Let’s Audit!

Gerben de Ruiter, lead auditor

10 februari 2026

kiwa

Let’s audit!

Multi-site organisaties

- Kenmerken
- Toetsing

Meerdere certificaten

Voorbeeld: ISO27001 en NIS2

Jullie uitdagingen?

Multi-site organisaties

Eén centrale functie waar activiteiten worden gepland en gecontroleerd.

+

locatie(s) waar de activiteiten worden uitgevoerd

Voorbeelden:

- Ziekenhuis met locaties en posten
- Holding met meerdere BV’s

Kenmerken multi-site organisaties

- Eén managementsysteem
- Centrale aansturing (mag niet uitbesteed)
- Centraal selecteren, opzetten en beoordelen van het systeem
- Alle locaties volgen interne assessment-programma
- Centraal verantwoordelijk voor PDCA + eventuele maatregelen, bijvoorbeeld:
  - Documentatie
  - Klachten
  - Planning en evaluatie

Let op! Een tekortkoming werkt op alle locaties door.

Toetsing multi-site organisaties

Toetsing van de locatie als:

- Zeer vergelijkbare activiteiten
- Meerdere sets van vergelijkbare activiteiten

Steekproef (bezoek):

Initieel : 1 + √(aantal sites)

Opvolging: 1 + 0,6 x √(aantal sites)

Her : 1 + 0,8 x √(aantal sites)

Meerdere certificaten

Voorbeelden

- ISO27001 en HKZ
- ISO9001 en ISO42001
- NEN7510:2017 en ISO27001:202
- ISO27001 en NIS2

Meerdere certificaten

Gecombineerde audit

- Afzonderlijke audits, zoveel als mogelijk op elkaar afgestemd
- Overeenkomsten in Harmonized Stucture (H4t/m H10)
- Auditduur is o.b.v. accreditatiestandaarden

Geïntegreerde audit

- Overlap in Harmonized Structure (H4 /tm H10) = Zelfde basisstructuur
- Auditor (of auditteam) moet kwalificaties, expertise en ervaring beschikken.
- Verkorte auditduur, mits schema onder accreditatie vallen
- Eén rapport

Meerdere certificaten

Voorbeelden

- ISO27001 en HKZ - gecombineerd
- ISO9001 en ISO42001 - geïntegreerd
- NEN7510:2017 en ISO27001:2022 – geïntegreerd (Verschil in versies speelt geen rol)
- ISO27001 en NIS2 - gecombineerd

Voorbeeld: Combinatie van ISO27001 en NIS2

- Beiden een managementsysteem, gericht op informatiebeveiliging en risicobeheer
- Het CSMS/ISMS vormt de kern van de cyberbeveiliging van uw organisatie
- Het biedt structuur, beleid, processen en technologieën om voorbereid te zijn op cyberdreigingen
- Veel gelijksoortige maatregelen

Dit kan niet geïntegreerd, wel gecombineerd.

NIS2 en ISO27001 vergelijking

Aspect	ISO27001	NIS2
Juridische status	Vrijwillige internationale norm (certificering via audit)	Europese wetgeving → verplicht voor organisaties in kritieke sectoren (keurmerk mogelijk)
Scope	Brede toepasbaarheid (elk type organisatie kan certificeren)	Gericht op essentiële en belangrijke entiteiten (bv. energie, zorg, transport, digitale diensten)
Focus	ISMS (Information Security Management System): procesmatig, continu verbeteren	Minimale wettelijke eisen: 4 hoofdverplichtingen + 10 zorgplichtmaatregelen
Toezicht & boetes	Geen boetes, enkel verlies van certificaat bij auditfalen	Strenge boetes en toezicht door toezichthouders
Governance	Management commitment vereist, maar zonder juridische aansprakelijkheid	Bestuur/management persoonlijk aansprakelijk bij non-compliance
Rapportage	Geen wettelijke meldplicht, alleen interne opvolging	Verplichte incidentmelding binnen strikte termijnen
Supply Chain	Aanbevolen om leveranciers te beoordelen	Verplicht: uitgebreide aandacht voor keten- en leveranciersrisico's
Continuïteit & herstel	Business Continuity Management aanbevolen maar optioneel	Expliciete verplichting in wetgeving

ISO 27001 als bewijslast voor NIS2

NIS2 schrijft niet exact **hoe** je moet voldoen, alleen **dat** je bepaalde beveiligingsmaatregelen en processen moet hebben.

ISO 27001 geeft een gestructureerd **ISMS** (Information Security Management System) waarmee je kunt laten zien dat je de zorgplicht en meldplicht systematisch hebt ingebouwd.

Daarmee kan ISO 27001 dienen als **compliance framework** richting toezichthouders.

Veel van de 10 zorgplichtdomeinen van NIS2 **overlappen** met controls in ISO 27001 en de bijbehorende Annex A (2022 versie).

- Risicoanalyse → ISO 27005 / ISMS verplichting
- Incidentmanagement → A.5.24~A5.28
- Continuïteit & back-ups → A.5.30 & A8.13 Supply chain security → A.5.15~A.5.19
- Training & awareness → $7.3, A.6.3
- Door te laten zien dat ISO 27001 al veel afdekt, positioneer je de norm als praktische routekaart voor NIS2

Uitdagingen

- Aanpak in certificeren: Bottom-up of top-down
- Tijdlijnen van controle operationele processen
- Internationaal? Wetgeving, Inzet van technical expert

Welke uitdaging hebben jullie?

Dank!

Kiwa.com