KPMG

De proef op de DORA-som: De weg naar duurzame compliance

Een nieuwe uitdaging voor verzekeringsprofessionals

Introductie

Als professional in de verzekeringssector heb je ongetwijfeld de implementatiefase van de Digital Operational Resilience Act (DORA) meegemaakt. Op 16 januari 2023 trad deze Europese regelgeving in werking, met een tweejarige implementatietermijn die op 17 januari 2025 afliep. DORA stelt minimale eisen aan de digitale en operationele weerbaarheid van je organisatie, en nu is het moment aangebroken om de daadwerkelijke proef op de som te nemen.

Een belangrijk aspect dat aandacht verdient: DORA gaat niet alleen over jouw organisatie, maar over de gehele keten waarin jullie opereren. Dit maakt de implementatie complexer dan veel andere regelgeving; the devil is in the detail.

Waar staat je organisatie?

Als C-level executive in de verzekeringssector zie je waarschijnlijk dat er nog veel werk verzet moet worden. Wat wij in de financiële sector observeren, is dat organisaties worstelen met verschillende aspecten van DORA-compliance. De regelgeving brengt namelijk zeer specifieke deliverables met zich mee die aanzienlijke inspanningen vereisen:

- Het opzetten van het informatieregister voor ICT Third Party Service Providers;
- Het ontwikkelen van een Digital Operational Resilience Strategy;
- Het implementeren van een volledig beleids- en procedureraamwerk als onderdeel van ICT-risicomanagement.

De meeste organisaties zijn goed op weg, maar er moeten nog veel documenten worden aangepast en systemen moeten veiliger worden.

Er is beleid en er zijn procedures, maar de echte uitdaging ligt in de vertaling naar de werkvloer: hoe past DORA in de dagelijkse werkwijze van jullie medewerkers?

Voor veel verzekeraars die onder DORA vallen, is dit IT-gerelateerde regelgevend toezicht relatief nieuw terrein. Als professional in deze sector merk je waarschijnlijk dat extra inspanningen nodig zijn om aan alle vereisten te voldoen. De aandacht vanuit De Nederlandsche Bank (DNB) voor DORA-compliance geeft het belang van een grondige aanpak aan.

De volgende fase: van implementatie naar duurzame compliance

We bevinden ons nu op de drempel van een nieuwe fase. Na de initiële implementatie-inspanningen, gaat het er nu om volledige naleving aan te tonen en deze te bestendigen. In termen van de 'Plan-Do-Check-Act'-cyclus: het Plan is er, de Do-fase loopt, en we bewegen nu richting de Check- en Act-fasen.

Voor jou als verzekeringsexecutive betekent dit dat alle geïmplementeerde vereisten hun weg moeten vinden naar jullie dagelijkse (bedrijfs)processen en naar jullie externe ICT-dienstverleners.

Het is verstandig om proactief te handelen en niet te wachten op een uitvraag door de toezichthouder.

De weg naar duurzame compliance

Hoe begin je aan deze reis en bereik je duurzame compliance? In onze visie zijn de volgende elementen van belang:

1. **Geïntegreerd controleframework**
Is jullie internal control framework (ICF) voldoende geïntegreerd om rekening te houden met zowel DORA als andere (ICT-gerelateerde) regelgeving? Dit maakt het 'test once, comply to many'-principe mogelijk, waardoor je als verzekeringsexecutive zowel effectief als tijdsefficiënt kunt opereren.

De Nederlandse Orde van Register EDP-Auditors (NOREA) biedt een DORA Control Framework waarmee je naleving kunt aantonen en de controls met betrekking tot onderliggende stromen op orde kunt brengen. Dit kan jullie implementatieproces aanzienlijk versnellen.

Een echte efficiëntieslag wordt bereikt als controls en testen voor meerdere doelen gebruikt kunnen worden, dus naast DORA bijvoorbeeld ook voor cybersecurity, privacy, accountantscontroles, ISO-certificeringen en andere rapportages.

2. **Effectieve rapportageprocessen**
Als professional in de verzekeringssector moet je ervoor zorgen dat de processen voor verschillende DORA-rapportagevereisten goed zijn geïmplementeerd en effectief werken. Dit omvat de rapportageprocessen voor:

- de herziening van het ICT-risicobeheerraamwerk
- ernstige ICT-gerelateerde incidenten
- het informatieregister voor ICT Third Party Service Providers (door DNB en AFM aangemerkt als essentiële compliance-items)
- kosten en verliezen als gevolg van ICT-gerelateerde incidenten

3. **Testprogramma voor digitale operationele veerkracht**
Is het testprogramma gedefinieerd en worden externe partijen betrokken bij het uitvoeren van tests?

4. **Management van externe ICT-dienstverleners**
Voor een C-level executive is het essentieel dat:

- DORA-contractwijzigingen worden voltooid
- DORA-vereisten voor uitbestede diensten correct worden geïmplementeerd
- zekerheid wordt verkregen over naleving van de nieuwe DORA-contractbepalingen door de ICT-leveranciers
- interne (binnen een groep) ICT-dienstverleners dezelfde behandeling krijgen als externe leveranciers

5. **Gedocumenteerde compliance**
Gezien de omvang van de DORA-vereisten, is het voor jou als verzekeringsprofessional essentieel om per DORA-artikel te documenteren welke controles zijn geïmplementeerd. Bijvoorbeeld door een 'DORA Compliance Chart' te ontwikkelen.

