DORA-Compliance met behulp van onze tools en oplossingen

InAudit begrijpt dat de naleving van de Digital Operational Resilience Act (DORA) veel tijd en inspanning van bedrijven vereist. Tijd die ze liever besteden aan andere belangrijke zaken. Om financiële instellingen te ondersteunen in hun DORA implementatieproces, heeft InAudit vier producten ontwikkeld. Deze oplossingen van InAudit zetten financiële instellingen op de fast track naar DORA-Compliance.

Onze 4 oplossingen:
1. Gap-analyse tool
2. Voorbeeld van het evaluatieverslag
3. Template voor ICT-incidentmelding
4. Template voor uitbesteding aan service-providers

1. Gap-analyse tool
Een van de ontwikkelde producten is de Gap-analyse tool. Deze tool is speciaal ontwikkeld om organisaties te helpen identificeren wat er tussen hun bestaande status en DORA-Compliance staat, en welke acties ze kunnen ondernemen om deze kloof te dichten. Met deze tool kunnen organisaties per DORA-wetsartikel en per lid een evaluatie uitvoeren, waarbij ze hun huidige nalevingsstatus kunnen beoordelen op gebieden zoals incident response, ICT-risicomanagement en operationele veerkracht. Door de resultaten te visualiseren in een overzichtelijk dashboard, kunnen bedrijven gericht sturing geven aan hun inspanningen en eventuele hiaten identificeren, prioriteren en aanpakken. Door de tool periodiek te updaten kan ook de voortgang worden bewaakt.

2. Evaluatieverslag
In DORA is opgenomen dat organisaties jaarlijks, én na een ernstig ICT-incident, een evaluatieverslag opstellen waarbij zij gedetailleerd alle gebeurtenissen en ontwikkelingen binnen het ICT-landschap vastleggen. Dit evaluatieverslag kan de toezichthouder opvragen. Wat er in het verslag moet worden vastgelegd en hoe dit vorm moet krijgen is door de ESA's gedetailleerd voorgeschreven in de Regulatory Technical Standards. Het betreft twee pagina's aan voorschriften waar dit verslag aan moet voldoen. Vanuit een blanco opzet uitwerken van een voorbeeldverslag kan tijdrovend zijn. Om dit alles te vergemakkelijken heeft InAudit op basis van de voorschriften een voorbeeldverslag

Sneak peek van het dashboard uit onze gap-analyse tool

opgesteld. Aan de hand van een fictieve entiteit bieden we een voorbeeld van hoe zo'n verslag er uit kan zien. Organisaties kunnen dit template gebruiken als inspiratie om aan de opgestelde voorschriften qua vorm en inhoud te voldoen. In plaats van zich door alle regelgeving heen te worstelen helpen we organisaties zo op weg. Door het door ons ontwikkelde template in de eigen context te brengen is al een belangrijk deel van het werk gedaan.

3. ICT-incidentmelding
De wettelijke norm om een ernstig ICT-incident te melden is binnen vier uur voor de eerste kennisgeving aan de toezichthouder. Om ervoor te zorgen dat organisaties zich tijdens deze vier uur kunnen focussen op het incident en niet op de vormvoorschriften van de kennisgeving, heeft InAudit een template gecreëerd, waarin alle te melden datavelden zijn opgenomen. Deze tool stelt organisaties in staat om te oefenen met het melden van ernstige ICT-gerelateerde incidenten conform de voorschriften van de ESA's. In het tool zitten verwijzingen naar de classificatie-criteria, drop-down menu's als het gaat om 'closed lists' en de toelichtingen zijn vertaald. Door te oefenen met dit tool, kan beter inzicht worden verkregen in welke informatie moet worden verzameld en gerapporteerd, wanneer een 'ernstig' ICT-incident zich voordoet.

4. Ketenpartners
Als het gaat om het onderdeel 'uitbesteding aan serviceproviders' gaat veel aandacht uit naar de toets en de update van de uitbestedingsovereenkomsten. Maar een ander belangrijk onderdeel is de verplichting om een 'informatieregister' bij te houden van alle serviceproviders. Daarbij gaat het niet alleen om de directe ICT-uitbestedingsrelaties, maar ook (als het belangrijke of kritieke processen betreft) om de onderaannemers van deze directe relaties en mogelijk zelfs de onderaannemers daarvan. De ESA's hebben het format daarvan gepubliceerd, maar wij hebben dat in een prettige layout gezet, verrijkt met toelichtingen, drop-down menu's en toelichtingen in het Nederlands. Op deze manier kom je wat gemakkelijker tot een eerste opzet. Vanaf het moment dat DORA van kracht is kan de toezichthouder dit register opvragen.

We zijn er om u te helpen!
Veel organisaties vliegen de DORA aan als een complianceproject vergelijkbaar met de invoering van de AVG. Daarvan heeft het ook zeker wel enkele kenmerken. Maar DORA gaat ook inhoudelijk over de inrichting van uw ICT-security management en daarin hebben we ook enige expertise opgebouwd. Met deze vier tools willen we u graag ondersteunen met uw implementatieproject.