NIS2-zelfevaluatie-checklist-2026

# NIS2 Zelfevaluatie Checklist 2026

**voor kritieke dienstverleners en essentiële dienstverleners**

Versie 1.0 | April 2026

---

## Inleiding

Deze zelfevaluatie checklist helpt uw organisatie aan de hand van concrete vragen te bepalen in hoeverre u aan de zorgplichteisen van de NIS2-richtlijn voldoet. NIS2 (Richtlijn 2022/2555/EU) verplicht kritieke en essentiële dienstverleners cyberbeveiliging aanzienlijk uit te breiden.

De checklist is gegroepeerd naar zorgplichtthema's, elk met specifieke controlevragen. Markeer per vraag: - [ ] **Niet geïmplementeerd** — geen maatregelen - [~] **Gedeeltelijk geïmplementeerd** — basale/onvolledig - [ ] **Volledig geïmplementeerd** — volledig en getest

Gebruik deze checklist voor interne risk assessments en voorbereiding op naleving.

---

## 1. Governance & Bestuur

### Cyberbeveiliging in directie & bestuur

- ☐ Heeft de raad van bestuur/MT cyberbeveiliging als strategisch agendapunt?
- ☐ Is er een benoemd CISO of cyberbeveiliging-verantwoordelijke met management-status?
- ☐ Zijn rollen en verantwoordelijkheden voor cyberbeveiliging schriftelijk vastgelegd?
- ☐ Heeft de organisatie een gedocumenteerde cyberbeveiliging-strategie voor 2-3 jaar?
- ☐ Worden cyber-risico's minimaal jaarlijks gereviewd door de directie?

### Beleid en procedures

- ☐ Exist schriftelijke cybersecurity-beleidslijnen (minimum 10 pagina's)?
- ☐ Is er een incident response plan gepubliceerd en geoefend?
- ☐ Zijn er duidelijke beveiligingsrichtlijnen voor medewerkers?
- ☐ Worden beleidslijnen minimaal jaarlijks gereviewed en bijgewerkt?
- ☐ Is er een compliance/audit trail beschikbaar voor naleving?

---

## 2. Risicomanagement

### Identificatie en analyse

- ☐ Voert uw organisatie jaarlijks een cyber-risk assessment uit?
- ☐ Zijn cyberrisico's gemapt naar bedrijfskritieke processen?
- ☐ Zijn risico's ingedeeld naar waarschijnlijkheid en impact?
- ☐ Zijn derde partijen (leveranciers) in de risicoanalyse opgenomen?
- ☐ Zijn risk tolerance-grenzen formeel vastgesteld?

### Beheersmaatregelen

- ☐ Zijn er maatregelen geïmplementeerd voor top-3 risico's?
- ☐ Is er een vastleggingsplan voor restrisico's?
- ☐ Worden beheersmaatregelen regelmatig getest op effectiviteit?
- ☐ Is er een risicokader dat aan NIS2 voldoet?

---

## 3. Incidentbeheer & Crisis

### Preparatie

- ☐ Is er een gedetailleerd incident response plan (minimaal 15 pagina's)?
- ☐ Zijn rollen en contactgegevens voor crises gedocumenteerd?
- ☐ Zijn communicatiekanalen voor incidenten vooraf bepaald?
- ☐ Bestaan er out-of-office procedures voor kritieke rollen?

### Reactie

- ☐ Kunnen incidenten binnen 4 uur worden gerapporteerd aan relevante teams?
- ☐ Is er een procedure om betrokken partijen (klanten, autoriteiten) in te lichten?
- ☐ Worden incidenten gelogd met timestamp en severity-level?
- ☐ Is er een postmortem-proces voor analyse na incidenten?

### Testing

- ☐ Wordt het incident response plan minimaal 1x per jaar geoefend?
- ☐ Zijn tabletop-oefeningen met Management/directie uitgevoerd?
- ☐ Zijn realistische cyberincident-scenario's doorgespeeld?

---

## 4. Bedrijfscontinuïteit & Herstel

### Continuïteitplanning

- ☐ Bestaan business continuity plans (BCP) voor kritieke diensten?
- ☐ Is er een Disaster Recovery Plan (DRP) met Recovery Time Objectives (RTO)?
- ☐ Zijn Recovery Point Objectives (RPO) voor gegevens bepaald?
- ☐ Zijn kritieke IT-systemen geïdentificeerd?

### Backup & Redundantie

- ☐ Worden gegevens minimaal dagelijks gebackupd?
- ☐ Zijn backups gescheiden van productieomgevingen?
- ☐ Worden backups regelmatig getest op herstelbaarheid?
- ☐ Bestaat geografische redundantie voor kritieke systemen?

