GIDS

De complete gids voor de ISO 27001 externe audit

Kosten, auditproces, certificerende instellingen, NIS2-verband en veelgemaakte fouten. Met actuele Nederlandse marktdata.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

ISO 27001 certificering groeit wereldwijd explosief. In Nederland is het nog een klein percentage, maar de komst van NIS2 verandert dat snel.

~1.200
Geschat aantal ISO 27001 certificaten in Nederland
NormSupport [1]

<0,5%
van alle Nederlandse bedrijven is ISO 27001 gecertificeerd
NormSupport [1]

+99%
Wereldwijde groei ISO 27001 certificaten in 2024 -- bijna verdubbeld
ISO Survey 2024 / HEIC [2]

EUR 5K--15K
Kosten initiële certificeringsaudit voor MKB in Nederland
DigiTrust / Diks Process Support [3][4]

3 jaar
Geldigheid van een ISO 27001 certificaat, met jaarlijkse surveillance
ISO 27001 norm [5]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- ~10.000 bedrijven
Digitale Overheid [6]

50--70%
Minder beveiligingsincidenten bij gecertificeerde organisaties
BSI [7]

3--9 mnd
Gemiddelde doorlooptijd ISO 27001 traject voor MKB
CertificeringsAdvies NL [8]

1. Wat is een ISO 27001 externe audit?

Een externe audit is de onafhankelijke beoordeling van jouw informatiebeveiliging door een geaccrediteerde certificerende instelling (CI). Het is de eindtoets die bepaalt of je een ISO 27001 certificaat krijgt.

Bij een externe audit beoordeelt een onafhankelijke auditor of jouw Information Security Management System (ISMS) voldoet aan de eisen van ISO 27001:2022. De auditor werkt voor een certificerende instelling die geaccrediteerd is door de Raad voor Accreditatie (RvA) [9].

De externe audit is iets fundamenteel anders dan een interne audit. Bij een interne audit controleer je jezelf (of laat je dat doen); bij een externe audit oordeelt een volledig onafhankelijke partij. De CI mag je geen advies geven -- alleen beoordelen [10].

> **Wanneer ben je klaar voor een externe audit?** Je ISMS moet minimaal 3 maanden operationeel zijn. Je hebt minimaal 1 interne audit en 1 management review uitgevoerd. Je risicoanalyse en Statement of Applicability (SoA) zijn actueel en compleet [11].

WIE VOERT DE AUDIT UIT?

De audit wordt uitgevoerd door een lead auditor van een RvA-geaccrediteerde CI. In Nederland zijn er circa 9 geaccrediteerde CI's voor ISO 27001, waaronder BSI, DNV, DEKRA, DigiTrust en Brand Compliance [9]. De auditor is opgeleid als ISO 27001 Lead Auditor (IRCA of PECB gecertificeerd) en heeft ervaring in jouw sector.

WAAROM EEN EXTERNE AUDIT?

- Je krijgt een internationaal erkend certificaat (via IAF MLA)
- Klanten, partners en aanbesteders vertrouwen een onafhankelijk oordeel
- Het is een bewijs van conformiteit richting de NIS2-toezichthouder
- Verzekeraars geven soms korting op cyberverzekeringen bij certificering

2. Stage 1 en Stage 2: het auditproces

De certificeringsaudit bestaat uit twee fasen: Stage 1 (documentatiebeoordeling) en Stage 2 (implementatie-audit). Tussen beide fasen zit maximaal 3 maanden.

STAGE 1: DOCUMENTATIE-AUDIT

In Stage 1 beoordeelt de auditor of jouw ISMS op papier compleet is en of je gereed bent voor de implementatiebeoordeling. Dit kan on-site of remote plaatsvinden en duurt doorgaans 1 tot 2 dagen [3].

WAT CONTROLEERT DE AUDITOR IN STAGE 1?

