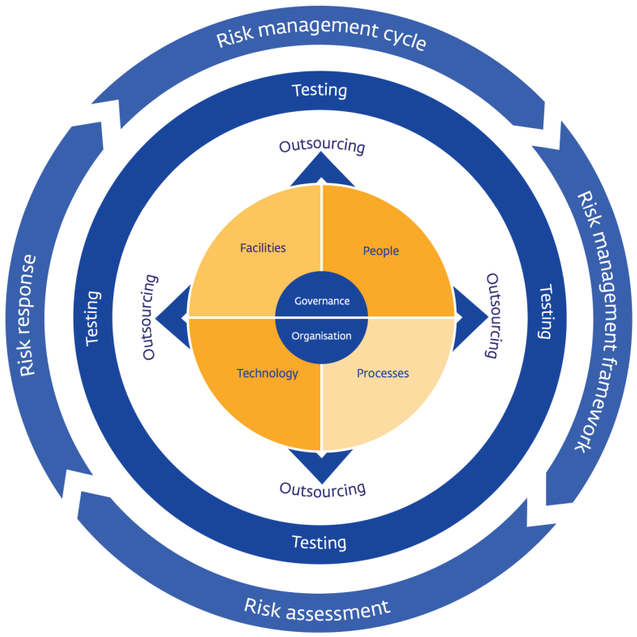
DNB's Good Practice Informatiebeveiliging 2023

De cybercrime industrie wordt steeds professioneler en dat leidt tot toenemende dreigingen. Financiële instellingen zullen hun weerbaarheid voortdurend moeten verbeteren. De Nederlandsche Bank (DNB) speelt een belangrijke rol bij deze bescherming, door het opstellen van Good Practices voor informatiebeveiliging. De Good Practice uit 2019/2020 is in 2023 bijgewerkt en reflecteert de toenemede eisen aan het ICT-risico raamwerk. Dit artikel duikt in de belangrijkste veranderingen en hun impact op de financiële sector.

Van compliance naar weerbaarheid
De nieuwste update laat zien hoe financiële instellingen zich bewust moeten worden hoe groot de risico's en dreigingen zijn. De invoering van de Digital Operational Resilience Act (DORA), die de cyberweerbaarheid van de financiële sector beoogt te verhogen, is door DNB aangegrepen om heldere handvaten en beheersmaatregelen te geven aan financiële instellingen.

Het belang van continue aandacht
DNB benadrukt dat informatiebeveiliging en cybersecurity permanente aandacht vereisen, vooral ook op strategisch en bestuurlijk niveau. De Good Practice 2023 is een reflectie van deze behoefte en biedt de financiële sector de handvatten om niet alleen te voldoen aan de wettelijke bepalingen, maar ook om proactief te reageren op het constant veranderende dreigingslandschap.

Ontwerpen van Information Security Management Systeem
Voor het inrichten van een Information Security Management Systeem (ISMS) is de Good Practice Informatiebeveiliging 2023 (GP IB 2023) van DNB een effectieve manier om het proces rond informatiebeveiliging te structureren, monitoren en versterken. Op basis van de 58 controls kan je als organisatie een risicoanalyse, beleid en beheersmaatregelen implementeren. De Good Practice geeft de juiste basis voor een algeheel ISMS, in onze opinie beter dan de DORA (dat veel focus op een beperkt aantal onderwerpen legt).



De visuele weergave van de focusgebieden van informatiebeveiliging, de onderlinge relaties en de inbedding in het risicobeheer is (afgezien van de kleurstelling) ongewijzigd ten opzichte van de 2019 versie.

Nieuwe en relevantste wijzigingen

De Good Practice Informatiebeveiliging 2023 introduceert belangrijke wijzigingen die een robuust fundament leggen voor financiële instellingen om de voortdurende dreigingen in kaart te brengen:

- **Strategie ICT-risicobeheer:** Nadruk op een digitale operationele weerbaarheid strategie op korte, middellange, en lange termijn, die richting geeft aan het (ICT) Risk Management Framework inclusief het beheer over derde partijen.
- **Risico-gebaseerd:** Aandacht voor een risico-gebaseerde invulling per control. Hierdoor kunnen instellingen steeds verdergaand maatwerk toepassen ten aanzien van de inrichting en implementatie van hun specifieke informatiebeveiligingsmaatregelen.
- **Business Impact Analyse:** Het belang van het uitvoeren van een business impact analyse wordt benadrukt, om de blootstelling aan ernstige bedrijfsstoringen en de potentiële gevolgen daarvan beter te kunnen inschatten.
- **Bestuurlijke betrokkenheid:** De gewenste rol van het bestuur is explicieter gemaakt, inclusief het ontwikkelen en bijhouden van relevante kennis en opleidingen door bestuursleden en sleutelfunctiehouders.
- **Uitbestedingsketen:** Extra aandacht voor (kritieke) uitbestedingen wordt aangekaart. Meer voorbeelden en normen om te zorgen dat financiële instellingen een gestructureerd en overzichtelijk uitbestedingsproces inrichten.

DORA vs Good Practice
Hoewel de implementatie van de GP IB 2023 van DNB een sterke basis legt voor het verbeteren van de cyberweerbaarheid, is het voldoen aan de Good Practice niet voldoende om ook gereed te zijn voor DORA. DORA is namelijk meer rule-based en gedetailleerder. DORA heeft een bredere reikwijdte en bevat specifieke vereisten die niet volledig worden gedekt door de controls van DNB. Daarom moeten financiële instellingen aanvullende maatregelen nemen om volledig aan DORA te voldoen, boven op de richtlijnen van de Good Practice.

Conclusie
Met de GP IB 2023 zet DNB een belangrijke stap vooruit in de bescherming van de financiele sector tegen cyberdreigingen. De update is een erkenning van de noodzaak voor financiële instellingen om hun cyberweerbaarheid continu te evalueren en te versterken in reactie op een steeds veranderend dreigingslandschap. Het is een oproep aan alle financiële instellingen om hun beleid en procedures rond informatiebeveiliging te herzien en te versterken. Dit is essentieel om niet alleen te voldoen aan de wettelijke vereisten maar ook om een stap voor te blijven in de voortdurende strijd tegen cyberdreigingen.

Hoewel de Good Practice Informatiebeveiliging 2023 van DNB financiële instellingen een sterke basis biedt voor informatiebeveiliging en de bevordering van cyberweerbaarheid, moeten instellingen zich ook direct richten op de vereisten van DORA om te zorgen voor volledige compliance met deze Europese wetgeving.
Het is belangrijk dat financiële instellingen zich bewust zijn van en actief werken aan het voldoen aan beide sets van richtlijnen om hun cyberweerbaarheid te maximaliseren.