### Testing

- ☐ Is het DRP minimaal 1x per jaar getest?
- ☐ Kunnen kritieke services binnen 24-48 uur worden hersteld?
- ☐ Zijn failover-procedures gedocumenteerd en geoefend?

---

## 5. Toegangsbeheer & Authenticatie

### Identiteit en Authenticatie

- ☐ Wordt multi-factor authenticatie (MFA) voor alle kritieke systemen gecontroleerd?
- ☐ Zijn sterke wachtwoordvereisten geïmplementeerd (minimaal 12 karakters)?
- ☐ Is er een Single Sign-On (SSO) oplossing voor kritieke systemen?
- ☐ Worden wachtwoorden minstens elke 90 dagen gewijzigd?
- ☐ Zijn standaard/factory-accounts verwijderd of uitgeschakeld?

### Toegangsrechten

- ☐ Worden toegangsrechten gebaseerd op rollen (RBAC)?
- ☐ Worden kritieke administratieve accounts gemonitord?

☐ Worden afgestoten medewerkers onmiddellijk verwijderd?
☐ Bestaat een procedure voor bevoegdheidsevaluatie (minimaal jaarlijks)?
☐ Zijn beheerderaccount-activiteiten gelogd en gemonitord?

---

## 6. Cryptografie

### Encryptie & Sleutelbeheer

☐ Worden gevoelige data in transit versleuteld (TLS 1.3 of hoger)?
☐ Worden gevoelige data at rest versleuteld (AES-256 of gelijk)?
☐ Is er een Key Management System (KMS) geïmplementeerd?
☐ Worden cryptografische sleutels veilig opgeslagen (Hardware Security Module)?
☐ Bestaan procedures voor sleutelrotatie en vernietiging?

### Certificaten

☐ Worden SSL/TLS-certificaten minimaal jaarlijks vernieuwd?
☐ Is er een automatische monitoring voor vervallende certificaten?
☐ Worden certificaten van vertrouwde CA's gebruikt?

---

## 7. Operationele Beveiliging

### Monitoring & Logging

☐ Bestaan centraliseerde logging-systemen voor alle kritieke systemen?
☐ Worden logs minimaal 1 jaar bewaard?
☐ Zijn er alerts ingericht voor verdachte activiteiten?
☐ Worden logs regelmatig (minimaal maandelijks) gereviewd?
☐ Zijn logverwerkingssystemen gerepliceerd/beveiligd?

### Patch Management

☐ Is er een vastgesteld schema voor security patches (maximaal 30 dagen)?
☐ Worden patches getest voordat ze in productie gaan?
☐ Zijn End-of-Life producten geïnventariseerd en vervangen?
☐ Wordt het patchstatus minimaal maandelijks gerapporteerd?

### Malware & Antivirus

☐ Zijn alle werkstations uitgerust met actuele malwarebescherming?
☐ Is er centraliseerde antivirus-monitoring?
☐ Worden virus-definities minstens dagelijks bijgewerkt?

---

## 8. Toeleveringsketen & Externe Leveranciers

### Identificatie en Assessment

- ☐ Zijn kritieke leveranciers geïdentificeerd en gedocumenteerd?
- ☐ Worden leveranciers gescreend op cybersecurity-capaciteit?
- ☐ Zijn er SLA's vastgesteld voor security-performance?
- ☐ Worden leveranciers minimaal jaarlijks herbeoordeeld?

### Contracten en Monitoring

- ☐ Bevatten leverancierscontracten cyberbeveiliging-clausules?
- ☐ Zijn audit/inspectierechten contractueel vastgelegd?
- ☐ Worden leveranciers monitord op security-incidenten?
- ☐ Bestaan breakup-procedures voor kritieke leveranciers?

### Subcontractoren

- ☐ Worden subcontractoren van kritieke leveranciers gescreend?
- ☐ Zijn dataverwerking-overeenkomsten (DPA's) gesloten?
- ☐ Worden subcontractoren in cybersecurity-trainingen meegenomen?

---

## 9. Gegevensbescherming & Privacy (AVG/GDPR)

### Data Governance

- ☐ Is er een dataclassificatiesysteem (public/internal/confidential)?
- ☐ Zijn persoonlijke gegevensstromen gedocumenteerd?
- ☐ Bestaan procedures voor dataminimalisatie en opschooning?
- ☐ Is er een Data Protection Officer (DPO) benoemd?

### DPIA & Compliance

- ☐ Worden Data Protection Impact Assessments (DPIA's) voor grote verwerking uitgevoerd?
- ☐ Zijn gegevensverwerking-contracten (DPA's) met alle partijen gesloten?
- ☐ Worden gegevenslek-notificaties volgens AVG-timeframes (72 uur) afgehandeld?
- ☐ Zijn er procedures voor betrokkenenwensen (inzage, verwijdering)?

