NIS2-compliance-checklist

Achtentwintig punten om na te gaan of u de Belgische NIS2-wet naleeft: toepassingsgebied, registratie, governance, de tien risicobeheersmaatregelen, incidentmelding en bewijzen.

NIS2 Aware · nis2aware.eu · november 2026

1. Toepassingsgebied en registratie

- [ ] **Ga na of uw organisatie onder NIS2 valt**
  Controleer uw sector (bijlage I of II) en uw omvang (50 of meer werknemers, of meer dan 10 miljoen euro omzet en balanstotaal), partner- en verbonden ondernemingen inbegrepen. Documenteer de analyse.
- [ ] **Bepaal uw categorie: essentieel of belangrijk**
  Grote organisaties in sectoren met een hoge kriticiteit zijn doorgaans essentieel; de andere organisaties die onder de wet vallen, zijn doorgaans belangrijk. Uw toezichtsregime hangt ervan af.
- [ ] **Registreer u via Safeonweb@Work**
  Registratie bij het CCB is verplicht. Houd de contactgegevens van uw vertegenwoordigers actueel.
- [ ] **Ga na of een sectorale overheid of andere regels van toepassing zijn**
  Sommige sectoren hebben naast het CCB een sectorale overheid. Financiële entiteiten vallen voor ICT-risico vooral onder DORA.

2. Governance

- [ ] **Het bestuursorgaan heeft de cyberbeveiligingsmaatregelen goedgekeurd**
  Leg de goedkeuring vast in de notulen van een bestuursvergadering.
- [ ] **Het bestuursorgaan ziet toe op de uitvoering**
  Voorzie een regelmatige rapportering (bijvoorbeeld per kwartaal) met enkele duidelijke indicatoren.
- [ ] **De leden van het bestuursorgaan hebben een opleiding gevolgd**
  Dit is een wettelijke verplichting. Bewaar de aanwezigheidslijsten en plan opfrissingen.
- [ ] **Iemand is verantwoordelijk voor cyberbeveiliging**
  Wijs een verantwoordelijke aan (intern of extern) met tijd, zeggenschap en een vervanger.

- [ ] **Een budget en een roadmap voor 12 maanden zijn goedgekeurd**
  Leg een doel vast, zoals een zekerheidsniveau van CyberFundamentals, en de middelen om het te halen.

3. Risicobeheersmaatregelen

De tien domeinen die de wet minimaal oplegt, volgens een “alle risico's”-benadering.

- [ ] **Risicoanalyse en beveiligingsbeleid voor informatiesystemen**
  Breng uw kritieke activa en risico's in kaart, en keur een beveiligingsbeleid goed dat erop gebaseerd is.
- [ ] **Incidentenbehandeling**
  Incidenten opsporen, analyseren, indammen en ervan herstellen, met vastgelegde rollen.
- [ ] **Bedrijfscontinuïteit: back-ups, herstel na een ramp, crisisbeheer**
  Bewaar minstens één back-up offline of onveranderbaar, test het herstel en schrijf een crisisplan.
- [ ] **Beveiliging van de toeleveringsketen**
  Breng de kritieke leveranciers in kaart en leg beveiligingseisen vast in de contracten.
- [ ] **Beveiliging bij aankoop, ontwikkeling en onderhoud, inclusief de behandeling van kwetsbaarheden**
  Installeer patches binnen vastgelegde termijnen, scan op kwetsbaarheden en behandel meldingen van kwetsbaarheden.
- [ ] **Beoordeling van de doeltreffendheid van de maatregelen**
  Gebruik audits, tests en indicatoren om na te gaan of de maatregelen werken.
- [ ] **Basispraktijken voor cyberhygiëne en opleiding in cyberbeveiliging**
  Leid al het personeel minstens één keer per jaar op: phishing, wachtwoorden, melden.
- [ ] **Cryptografie en versleuteling**
  Versleutel laptops, gevoelige gegevens en communicatie, en beheer de sleutels correct.
- [ ] **Beveiliging van personeel, toegangsbeheer en beheer van activa**
  Houd een inventaris van activa bij, geef alleen de nodige rechten en beheer instroom, doorstroom en uitstroom.
- [ ] **Multifactorauthenticatie en beveiligde communicatie**
  MFA op e-mail, toegang op afstand, cloud en beheerdersaccounts; beveiligde spraak-, video-, tekst- en noodcommunicatie.

4. Incidentmelding

- [ ] **De criteria voor een significant incident zijn vastgelegd**
  Ernstige operationele verstoring, financieel verlies of aanzienlijke schade aan anderen.

- [ ] **De procedure 24 uur / 72 uur / één maand staat op papier**
  Wie beslist, wie meldt aan het CCB, met welke informatie. Bewaar een kopie offline.
- [ ] **De meldingskanalen en contactpersonen zijn gekend en getest**
  Weet hoe u een melding doet bij het CCB en houd de contactlijst van het crisisteam actueel.
- [ ] **U weet wanneer u de afnemers van uw diensten moet inlichten**
  Bereid berichten voor om klanten in te lichten die door een significant incident getroffen zijn.
- [ ] **Incidenten worden geregistreerd en er worden lessen uit getrokken**
  Houd een incidentenregister bij en werk uw risicoanalyse bij na elk incident.

5. Bewijzen en conformiteit

- [ ] **Er is een referentiekader gekozen**
  CyberFundamentals (Basic, Important, Essential) of ISO/IEC 27001.
- [ ] **Er is een lacuneanalyse gemaakt en een doelniveau vastgelegd**
  Meet waar u staat ten opzichte van het kader en plan de verbeteringen.
- [ ] **Essentiële entiteiten: de conformiteitsbeoordeling is gepland**
  Plan de verificatie of certificering met een geaccrediteerde instantie en ga na welke termijnen van het CCB voor u gelden.
- [ ] **Bewijzen worden bewaard en geordend**
  Notulen van het bestuur, beleid, opleidingslijsten, test- en auditrapporten, incidentenregister.

> **Een checklist is geen compliance.** NIS2 vraagt een risicogebaseerde aanpak die u actueel houdt. Gebruik deze lijst om het werk te structureren, niet om eenmalig vakjes aan te vinken.

Algemene informatie over het Belgische NIS2-kader op datum van november 2026, geen juridisch advies. Raadpleeg altijd de meest recente informatie van het CCB (ccb.belgium.be en atwork.safeonweb.be).