# *DORA vs. ISO 27001:* WAT BETEKENT DIT VOOR ORGANISATIES?

In een wereld waarin cyberdreigingen aan de orde van de dag zijn, moeten organisaties zich wapenen met de juiste richtlijnen en regelgeving. Twee belangrijke kaders die hierbij een rol spelen, zijn DORA (Digital Operational Resilience Act) en ISO 27001. Beide zijn gericht op informatiebeveiliging en risicobeheer, maar verschillen in hun aanpak en toepassing. Wat betekenen deze kaders in de praktijk en hoe kunnen organisaties zich voorbereiden?

Wat is DORA? DORA is een Europese verordening die specifiek is ontwikkeld voor de financiële sector. De wetgeving is bedoeld om de operationele digitale weerbaarheid van financiële instellingen te verbeteren. Dit betekent dat banken, verzekeraars en andere financiële spelers verplicht worden om strikte maatregelen te treffen op het gebied van ICT-risicobeheer. Denk hierbij aan:

- Strenge eisen voor risicobeheer: Organisaties moeten een goed gedocumenteerd risicobeheerproces hanteren voor digitale dreigingen.
- Incidentrapportage: Financiële instellingen moeten cyberincidenten snel en op gestandaardiseerde wijze rapporteren aan toezichthouders.
- Verplichte stresstests: Regelmatige tests om de digitale veerkracht te beoordelen.
- Toezicht op ICT-leveranciers: Strikte controle op de cybersecuritymaatregelen van externe ICT-dienstverleners.

DORA stelt organisaties niet alleen in staat om cyberdreigingen te voorkomen, maar ook om snel te herstellen na een incident. Dit is een cruciale verandering binnen de financiële sector.

**Wat is ISO 27001?**

ISO 27001 is een internationale norm die zich richt op informatiebeveiligingsmanagement. Het helpt organisaties om gevoelige gegevens te beschermen door middel van een gestructureerde aanpak. Enkele kernaspecten van ISO 27001 zijn:

- Risicobeoordeling en -behandeling: Organisaties moeten risico's identificeren en beheersen met specifieke maatregelen.
- Beheersmaatregelen (Annex A): Een

'DORA stelt organisaties niet alleen in staat om cyberdreigingen te voorkomen, maar ook om snel te herstellen na een incident'

uitgebreide set richtlijnen voor onder andere toegangsbeheer en encryptie.
- Continue verbetering: Het ISMS (Information Security Management System) moet voortdurend worden geoptimaliseerd.
- Certificering: Organisaties kunnen zich laten certificeren om aan te tonen dat zij voldoen aan de norm.

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

**Overeenkomsten DORA en ISO 27001**

Hoewel DORA en ISO 27001 verschillend van aard zijn, delen ze meerdere overeenkomsten:
- 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.

**Wat zijn de belangrijkste verschillen?**

Hoewel DORA en ISO 27001 beide gericht zijn op informatiebeveiliging, zijn er enkele duidelijke verschillen in hun aanpak en toepassing. DORA is een verplichte verordening 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 een vrijwillige, internationale norm die elke organisatie kan toepassen, ongeacht de sector waarin zij actief is.

Een ander belangrijk onderscheid is de focus. Waar ISO 27001 zich primair richt op het opzetten van een beheersysteem voor informatiebeveiliging en de bescherming van vertrouwelijke gegevens, gaat DORA verder door ook de digitale weerbaarheid van organisaties te reguleren. Dit houdt in dat DORA niet alleen eisen stelt aan risicobeheer en incidentrespons, maar ook verplichte stresstests en continue monitoring van ICT-leveranciers voorschrijft.

Daarnaast kent DORA strikte vereisten voor incidentrapportage. Organisaties moeten cyberincidenten binnen een vastgesteld tijdsbestek melden aan toezichthouders, wat bij ISO 27001 niet verplicht is. Ook verplicht DORA financiële instellingen om regelmatig operationele weerbaarheidstesten uit te voeren om hun digitale veerkracht te waarborgen. Kort samengevat; DORA legt de nadruk op wettelijke naleving en digitale veerkracht binnen de financiële sector, terwijl ISO 27001 een generieke, sectoronafhankelijke benadering biedt voor informatiebeveiliging.

**Beide toepassen**

Hoe kunnen organisaties beide toepassen? Voor veel organisaties in de financiële sector is naleving van zowel DORA als ISO 27001 noodzakelijk. Dit kan efficiënt door:
- ISO 27001 als basis te gebruiken – Een ISO 27001-gecertificeerd ISMS kan als fundament dienen voor de implementatie van DORA-vereisten.
- Risicobeoordelingen te stroomlijnen – DORA eist een strikte risicobeoordeling, die grotendeels kan worden gedekt door het bestaande ISO 27001-raamwerk.
- Incidentmanagementprocessen te 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 compliancemaatregelen.

Door DORA en ISO 27001 samen te implementeren, kunnen financiële instellingen niet alleen voldoen aan de wettelijke verplichtingen, maar ook hun algehele cyberweerbaarheid verbeteren.

**Conclusie**

DORA en ISO 27001 zijn beide cruciaal voor cybersecurity en risicobeheer, maar ze hebben verschillende toepassingen. DORA is een verplichte EU-wetgeving voor financiële instellingen, terwijl ISO 27001 een wereldwijd erkende vrijwillige norm is. Voor financiële instellingen is een combinatie van beide de beste aanpak: ISO 27001 biedt een solide basis voor informatiebeveiliging, terwijl DORA extra verplichtingen stelt aan digitale weerbaarheid en compliance. Door slim gebruik te maken van beide kaders kunnen organisaties niet alleen voldoen aan de regelgeving, maar ook een veerkrachtige cybersecuritystrategie ontwikkelen, die bestand is tegen de steeds veranderende digitale dreigingen. ●

**foto HR aanleveren**

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