DORA-implementatieproces: Een praktische benadering

De Digital Operational Resilience Act (DORA) treedt in 2025 in werking. InAudit ondersteunt klanten gedurende het volledige implementatieproces om te voldoen aan de strikte vereisten van deze wetgeving. Om bedrijven te helpen DORA-compliant te worden en hun digitale veerkracht te versterken, delen we praktijkvoorbeelden en inzichten uit eerdere trajecten bij verschillende klanten.

Uitdagingen tijdens de gap-analyse

De DORA-verordening laat weinig ruimte voor interpretatie. Tijdens de uitvoering van de gap-analyse wordt duidelijk dat de wetgeving zeer gedetailleerd is. De artikelen in DORA specificeren nauwkeurig wat er verwacht wordt, zonder grijs gebied. Een concreet voorbeeld is de classificatie van ernstige incidenten, waarbij de wet precies aangeeft aan welke voorwaarden een incident moet voldoen om als ernstig te worden beschouwd.

In tegenstelling tot de Good Practice Informatiebeveiliging (GP-IB) van De Nederlandsche Bank (DNB), die een meer globale en soepele benadering heeft, biedt DORA keiharde regels. Elk onderdeel is tot in detail uitgewerkt en voorgeschreven, waardoor er weinig flexibiliteit is.

Voorbereiding: Interne gap-analyse
Een goed startpunt voor de implementatie is een intern uitgevoerde gap-analyse, die een groot deel van de te toetsen artikelen omvat. Vanwege de omvang van de analyse, het aantal betrokken partijen en de tijdsdruk, is dit een uitdagende taak.

Gebruik van DORA-templates
Een andere uitdaging is de enorme hoeveelheid informatie waarmee men te maken krijgt. De DORA-templates, ontwikkeld door InAudit, bieden een handig hulpmiddel om de informatie behapbaar te maken en toegevoegde waarde te leveren. Hoewel er nog vele uren nodig zijn om de analyse volledig af te ronden, blijken de templates een waardevol instrument.

Inzicht door Dashboards
De resultaten van de gap-analyse worden overzichtelijk gepresenteerd in dashboards. Dit geeft het management een duidelijk beeld van de huidige situatie, de belangrijkste knelpunten en de nodige stappen om compliant te worden met DORA. Door de informatie visueel weer te geven, kunnen klanten door de complexe wet- en regelgeving heen kijken en een effectief plan van aanpak opstellen, wat hen uiteindelijk veel tijd bespaart.

Uitvoering en ervaring van de klant

Het uitvoeren van de gap-analyse blijkt voor zowel InAudit als de klant een intensief proces. De klant moet bijvoorbeeld tijd en capaciteit organiseren voor het aanleveren van documentatie en het beantwoorden van vragen. Samen met bijvoorbeeld de IT-manager, de (C)ISO en de Compliance Officer beoordelen we elk artikel van DORA, wat een intensieve maar lonende klus is. Het levert uiteindelijk een helder beeld op van de stand van zaken en biedt zuivere informatie voor het verdere implementatietraject.

Resultaten van de gap-analyse

De gap-analyse resulteert in een dynamisch dashboard, dat dient als een levend document. Eventuele doorgevoerde verbeteringen kunnen hierin worden bijgewerkt. Wij valideren of deze verbeteringen effect hebben op het volwassenheidsniveau, gemeten volgens de normen van DNB. Op basis hiervan ondersteunen we klanten om volledig compliant te worden en te blijven met DORA.

Implementatie en volgende stappen

Het integreren van DORA in de dagelijkse bedrijfsvoering is voor alle betrokken instellingen een uitdaging. Op de korte termijn zullen vooral de aanbevelingen uit de gap-analyse worden doorgevoerd. Dit vergt tijd en capaciteit en dit vrijmaken kan voor klanten een behoorlijke uitdaging zijn. Het opzetten van een werkgroep om de ‘gaps’ systematisch te implementeren zou voor onze klanten een volgende stap kunnen zijn.

Een andere uitdaging is het zorgvuldig doorlopen van elk DORA-artikel. Sommige artikelen vereisen meerdere lezingen om goed te begrijpen wat geïmplementeerd moet worden. Dit kost tijd, maar voorkomt dat belangrijke elementen worden overgeslagen.

Uitdagingen in de transitie van GP-IB naar DORA
De overgang van GP-IB naar DORA brengt aanzienlijke uitdagingen met zich mee. Waar GP-IB een soepelere aanpak kende, is DORA veel strikter en gedetailleerder. Vooral de beheersing van risico’s rondom de samenwerking met ICT-dienstverleners (pijler 4) en het opstellen van een register van informatie zijn complexe en tijdsintensieve taken. Financiële instellingen moeten niet alleen in kaart brengen bij welke dienstverleners IT-functies zijn ondergebracht, maar ook of deze dienstverleners gebruik maken van onderleveranciers. Dit moet zorgvuldig worden geregistreerd en de financiële instellingen moeten dit naar verwachting begin 2025 delen met DNB.

Vanwege het rule-based karakter van DORA hebben veel financiële instellingen aanzienlijke stappen te zetten om compliant te worden. Het zal voor onze klanten een grote uitdaging zijn om alles vóór 17 januari 2025 geïmplementeerd te krijgen. Daarom is een gedegen en gedragen plan van aanpak essentieel, gebaseerd op een grondige analyse. Het vinden van voldoende kwalitatieve capaciteit om het werk uit te voeren blijft een uitdaging in de markt, wat vraagt om een slimme, pragmatische aanpak. InAudit heeft voldoende expertise opgebouwd de afgelopen tijd en ondersteunt haar klanten daar waar nodig.

InAudit is trots om een bijdrage te leveren aan dit belangrijke ontwikkelproces en blijft klanten graag ondersteunen op hun weg naar volledige compliance met DORA.

Ricardo Henriques
Audit Manager
06-21 37 33 66