---

## 10. Fysieke Beveiliging

### Toegang & Controle

- ☐ Zijn kritieke serverruimtes met beveiligingscamera's gecontroleerd?
- ☐ Wordt fysieke toegang aan serverruimtes gelogd?

☐ Zijn ongebruikte fysieke poorten en connectors beschermd/uitgeschakeld?
☐ Bestaan procedures voor bezoekersbegeleiding in sensitieve zones?

**Hardware & Apparaten**

☐ Worden afgewerkte apparaten beveiligd gewist (NIST-standaard)?
☐ Zijn draagbare apparaten (laptops) versleuteld?
☐ Bestaan procedures voor lost & found voor IT-apparaten?
☐ Zijn privacy-schermen op werkstations in sensitieve rollen geïnstalleerd?

---

## 11. Personeels- & Bewustzijnstraining

**Training & Competentie**

☐ Volgen alle medewerkers jaarlijkse cybersecurity-training (minimaal 2 uur)?
☐ Is er gerichte training voor IT/administratief personeel?
☐ Worden nieuwe medewerkers binnen 1 maand getraind?
☐ Is er specifieke training voor Management/directie?

**Bewustzijn & Cultuur**

☐ Zijn er phishing-simulaties uitgevoerd (minimaal 2x per jaar)?
☐ Wordt cybersecurity regelmatig in interne communicatie besproken?
☐ Bestaat een geheimhoudingsbeleid en niet-medewerking-overeenkomsten?
☐ Is er een procedure voor security-waarschuwingen?

**Veiligheidsgedrag**

☐ Worden medewerkers afgewezen die security-trainingen niet voltooien?
☐ Bestaat een disciplinair kader voor security-overtredingen?
☐ Is er een whistleblower-procedure voor security-problemen?

---

## 12. Audit & Compliance Monitoring

**Interne Controles**

☐ Worden cybersecurity-maatregelen minimaal jaarlijks intern geaudit?
☐ Bestaan checklists voor naleving van NIS2-eisen?
☐ Worden audit-bevindingen vastgelegd en opgelost?
☐ Is er een board-reportage over audit-resultaten?

**Externe Audits**

☐ Zijn externe ISO 27001 of equivalent certificeringen bereikt?

☐ Worden penetration tests minimaal jaarlijks door derden uitgevoerd?
☐ Worden vulnerability assessments regelmatig (minimaal halfjaarlijks) gedaan?
☐ Zijn audit-bevindingen aan belanghebbenden gerapporteerd?

**Documentatie**

☐ Wordt een cybersecurity-registratie bijgehouden met alle maatregelen?
☐ Is er een evidence-biblioteca met proof-of-implementation?
☐ Worden beleid en procedures versioned en gearchiveerd?

---

## Evaluatie & Volgende Stappen

Na invulling van deze checklist:

1. **Tally** — Tel het aantal  , ~, en blanco antwoorden per sectie
2. **Score** — Bereken percentage: (  + 0.5×~) / totaal × 100%
3. **Gap Analysis** — Identificeer top-3 ontbrekende maatregelen
4. **Prioriteit** — Focus eerst op governance, risico, en incidentbeheer
5. **Timeline** — Stel implementatieplan op (beginjaar:  governance; jaar 2: operationeel)
6. **Rollen** — Wijs eigenaren aan per maatregel
7. **Budget** — Schat kosten voor tooling, training, consultancy
8. **Review** — Plan kwartaallijkse voortgangskijkingen

---

## Aanbevolen Structuur voor Implementatie (18-36 maanden)

| Kwartaal | Governance | Risico | Incident | Operationeel | Externe |
|---|---|---|---|---|---|
| Q1-Q2 | Beleidslijnen; CISO-rol | Risk framework | IR plan draft | Logging-setup | Leverancier-assessment |
| Q3-Q4 | Training; Audit-setup | Risk assess-ment; Tools | IR-testing | Patch-schema; MFA | Contracten |
| Q5-Q6 | Directie-alignment | Tools; Ownership | Tabletop-oefening | Antivirus; Monitoring | Audits |
| Q7+ | Jaarlijkse reviews | Quarterly updates | Annual test | Continuous | Annual reviews |

---

## Contactgegevens

Voor vragen over NIS2-naleving: - **iso2700x.nl** — Cyberbeveiliging consultancy - Email: info@iso2700x.nl - Website: https://iso2700x.nl

*Deze checklist is geen juridisch advies. Raadpleeg uw juridisch adviseur voor specifieke compliance-vragen.*

---

**Versiegeschiedenis** - v1.0 (April 2026): Initiële release voor NIS2 2024-naleving