Proportionele certificering is conform de NIS2 Cyberbeveiligingswet

Waarom één zware norm voor alle leveranciers niet logisch is

De NIS2 Cyberbeveiligingswet verplicht organisaties om hun **cyberrisico's structureel in kaart te brengen**. Een belangrijk onderdeel daarvan is de risicoanalyse van leveranciers. NIS2 schrijft daarbij nadrukkelijk **geen one size fits all certificering** voor. Integendeel: proportionaliteit staat centraal.

Stap 1: de verplichte risicoanalyse

Onder NIS2 start je altijd met een risicoanalyse. Daarbij beoordeel je per leverancier:

- **Is er een risico?**
  Heeft deze leverancier toegang tot systemen, data of processen die relevant zijn voor jouw organisatie?
- **Hoe groot is dat risico?**
  Hoe waarschijnlijk is het dat een incident bij deze leverancier jou raakt?
- **Wat is de impact als het misgaat?**
  Denk hierbij aan concrete vragen zoals:
    - Heeft een incident directe impact op primaire processen?
    - Komt de levering van producten of diensten in gevaar?
    - Zijn er gevoelige of vertrouwelijke gegevens in het spel?
    - Hoe lang duurt het voordat een alternatief beschikbaar is?
    - Is er überhaupt een realistisch alternatief?

Deze vragen vormen samen de basis voor een **inhoudelijk onderbouwde keuze**.

Stap 2: risico vertalen naar passende maatregelen

NIS2 vereist dat je **passende en proportionele maatregelen** neemt. Dat betekent:

- Een leverancier met **lage impact** vraagt om een **lagere mate van zekerheid**
- Een leverancier met **hoge impact of kritische afhankelijkheid** vraagt om **zwaardere waarborgen**

Het is dus volledig conform NIS2 om:

- Bij niet-kritische leveranciers te kiezen voor een **lichte normering**
- Alleen bij kritische leveranciers een **zwaardere certificering** te verlangen

Dit is geen versoepeling, maar juist **professioneel risicomanagement**.

Waarom te zware eisen averechts werken

In de praktijk zien we dat organisaties soms geneigd zijn om alle leveranciers dezelfde zware norm op te leggen. Dat lijkt veilig, maar brengt serieuze risico's met zich mee:

- **Leveranciers haken af** omdat de eisen niet in verhouding staan tot hun rol
- **Kosten lopen onnodig op**, en worden uiteindelijk doorberekend
- **Relaties in de keten verslechteren**, terwijl samenwerking cruciaal is
- **Alternatieven verdwijnen**, waardoor je afhankelijker wordt in plaats van onafhankelijker

Belangrijk om te realiseren: **iemand betaalt altijd de rekening**.
Als een leverancier extra audits, tooling of consultants nodig heeft, zie je dat terug in de prijs. Te zware eisen verhogen dus structureel jouw inkoopkosten.

De kern van NIS2: sturen op risico, niet op vinkjes

NIS2 draait niet om het afdwingen van maximale certificering, maar om:

- Bewuste keuzes maken
- Risico's aantoonbaar beheersen
- Proportioneel omgaan met leveranciers
- De keten veilig houden zonder haar te beschadigen

Een lagere normering bij een leverancier met lage impact is dus niet alleen toegestaan, maar **logisch en verdedigbaar**.

Hoe NIS2 Supply Chain (NIS2 SC) aansluit op proportionele certificering

Om proportionaliteit in de praktijk werkbaar te maken, is **NIS2 Supply Chain (NIS2 SC)** ontwikkeld. Dit model vertaalt de uitkomst van je risicoanalyse direct naar een **passend certificeringsniveau per leverancier**, volledig in lijn met de NIS2 Cyberbeveiligingswet.

Van risicoanalyse naar concreet niveau

Na het uitvoeren van de risicoanalyse bepaal je per leverancier:

- de **kritikaliteit**
- de **impact bij uitval**
- de **mate van afhankelijkheid**
- de **gevoeligheid van data of systemen**

Op basis daarvan kies je één van de NIS2 SC-niveaus.

Overzicht van de NIS2 SC-niveaus

NIS2 SC10 – Basis cyberhygiëne
Geschikt voor leveranciers met **lage impact**

- Geen directe impact op primaire processen
- Beperkte of indirecte toegang tot systemen of data
- Alternatieven relatief snel beschikbaar

Dit niveau borgt basismaatregelen zoals beveiligde toegang, back-ups, bewustwording en incidentmelding, zonder leveranciers onnodig te belasten.

NIS2 SC20 – Verhoogd risicoprofiel
Geschikt voor leveranciers met **middelmatige impact**

- Ondersteunend aan primaire processen
- Regelmatige toegang tot systemen of data
- Beperkte uitwijkmogelijkheden

Hier ligt de focus op aantoonbare procesbeheersing, verantwoordelijkheden, leveranciersbeheer en structurele beveiligingsmaatregelen.

NIS2 SC30 – Kritische leveranciers
Geschikt voor leveranciers met **hoge impact**

- Directe invloed op primaire processen
- Geen of nauwelijks alternatieve leveranciers
- Grote impact bij uitval of datalek

Dit niveau vraagt om uitgebreide borging, governance en controle, passend bij de afhankelijkheid en het risico.

Waarom dit precies is wat NIS2 bedoelt

NIS2 verplicht organisaties om:

- risico's te identificeren,
- maatregelen af te stemmen op die risico's,
- en dit aantoonbaar te doen.

NIS2 SC maakt dat concreet en uitvoerbaar, zonder:

- leveranciers onnodig op kosten te jagen,

- ISO-achtige zwaarte op te leggen waar dat niet nodig is,
- of de supply chain onder druk te zetten.

Je kiest dus **niet voor gemak**, maar voor **verantwoord risicobeheer**.

Belangrijk om te onthouden

- Niet elke leverancier hoeft dezelfde norm
- Proportionaliteit is geen uitzondering, maar de regel
- Te zware eisen leiden tot hogere prijzen en minder leveranciers
- NIS2 SC helpt je compliant te zijn én je keten gezond te houden

ISO 27001 is een sterke norm voor interne informatiebeveiliging, maar de norm is **niet ingericht op ketenverantwoordelijkheid zoals NIS2 die vraagt**. ISO 27001 is op zichzelf **niet voldoende** om aan de NIS2 Cyberbeveiligingswet te voldoen. Er ontbreken onderdelen die wel in de wet staan. Organisaties die al ISO 27001 gecertificeerd zijn, hebben een groot deel van de vereiste maatregelen al op orde. Voor hen is het traject naar **NIS2 Supply Chain SC20** beperkt en efficiënt. Bestaande maatregelen hoeven **niet opnieuw te worden ingericht of volledig opnieuw geaudit**, maar worden hergebruikt en aangevuld met de specifieke NIS2-ketenonderdelen.

Conclusie

Proportionele certificering is volledig in lijn met de NIS2 Cyberbeveiligingswet. Door per leverancier het risico en de impact te beoordelen, voorkom je dat je:

- Onnodige kosten veroorzaakt
- Leveranciers verliest
- Je eigen supply chain onder druk zet

Slimme cybersecurity begint met **realistische keuzes**, niet met de zwaarst mogelijke eis.