Digitale weerbaarheid:

ZO VULLEN DORA EN ISO 27001 ELKAAR AAN

Cyberdreigingen worden steeds geraffineerder en complexer. Voor organisaties is het essentieel om niet alleen goed beveiligd te zijn, maar ook snel te kunnen reageren als iets misgaat. Twee kaders die daarbij een sleutelrol spelen, zijn de Europese verordening DORA (Digital Operational Resilience Act) en de internationale ISO 27001. Beiden bieden houvast bij het beheersen van risico's en informatiebeveiliging, maar verschillen sterk in aanpak en toepassing. Wat houden deze kaders precies in? En hoe versterken ze elkaar in de praktijk?

De Digital Operational Resilience Act is een Europese wetgeving die specifiek gericht is op financiële organisaties. De wetgeving is bedoeld om de operationele digitale weerbaarheid van financiële instellingen te verbeteren. Banken, verzekeraars en andere financiële spelers moeten hiermee hun digitale weerbaarheid aantoonbaar op orde hebben. De verordening schrijft onder meer het volgende voor:

- Strenge eisen voor risicobeheer: Organisaties moeten een grondig gedocumenteerd risicobeheerproces hanteren voor het identificeren en beheersen van digitale risico's.
- Incidentrapportage: Financiële instellingen moeten cyberincidenten snel en via gestandaardiseerde procedures rapporteren aan de toezichthouders.
- Verplichte stresstests: Digitale veerkracht wordt periodiek getoetst door middel van tests.
- Controle op ICT-leveranciers: Ook externe ICT-dienstverleners vallen onder het toezicht – met eisen voor cybersecurity en naleving.

Het doel van DORA is niet alleen om cyberincidenten te voorkomen, maar juist ook om organisaties in staat te stellen snel en effectief te herstellen na een incident. Dit is een cruciale verandering binnen de financiële sector.

Internationaal fundament

ISO 27001 is een wereldwijd erkende norm voor informatiebeveiligingsmanagement. Het helpt organisaties om gevoelige gegevens te beschermen door middel van een gestructureerde aanpak. ISO 27001 draait om:

- Risicobeoordeling en -behandeling: Organisaties moeten risico's identificeren en beheersen met passende maatregelen.
- Beheersmaatregelen (Annex A): Een uitgebreide set voorschriften voor onder meer toegangsbeheer en encryptie.
- Continue verbetering: Het Information Security Management System (ISMS) moet structureel worden bijgewerkt en verbeterd.
- Certificering: Organisaties kunnen zich laten certificeren om aan te tonen dat zij voldoen aan de norm.

J.J. (Joyce) Koops, Manager Compliance bij SVC Groep te Amersfoort

ISO 27001 is sectoronafhankelijk. Dat betekent dat het niet alleen toepasbaar is op financiële instellingen, maar op alle organisaties die hun informatiebeveiliging willen versterken.

Gedeelde thema's

Hoewel DORA en ISO 27001 allebei een eigen insteek hebben, raken ze elkaar op meerdere fronten:

- Focus op risicobeheer – Beide kaders benadrukken het belang van een gestructureerde aanpak om cyberrisico's te beheersen.
- Incidentrespons en continuïteitsbeheer – Organisaties moeten plannen hebben om cyberincidenten snel en effectief te bestrijden.
- Leveranciersbeheer – Zowel DORA als ISO 27001 leggen nadruk op het belang van cybersecurity bij externe dienstverleners.
- Compliance en audits – Regelmatige controles en nalevingsaudits spelen een essentiële rol in beide kaders.

Verschillen die ertoe doen

Zowel DORA als ISO 27001 zijn gericht op informatiebeveiliging. De belangrijkste verschillen zitten in de aanpak en toepassing. DORA is verplicht binnen de Europese Unie en richt zich specifiek op de financiële sector. Dit betekent dat banken, verzekeraars en andere financiële instellingen wettelijk verplicht zijn om te voldoen aan de strikte eisen die DORA stelt. ISO 27001 daarentegen is vrijwillig. Deze internationale norm kan elke organisatie toepassen, ongeacht de sector waarin zij actief is.

'WAAR DORA WETTELIJKE VERPLICHTINGEN OPLEGT, BIEDT ISO 27001 EEN SOLIDE BASIS VOOR STRUCTURELE INFORMATIEBEVEILIGING'

De focus is een ander belangrijk onderscheid. ISO 27001 richt zich primair op het opzetten van een beheersysteem voor informatiebeveiliging en de bescherming van vertrouwelijke gegevens. DORA gaat een stap verder en reguleert ook de digitale weerbaarheid van organisaties. Dat betekent dat DORA niet alleen eisen stelt aan risicobeheer en incidentrespons, maar ook verplichte stresstests en continue monitoring van ICT-leveranciers voorschrijft.

Bovendien kent DORA strikte regelgeving voor incidentrapportage. Organisaties moeten cyberincidenten binnen een vastgesteld tijdsbestek melden aan toezichthouders. Dat is bij ISO 27001 niet verplicht. Ook eist DORA van financiële instellingen dat ze regelmatig operationele weerbaarheidstesten uitvoeren om hun digitale veerkracht te waarborgen. DORA legt dus de nadruk op wettelijke naleving en digitale veerkracht binnen de financiële sector, terwijl ISO 27001 een generieke, sectoronafhankelijke benadering biedt voor informatiebeveiliging.

DORA EN ISO 27001 ZIJN ALLEBEI CRUCIAAL VOOR CYBERSECURITY ÉN RISICOBEHEER

Hoe combineer je DORA en ISO 27001?

Hoe kun je als organisaties beide kaders toepassen? Voor veel financiële organisaties is naleving van zowel DORA als ISO 27001 noodzakelijk. Dan is het verstandig om ISO 27001 als fundament te gebruiken. Daarmee kunnen veel vereisten van DORA efficiënt worden ingevuld.

- Een ISO 27001-gecertificeerd ISMS kan als fundament dienen voor de implementatie van DORA-vereisten.
- Risicobeoordelingen stroomlijnen. DORA vereist een strikte risicobeoordeling, die grotendeels kan worden gedekt door het bestaande ISO 27001-raamwerk.
- Incidentmanagementprocessen combineren. Bestaande incidentresponsprocedures onder ISO 27001 kunnen eenvoudig worden uitgebreid met de rapportagevereisten van DORA.
- Leveranciersbeheer te versterken. Terwijl ISO 27001 reeds richtlijnen biedt voor leveranciersbeheer, vereist DORA nog strengere controles en compliance-maatregelen.

Met deze integrale aanpak voldoe je niet alleen aan de regels van DORA en ISO 27001, maar werk je ook aan een hogere mate van digitale weerbaarheid.

Tot slot

DORA en ISO 27001 zijn allebei cruciaal voor cybersecurity én risicobeheer. ISO 27001 biedt een solide, internationaal erkend raamwerk voor informatiebeveiliging. DORA bouwt daarop voort met specifieke verplichtingen voor financiële instellingen binnen de EU. Door beide kaders strategisch te combineren, voldoen organisaties niet alleen aan de regelgeving, maar ontwikkelen ze ook een veerkrachtige cybersecuritystrategie, die bestand is tegen de steeds grotere impact van cyberdreigingen. <