- ISMS-scope en context van de organisatie
- Informatiebeveiligingsbeleid en doelstellingen
- Risicoanalyse en risicobehandelplan
- Statement of Applicability (SoA)
- Resultaten van de interne audit
- Notulen van de management review
- Competentie en bewustzijn van medewerkers

Na Stage 1 krijg je een rapport met bevindingen. Als er tekortkomingen zijn, heb je tot maximaal 3 maanden de tijd om deze op te lossen voordat Stage 2 plaatsvindt [12].

STAGE 2: IMPLEMENTATIE-AUDIT

Stage 2 is de meest uitgebreide fase. De auditor komt on-site om te beoordelen of je ISMS in de praktijk werkt. Dit duurt 2 tot 5 dagen, afhankelijk van de grootte van je organisatie [3].

WAT GEBEURT ER TIJDENS STAGE 2?

- Interviews met medewerkers op verschillende niveaus
- Controle van technische beveiligingsmaatregelen
- Beoordeling of processen daadwerkelijk worden gevolgd
- Steekproeven van bewijsmateriaal en registraties
- Beoordeling van incidentregistraties en -afhandeling
- Controle of corrigerende acties uit de interne audit zijn uitgevoerd

MOGELIJKE UITKOMSTEN

UITKOMST	BETEKENIS	ACTIE
Certificaat	Je voldoet aan alle eisen	Certificaat wordt afgegeven (3 jaar geldig)
Minor non-conformiteiten	Kleine afwijkingen	Corrigerende acties binnen 90 dagen, certificaat wordt afgegeven
Major non-conformiteiten	Ernstige tekortkomingen	Her-audit nodig, certificaat wordt uitgesteld

TIP

Bereid een "evidence pack" voor met alle documenten die de auditor waarschijnlijk opvraagt: risicoanalyse, SoA, interne auditrapport, management review notulen, incidentregistratie, trainingsregistraties en toegangslogboeken.

3. Wat kost het?

De kosten van een ISO 27001 externe audit variëren van EUR 5.000 tot EUR 25.000+, afhankelijk van je organisatiegrootte en complexiteit.

KOSTEN INITIËLE CERTIFICERINGSAUDIT

BEDRIJFSGROOTTE	STAGE 1 + STAGE 2	DUUR (DAGEN)
Klein MKB (<25 mdw)	EUR 5.000 -- EUR 8.000	3--4 dagen
Middelgroot (25--100 mdw)	EUR 8.000 -- EUR 15.000	4--6 dagen
Groot (100--250 mdw)	EUR 12.000 -- EUR 20.000	5--8 dagen
Enterprise (250+ mdw)	EUR 18.000 -- EUR 25.000+	7--12 dagen

Bron: DigiTrust [3], Diks Process Support [4], CertificeringsAdvies NL [8]

KOSTENOPBOUW PER FASE

FASE	KOSTEN	DUUR
Stage 1 (documentbeoordeling)	EUR 1.500 -- EUR 3.500	1--2 dagen
Stage 2 (implementatie-audit)	EUR 3.000 -- EUR 8.000	2--5 dagen
Reiskosten auditor	EUR 200 -- EUR 500	--

JAARLIJKSE KOSTEN NA CERTIFICERING

KOSTENPOST	BEDRAG	FREQUENTIE
Surveillance-audit	EUR 1.200 -- EUR 8.000	Jaarlijks (jaar 2 en 3)
Hercertificering	EUR 6.000 -- EUR 15.000	Elke 3 jaar
ISMS-onderhoud (intern)	EUR 3.000 -- EUR 10.000	Jaarlijks

De surveillance-audit kost circa 30--50% van de initiële certificeringsaudit [4].

Kostenbesparend: Organisaties met bestaande ISO-certificeringen (bijv. ISO 9001) kunnen 30--50% besparen door combinatieaudits. Goede voorbereiding verlaagt de audit-doorlooptijd en daarmee de kosten [3].

4. De certificatiecyclus

Een ISO 27001 certificaat is 3 jaar geldig. In die 3 jaar doorloop je een vaste cyclus van audits.

1

Jaar 1: Certificeringsaudit

STAGE 1 + STAGE 2

Volledige beoordeling van je ISMS. Bij voldoende resultaat ontvang je het certificaat.

