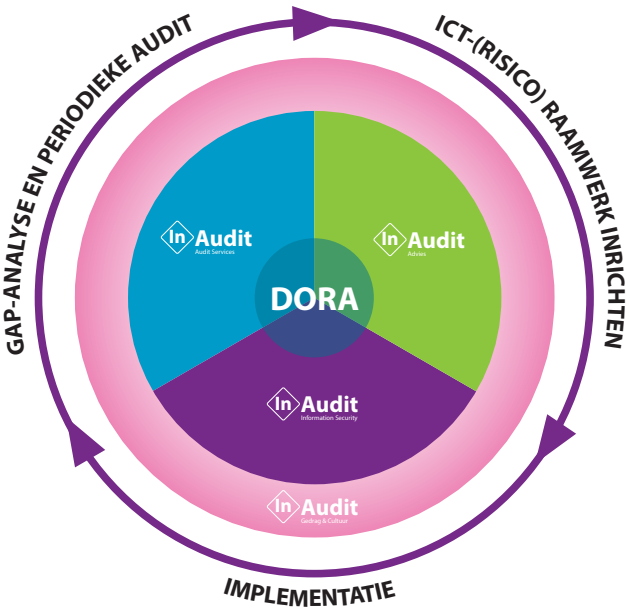
DORA
Digital Operational Resilience Act

Binnen de financiële sector is sprake van verregaande digitalisering en deze ontwikkeling blijft zich voortzetten. In combinatie met de grote hoeveelheid (persoonlijke) data en de ontwrichting van de samenleving bij omvangrijke verstoringen, zorgt dit ervoor dat het risico op cyberaanvallen in de financiële sector onverminderd hoog is. Om dit risico te beperken heeft de Europese Commissie een nieuwe verordening aangenomen, genaamd DORA (Digital Operational Resilience Act).

De DORA verordening moet de digitale weerbaarheid van de financiële sector in Europa versterken, zowel door de inzet van preventieve als correctieve maatregelen. Organisaties en hun IT-dienstverleners zouden cyberaanvallen en andere soorten IT-gerelateerde verstoringen en bedreigingen moeten kunnen weerstaan door het implementeren van best practices. DORA stelt eisen aan de financiële sector aan de hand van een vijftal pijlers, waaronder IT-incidentenbeheer, IT-risicomanagement en het periodiek testen van digitale weerbaarheid. Ook ligt er nadruk op de beheersing van IT-risico's bij uitbestedingen en op de uitwisseling van informatie binnen de sector en met de toezichthouders.

De DORA verordening is eind 2022 aangenomen en treedt vanaf 17 januari 2025 in werking. Dat betekent dat financiële entiteiten die binnen de reikwijdte van de verordening vallen nog twee jaar hebben om te voldoen aan de voorschriften.

Proces voorbereiding DORA



Bij InAudit verenigen wij onze verschillende expertises om bedrijven in de financiële sector, zoals dat van u, te helpen met het implementeren van DORA. Overigens is het ook voor organisaties buiten de scope van DORA verstandig om de weerbaarheid te verbeteren. In dit artikel geven wij per expertise aan hoe wij hieraan kunnen bijdragen.

Onze expertises:
- Audit Services,
- Information Security,
- Gedrag & Cultuur en
- Risicomanagement

Waar mogelijk bundelen wij onze krachten om u te helpen.

We kunnen ons voorstellen dat het ingewikkeld is om de vereisten die DORA stelt te vertalen naar uw organisatie. Neem gerust contact op met een van onze consultants voor een vrijblijvend gesprek.

Risicomanagement

De kern van DORA wordt gevormd door artikel 6: het kader voor ICT-risicobeheer. Financiële entiteiten moeten, als onderdeel van hun algemene risicobeheersysteem, beschikken over een solide, alomvattend en goed gedocumenteerd kader voor de beheersing van ICT-risico's. Dit betekent dat een entiteit strategieën, beleid, procedures, protocollen en instrumenten tot zijn beschikking heeft om informatie en ICT-activa te beschermen tegen ongeoorloofde toegang en gebruik. DORA schrijft vervolgens in gedetailleerde bewoordingen voor wat een financiële entiteit ingeregeld moet hebben. Die voorschriften eindigen niet bij de poorten van uw eigen organisatie, want u bent tevens verplicht het ICT-risico van uw IT-leveranciers te integreren in uw eigen kader voor ICT-risicobeheer. Het belang van adequaat uitbestedingsmanagement wordt met DORA wederom bevestigd.

Onze consultants van InAudit Advies hebben kennis van de DORA voorschriften en helpen u graag bij de naleving ervan. Dat kan via deeltrajecten, zoals de uitvoering van een gapanalyse of via de aanscherping van uw uitbestedingsbeleid en -regelingen, maar ook via integrale implementatietrajecten zodat uw kader voor ICT-risicobeheer op orde is, zowel in opzet als in werking. Uiteraard zoeken onze consultants daarbij naar een gezonde balans tussen proportionaliteit, best practices en uw eigen beleidslijnen.

