BDO

IT RISK ASSURANCE

DORA-checklist voor bestuurders

Artikel 5 van de Digital Operational Resilience Act (DORA) beschrijft de governance en organisatorische verantwoordelijkheden van het bestuur en het management (leidinggevend orgaan). Het bestuur is eindverantwoordelijk voor de beheersing van IT-risico's van de organisatie.

Verantwoordelijkheden bestuur

De specifieke verantwoordelijkheden die bestuurders en het uitvoerend management volledig moeten omarmen en prioriteit moeten geven zijn:

- ☐ **Uiteindelijke verantwoordelijkheid:** Accepteer de uiteindelijke verantwoordelijkheid voor de beheersing van ICT-risico's binnen de financiële entiteit om digitale operationele weerbaarheid te borgen.
- ☐ **Data-integriteit en vertrouwelijkheid:** Stel beleid op om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gevoelige informatie te waarborgen.
- ☐ **Duidelijke rollen en verantwoordelijkheden:** Definieer duidelijke rollen en verantwoordelijkheden voor ICT-gerelateerde functies en stel effectieve governanceregelingen vast.
- ☐ **Strategie voor digitale weerbaarheid:** Stel de strategie voor digitale operationele weerbaarheid vast en keur deze goed, inclusief risicotolerantieniveaus voor ICT-risico's.
- ☐ **ICT-bedrijfscontinuïteit en responseplannen:** Keur ICT-bedrijfscontinuïteitbeleid, -response en herstelplannen goed. Houd toezicht en evalueer periodiek.
- ☐ **Interne audit en budgettering:** Beoordeel interne ICT-auditplannen en budgettoewijzingen voor digitale operationele weerbaarheid en keur deze goed.
- ☐ **Beleid m.b.t. derde aanbieders van ICT-diensten:** Keur beleid dat verband houdt met het gebruik van ICT-diensten die worden geleverd door derde aanbieders (IT dienstverleners) goed en zorg dat deze is afgestemd op de strategie voor digitale operationele weerbaarheid.
- ☐ **Monitoren van ICT-diensten van derde aanbieders:** Monitor de risico's van het gebruik van ICT-diensten van derde aanbieders en de impact van wijzigingen aan deze diensten.
- ☐ **Continue educatie:** Blijf op de hoogte van ICT-risico's door regelmatige training en vaardigheidsontwikkeling om ICT-risico's effectief te kunnen beoordelen en te beheersen.

BDO: uw partner voor DORA-compliance

De Europese Unie heeft 17 januari 2025 vastgesteld als deadline voor het bereiken van DORA-naleving. Hoewel dit misschien een verre doelstelling lijkt, is het in feite een zeer complexe en uitdagende taak die een gezamenlijke inspanning vereist van de financiële entiteiten die onder de DORA-regelgeving vallen.

Wij begrijpen de diepgaande impact die de reis naar DORA-naleving heeft op financiële instellingen. Ons team van technische experts op het gebied van DORA staat klaar om uw organisatie te helpen bij het navigeren in deze complexe omgeving.

Wat kan BDO voor u betekenen?

- Training van bestuur en management over DORA;
- Deskundige begeleiding bij het voldoen aan DORA;
- Uitvoeren en reviewen van gap-analyses;
- Implementatie van DORA-vereisten en uitvoeren van het DORA-actieplan;
- Uitvoeren van risicoanalyses;
- Ontwikkelen en implementeren van incidentmanagement- en bedrijfscontinuïteitsplannen;
- Reviewen van ICT-contracten op DORA-vereisten;
- Bieden van een security officer;
- Security testen en security monitoring;
- Interne en externe IT & cybersecurity audits.

DORA: waar te beginnen?

Bepaal in welke mate de DORA-regelgeving van toepassing is op uw organisatie.

Voer een DORA-gap-analyse uit en beoordeel uw huidige nalevingsniveau rekening houdend met de beschikbare RTS- en ITS-beleidsproducten.

Stel een DORA actieplan op die DORA-specifieke vereisten voor uw organisatie omvat, maar die ook rekening houdt met de naleving van andere toepasselijke wet- en regelgeving.

Projectmanagement en uitvoeren van het DORA-actieplan, bijvoorbeeld het opstellen, aanpassen en implementeren van belangrijke beleidsstukken en procedures, het uitvoeren van securitytesten, het opstellen van het informatie-register en het uitvoeren van risicobeoordelingen op IT-leveranciers.

MEER INFORMATIE

Voor meer informatie over de Digital Operational Resilience Act (DORA), kunt u contact opnemen met:

Maurice Koetsier
Partner IT Risk Assurance | BDO Digital
T +31 (0)30 284 98 27
E maurice.koetsier@bdo.nl

www.bdo.nl

04/2024 – BA2414