



19 mei 2025

Richtlijn Network and Information Security 2

Wat betekent dat voor jou?

CROP

Richtlijn NIS2

Medio oktober van 2025 wordt de nieuwe regelgeving rondom het ‘Network and Information Security Directive (NIS2)’ opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Deze richtlijn heeft directe gevolgen voor een groot deel van ondernemingen en organisaties in Nederland die een belangrijke of essentiële rol spelen in onze vitale infrastructuur. Waar de oorspronkelijke NIS-richtlijn vooral gold voor een beperkt aantal branches in de vitale infrastructuur, breidt NIS2 het toepassingsgebied flink uit. In dit document leggen we uit wat deze NIS2 richtlijn inhoudt, wat dit voor jou betekent en hoe wij je kunnen helpen je voor te bereiden op de inwerkingtreding.

Wat is NIS2?

NIS2 is Europese wetgeving gericht op het verhogen van de digitale weerbaarheid van essentiële en belangrijke organisaties. Organisaties die onder NIS2 vallen, worden verplicht om maatregelen te nemen op het gebied van informatiebeveiliging, risicobeheer en incidentrespons.

Wat betekent dit voor jouw organisatie?

Als jouw organisatie binnen een bepaalde sector of omvang valt (bijv. IT-dienstverlening, productie, gezondheidszorg, transport, digitale infrastructuur, energie, drinkwater, overheid of financiële dienstverlening), dan moet je mogelijk aan NIS2 voldoen. Dit betekent o.a.:

- Verplichte risicobeoordelingen en technische en organisatorische beveiligingsmaatregelen;
- Aantoonbare naleving en documentatie;
- Meldplicht van ernstige beveiligingsincidenten binnen 24 uur;
- Aansprakelijkheid en sancties bij niet-naleving.

Om te controleren of je moet voldoen kun je de NIS2 zelfevaluatie invullen via <https://regelhulpenvoorbedrijven.nl/NIS-2-NL/>, of contact met ons opnemen om samen te kijken of, en in welke mate, deze richtlijn impact zal hebben op jouw organisatie.

Hoe pakken wij dit aan?

Wij helpen je grip te krijgen op de impact van NIS2 en bieden begeleiding op maat:

- **Workshop risicobeoordeling:** In interactieve sessies brengen we samen de belangrijkste risico's voor jouw organisatie in kaart en leggen we de link met de eisen uit NIS2.
- **0-meting / Gap-analyse:** We stellen vast waar jouw organisatie nu staat ten opzichte van de NIS2-vereisten. We maken samen inzichtelijk welke stappen nog nodig zijn om NIS2 compliant te zijn en we ondersteunen bij het compliant worden.

- **Geïntegreerde frameworks (NIS2 – ISO 27001 – SOC - ISAE¹)** : ben je al bezig met ISO 27001, ISAE en/of SOC ? Wij helpen je NIS2 in deze kaders slim te integreren, zodat jij efficiënter kunt voldoen aan meerdere wet- en regelgevingen tegelijk. We hanteren een zogeheten ‘one framework to comply all’ aanpak; slechts één stelsel van interne beheersingsmaatregelen en één auditor die meerdere frameworks simultaan controleert.

Wat levert dit jou op?

- **Grip op NIS2 zonder overbelasting** : Wij vertalen complexe wetgeving naar concrete acties, afgestemd op jouw organisatie.
- **Pragmatisch stappenplan** : Je krijgt een helder en uitvoerbaar plan met prioriteiten op basis van risico's en impact.
- **Efficiëntie door integratie** : Slimme koppeling met ISO 27001, ISAE en SOC voorkomt dubbel werk en versnelt naleving.
- **Versterkte concurrentiepositie** : Aantoonbare informatiebeveiliging versterkt het vertrouwen van jouw klanten, leveranciers en toezichhouders.
- **Totaalpakket vanuit één vertrouwde partner** : Als onderdeel van een accountantsorganisatie bieden wij meer dan alleen IT advies; van ISO certificering, ISAE/SOC assurance als dan niet in combinatie met jaarrekeningcontroles. Wij zijn een totaal dienstverlener en hebben alles onder één dak beschikbaar!

Wat is de volgende stap?

Heb je vragen over de NIS2 in het algemeen, ben je geïnteresseerd in hoe wij jouw organisatie NIS2 compliant kunnen maken, of wil je meer weten over andere diensten die CROP IT audit & services verricht? Neem dan vandaag nog contact met ons op of stuur een e-mail naar pmo@crop.nl voor een vrijblijvende kennismaking. Onze experts, Jack van Crooij en Sandor Kemper, maken graag kennis met je! In de bijlage geven we een inkijk in onze andere diensten.



Jack van Crooij

Director IT-Audit
pmo@crop.nl
088 - 426 30 75



Sandor Kemper

Director IT-audit
pmo@crop.nl
088 - 426 31 81

¹ Indien u DORA toepast, is NIS2 meestal niet van toepassing.

CROP IT-audit & services!

Wij staan met een team van 20 enthousiaste IT-auditors en data specialisten graag voor je klaar!

IT audit

Ons IT audit team ondersteunt accountants en hun controleteams bij de jaarrekeningcontrole als het gaat om de vraag welke ICT-risico's van belang zijn in het kader van de jaarrekeningcontrole en hoe de accountant hiermee rekening moet houden bij zijn/haar werkzaamheden. Maar daarnaast doen we veel meer.

IT services

Ons team Data-analytics (D&A) is gespecialiseerd in het ontsluiten en valideren van data in allerlei systemen als basis voor 'visuals' als een PowerBI. Zij maken enerzijds dashboards ten behoeve van de jaarrekeningcontrole op basis van audit files uit jouw financiële administratie en de koppeling met de gecontroleerde bankdata die partner IBANXS (onder vergunning van de Nederlandsche Bank) ons levert via een beveiligde API. Maar, misschien ook goed om te weten, ons team D&A maakt ook dashboards ten behoeve van management informatie. Zij vervangen handmatig opgestelde management informatie door volledig geautomatiseerde oplossingen.

Smart Auditing

Uiteraard is een IT-onderzoek in het kader van de jaarrekeningcontrole maar een klein deel van ons werk. Wij geven u ook graag assurance op basis van SOC (1, 2 en 3), ISAE 3000 (A of D) en ISAE 3402. Ook kunnen we ISO 27001 certificeren samen met onze partner. Ook combineren we deze opdrachten graag met elkaar. We hanteren een 'one framework to comply all' principe. We noemen dat **Smart Auditing**. Het uitgangspunt is dat we een beheersingsmaatregel in principe maar een keer testen voor meerdere inclusief de jaarrekeningcontrole. Je hebt maar een auditor nodig voor een efficiënt en effectief controleproces. Dit bespaart tijd en geld.

DORA

CROP IT audit & services heeft ook kennis van de Digital Operational Resilience Act (DORA) die geldt voor financiële instellingen. Ben je een financiële instelling, of wordt jou door een financiële instelling gevraagd naar compliance met DORA, neem dan contact met ons op. We hebben een apart document beschikbaar en we kunnen je ondersteunen bij specifieke vraagstellingen met betrekking tot DORA.