Information Security

De doelstelling van DORA is het verhogen van de cyberweerbaarheid van (financiële) organisaties. Het managementsysteem dat u daarvoor inricht moet u ook implementeren, testen, monitoren en periodiek uitdagen op effectiviteit (en efficiency). Dit alles moet u ook aantoonbaar maken.

Het implementeren van cybersecuritymaatregelen vergt een nuchtere houding, een gezond verstand, maar vooral een hands-on aanpak. Daarin proberen onze consultants zich te onderscheiden. Met de kennis en ervaring die we opdoen bij vergelijkbare organisaties kunnen we zorgen voor effectieve voortgang, maar zijn we tevens een goed klankbord om 'lessons learned' te delen. We helpen u graag !

Audit Services

Vanuit InAudit Audit Services kunnen wij op verschillende momenten van de implementatie van de DORA-wetgeving met u meekijken. Allereerst kunnen wij voor u een gap-analyse uitvoeren. Dit stelt ons in staat om eventuele tekortkomingen te identificeren en voor u in kaart te brengen wat er moet gebeuren om te voldoen aan de vereisten vanuit DORA. Zo'n analyse geeft daarmee een helder inzicht in wat u te doen staat zodat u kunt prioriteren en plannen.

Naast bovengenoemde gap-analyse die vóór de inwerkingtreding van DORA kan worden uitgevoerd, staat uw auditteam paraat om de implementatie van DORA te toetsen. Ook hieraan verbinden we, zoals u van ons gewend bent, aanbevelingen die u kunt gebruiken om uw bedrijfsvoering in lijn te brengen met deze nieuwe regelgeving.

Gedrag & Cultuur

Ook vanuit Gedrag & Cultuur kunnen we op een aantal vlakken met u meedenken die in het kader van DORA belangrijk zijn. Zo legt DORA de nadruk op de inrichting van een aantal governance-aspecten. Hierbij is het zoals altijd van belang dat degenen die verantwoordelijk worden gemaakt voor, in dit geval bijvoorbeeld het ICT-risicobeheer ook daadwerkelijk deze rol op zich nemen. Hoe gaat u dit inbedden in de organisatie? En hoe zorgt u dat de verantwoordelijke deze rol ook werkelijk kan en gaat vervullen? Ditzelfde geldt ook voor het inrichten van het crisiscommunicatieplan dat van kracht wordt bij ernstige ICT-gerelateerde incidenten. En zo bevat DORA nog een aantal elementen waarbij het loont om hier goed over na te denken.

Artikel 13 van DORA gaat over voorschriften rond scholing en ontwikkeling; óók een onderwerp dat raakt aan Gedrag en Cultuur. Dit artikel schrijft onder meer voor dat organisaties bewustmakingsprogramma's moeten ontwikkelen voor álle werknemers. De mate van complexiteit van deze programma's moet passen bij het takenpakket van de betreffende personeelsleden. Dit geldt ook voor het hoger leidinggevend personeel. Hoe denkt u dit te gaan oppakken? Hoe gaat u dit opnemen in uw opleidings- en/of geschiktheidsplan? En waar let u op als u dit gaat uitbesteden? In bredere zin besteedt DORA sowieso veel aandacht aan het continu signaleren en benutten van verbeterpotentieel. En ook dit is een onderwerp waar het loont om met aandacht naar te kijken: hoe gaat u dit inrichten? Hoe zorgt u dat dit daadwerkelijk, tijdig en volledig gebeurt?

Wat kunnen wij vanuit InAudit voor u betekenen?

Wij helpen u graag met het in beeld brengen van de regelgeving, een plan van aanpak en de bemensing om snel voortgang te realiseren.

Wij kunnen u ondersteunen bij het aanscherpen en structureren van de beleidsmatige opzet, zodat deze in lijn is met de vereisten vanuit DORA.

Wij kunnen u adviseren over het implementeren van dit beleid zodat compliance met DORA aantoonbaar is. Oók als het gaat om het aantoonbaar in control zijn wat betreft door u uitbestede werkzaamheden.

Wij kunnen u ondersteunen bij het rapporteren over ICT-gerelateerde incidenten. U kunt dan denken aan advies over het vormgeven van een beoordelingsformulier om ICT-gerelateerde incidenten te categoriseren. Wij kunnen u ook helpen bij het opstellen van een rapportageformat.

Wij kunnen een readiness-assessment of gap-analyse voor u uitvoeren.

Wij kunnen u adviseren over het organiseren van een PEN-test, en/of het laten uitvoeren hiervan binnen uw gehele uitbestedingsketen.

Wij kunnen met u meedenken over het inrichten van awareness-programma's en opleidingsprogramma's.

Wij kunnen u adviseren over het optimaal benutten van verbeterpotentieel.

Team DORA

Vragen of wilt u meer informatie? Neem gerust even contact met ons op. We denken graag met u mee.

Frederike Gieles
Senior Auditor en Consultant Gedrag & Cultuur
06-11 09 69 89

Annebeth Groen
Auditor en CISO
06-25 10 55 45

Niels Bokkers
Senior Risk Consultant
06-15 43 67 74

Robert Verweij
Auditmanager Audit Services
06-25 29 69 67

Ronald van de Langenberg
Algemeen Directeur InAudit
06-24 48 68 92