Integratie op alle niveaus

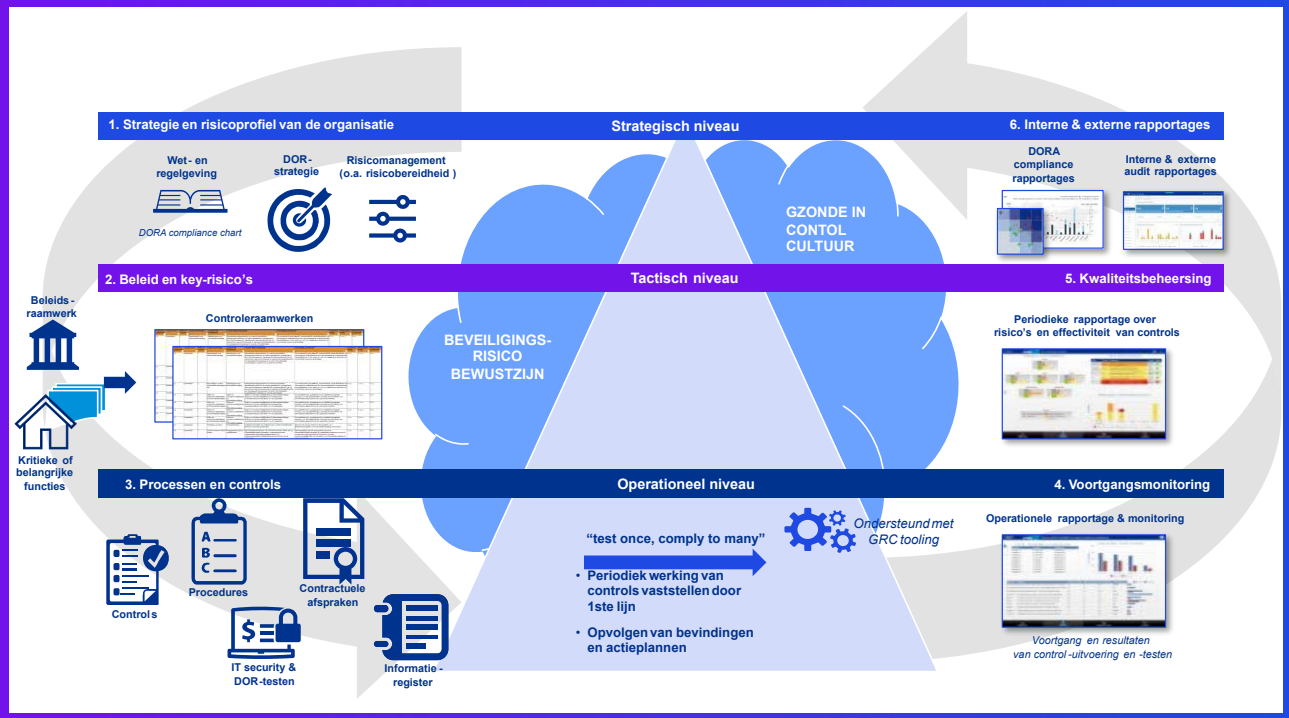
Om DORA volledig in je verzekeringsorganisatie te integreren en het 'test once, comply to many'-principe te bereiken, moet DORA worden ingebed op drie niveaus:

- **Strategisch niveau:** identificeren van wet- en regelgeving, risicobeoordeling, en beleidsontwikkeling
- **Tactisch niveau:** implementateren van beleid en het identificeren van de belangrijkste risico's en 'kritieke of belangrijke functies'
- **Operationeel niveau:** implementeren van processen en controles, en het testen daarvan

Voor veel verzekeraars is dit de huidige situatie na de implementatiefase. De volgende stap voor jou als executive is de overgang van operationeel niveau naar een hoger niveau, waarbij:

- de voortgang wordt bewaakt
- kwaliteitsbeheersing plaatsvindt
- interne en externe rapportage wordt verzorgd

In essentie is het een 'Plan-Do-Check-Act'-cyclus die begint op strategisch niveau en daar ook weer eindigt. Als verzekeringsprofessional sta je nu voor de uitdaging om deze cyclus volledig te doorlopen en een duurzame DORA-compliance te bereiken.



Key take-outs

Tot slot geven we je graag de volgende aandachtspunten mee:

1. Wees proactief:
Toezichthouders zijn momenteel nog voorzichtig in hun uitvraag, maar laat het er niet op aankomen. Zorg dat jullie DORA-compliance op orde is voordat je moet rapporteren. Overweeg een DORA Readiness Assessment om tussentijds de voortgang te meten.

2. Bereid de hele organisatie voor:
Het kost tijd om aanpassingen te laten landen in de dagelijkse praktijk. Voor je het weet is het weer het eind van het jaar.

3. Integreer DORA in de keten:
Vraag leveranciers om te sturen op effectiviteit van DORA-vereisten. Zoek naar oplossingen om te automatiseren en efficiënter met systemen om te gaan.

Verder praten?

KPMG biedt ondersteuning om je 'Plan-Do-Check-Act'-cyclus te laten voldoen aan de DORA-vereisten. Ook biedt KPMG Challenge Sessies voor boardmembers, waarin besproken wordt wat de verantwoordelijkheid en aansprakelijkheid van de board is ten aanzien van DORA. Neem contact met ons op om te bespreken hoe wij je kunnen ondersteunen bij jullie DORA-compliancetraject.

Contact

Meer informatie?

Neem contact op met onze experts:

Arno Kroese

Director

kroese.arno@kpmg.nl
+31 020 6 568460

Riccardo Altenburg

Director Digital Transformation

altenburg.riccardo@kpmg.nl
+31 020 6 568407

KPMG

www.kpmg.nl

Juni 2025