

1 Verzamel je basisgegevens om je analyse te maken

- Statuten van je organisatie
- Structuur van moeder- en dochterbedrijven
- Inspraakstructuur (aandeelhouders, stemrechten...)
- Jaaromzet, balanstotaal en personeelsaantallen (laatste drie boekjaren) van je eigen organisatie
- Verzamel een overzicht van effectieve diensten die je verstrekt (niet enkel KBO-registratie of NACE-codes), eventueel op basis van interviews.

2 Bepaal omvang & consolideer gegevens indien nodig (omvangcriterium)

Gebruik de EC-aanbeveling 2003/361/EG om te weten of je gegevens van andere organisaties bij die van je eigen organisatie moet optellen.

- Check of je een kleine, middelgrote of grote entiteit bent
- Bepaal je verbonden ondernemingen en partnerondernemingen
- Jaaromzet, balanstotaal en personeelsaantallen van je verbonden ondernemingen en partnerondernemingen
- Consolideer cijfers van verbonden en partnerondernemingen

3 Identificeer je NIS2-sector(en) (activiteitscriterium)

Check kritisch of je onder een of meerdere sectoren uit bijlage I of II van de NIS2 valt.

- Analyseer je primaire activiteiten
- Analyseer je deelactiviteiten
- Laat een juridische analyse uitvoeren indien je twijfelt of je onder een bepaalde NIS2-sector valt, want dat moet je met zekerheid bepalen om naar de volgende stappen te gaan.

4 Bepaal toepasselijke jurisdictie(s)

- Analyseer je hoofdvestiging en nevenvestigingen. Ook als je geen vestigingen in de EU hebt, kan je onder NIS2 vallen!
- Bepaal of je hoofdvestiging ook je hoofdvestiging is voor NIS2-compliance (want dat is niet noodzakelijk het geval)
- Onderzoek of je onder meerdere nationale wetten valt. Op basis van je NIS2-sectoren, kan het zijn dat je rekening moet houden met elke wet van het land waar je een vestiging hebt, dan wel of je enkel rekening moet houden met de wet van het land van de hoofdvestiging.
- Bepaal hoe je omgaat met multi-jurisdictie compliance (beleid + coördinatie)

5

Controleer of je naast je hoofdactiviteiten ook (deels) clouddiensten aanbiedt of beheerde diensten.

- Controleer of je optreedt als clouddienstaanbieder : bied je een clouddienst aan en is dit niet je hoofdactiviteit ? Dan kan je ook tegelijk als clouddienstaanbieder onder de NIS2 vallen. Dit heeft een impact op je NIS2-compliance.
- Controleer of je een aanbieder van beheerde diensten bent (Managed Service Provider) : bied je ook beheerde diensten aan ? Dan kan je ook tegelijk als MSP onder de NIS2 vallen. Dit heeft een impact op je NIS2-compliance.

6

Besteed extra aandacht aan het beveiligen van je toeleveringsketen.

- Breng je bestaande leveranciers in kaart
- Stel een leveranciersselectie proces op of kijk het bestaande proces na. Het beveiligen van je toeleveringsketen begint al op het moment dat je een leverancier selecteert. Zorg ervoor dat leveranciers die niet NIS2-compliant zijn, niet in de selectie worden opgenomen, of zorg ervoor dat je je daar minstens van bewust bent.
- Besteed voldoende aandacht aan due diligence van de leverancier. Vraag de juiste documentatie op bij de leverancier en beoordeel deze
- Beoordeel hoe kritiek de leverancier is voor je organisatie
- Onderhandel het contract met de nieuwe leverancier in functie van hoe kritiek de leverancier is. Teken het contract niet voordat de juiste maatregelen zijn afgesproken.
- Herbekijk je contracten met bestaande leveranciers in het licht van NIS2.
- Herbekijk eventueel bestaande Contracting Playbooks in het licht van NIS2-compliance.
- Actualiseer je eigen contracten en templates.

7

Documenteer je kwalificatie & analyse

- Laat een NIS2 scan uitvoeren door een juridische specialist of stel een intern rapport op met:
 - Gegevensverzameling
 - Cijferanalyse
 - Juridische inschatting
 - Sectorclassificatie
 - Jurisdictie(s)
 - Leveranciersanalyse
- Als je het rapport intern opstelt, is het raadzaam om het rapport juridisch te laten valideren door een expert. Dit is nodig omdat een foutieve kwalificatie verregaande gevolgen kan hebben, ook voor de persoonlijke aansprakelijkheid van bestuursorganen.

8

Leg je governancestructuur vast

Wie neemt ownership op?

- Wijs een juridisch-technische NIS2-verantwoordelijke aan (bv. DPO, CISO, legal counsel)
- Bepaal de taken van de NIS2-verantwoordelijke
- Zorg voor een gedegen opleiding voor de NIS2-verantwoordelijke
- Zorg voor voldoende resources voor de NIS2-verantwoordelijke
- Betrek andere departementen in de governancestructuur waar nodig (IT, legal, operations en management)