2

Jaar 2: Surveillance-audit

1--2 DAGEN

Steekproefsgewijze controle. De auditor kijkt of je het ISMS onderhoudt en verbetert. Niet alles wordt opnieuw beoordeeld.

3

Jaar 3: Surveillance-audit

1--2 DAGEN

Zelfde als jaar 2. Focus op wijzigingen, verbeteracties en resterende Annex A controls.

4

Jaar 4: Hercertificeringsaudit

STAGE 1 + STAGE 2 IN EEN

Volledige herbeoordeling. Vergelijkbaar met de initiële audit, maar met focus op de afgelopen 3 jaar.

LET OP

Als je een surveillance-audit mist of major non-conformiteiten niet oplost, kan je certificaat worden geschorst of ingetrokken. Plan surveillance-audits ruim van tevoren in.

5. Certificerende instellingen kiezen

De keuze voor een certificerende instelling (CI) bepaalt de kwaliteit van je audit-ervaring. Let op accreditatie, ervaring en tarieven.

RVA-ACCREDITATIE: NIET ONDERHANDELBAAR

De Raad voor Accreditatie (RvA) beoordeelt en accrediteert certificerende instellingen in Nederland. Een certificaat van een niet-geaccrediteerde CI wordt door veel klanten en aanbesteders niet geaccepteerd [9].

GEACCREDITEERDE CI'S IN NEDERLAND

CERTIFICERENDE INSTELLING	BIJZONDERHEDEN
BSI Group Nederland	Internationaal, ook NEN 7510
DNV Business Assurance	Internationaal, breed portfolio
Brand Compliance	Nederlands, ook NEN 7510 (RvA C548)
DigiTrust	Nederlands, informatiebeveiliging-specialist (RvA C618)
DEKRA Certification	Internationaal, ook NEN 7510
Kiwa Nederland	Nederlands, breed portfolio
TUV NORD	Internationaal
Duijnborgh Certification	Nederlands (RvA C590)
EBN Certification	Nederlands, onafhankelijk

Bron: RvA [9], ISO Register [13]

HOE KIES JE EEN CI?

- **Accreditatie** -- Is de CI RvA-geaccrediteerd voor ISO 27001? Dit is een harde eis.
- **Sectorervaring** -- Heeft de CI ervaring met jouw type organisatie?
- **Tarieven** -- Vergelijk minimaal 3 offertes. Tarieven variëren aanzienlijk.
- **Beschikbaarheid** -- Sommige CI's hebben wachttijden van weken tot maanden.
- **Communicatie** -- Hoe verloopt de rapportage? Is er een vast aanspreekpunt?

TIP

Op certificeerwijzer.nl vind je een actueel overzicht van geaccrediteerde CI's die ISO 27001 audits uitvoeren in Nederland. Dit helpt je bij het vergelijken op basis van ervaring, tarieven en sector.

BELANGRIJK

De consultant die je ISMS opbouwt, mag niet dezelfde partij zijn als de CI die certificeert. Dit is een accreditatieregel om belangenverstrengeling te voorkomen.

6. Waar kijkt de auditor naar?

Een auditor beoordeelt niet alleen je documentatie, maar vooral of je ISMS in de praktijk werkt. "Zeg wat je doet en doe wat je zegt" is het kernprincipe.

DOCUMENTATIE

- Informatiebeveiligingsbeleid en -doelstellingen
- Risicoanalyse en risicobehandelplan
- Statement of Applicability (SoA) -- welke Annex A controls zijn van toepassing en waarom (niet)
- Procedures voor incidentmanagement, toegangsbeheer, back-up, etc.
- Interne auditrapport en management review notulen

IMPLEMENTATIE

- Zijn medewerkers op de hoogte van het informatiebeveiligingsbeleid?
- Worden procedures daadwerkelijk gevolgd?
- Zijn technische maatregelen (MFA, encryptie, back-ups) geimplementeerd?
- Zijn incidenten geregistreerd en afgehandeld?
- Zijn corrigerende acties uit de interne audit uitgevoerd?

CONTINUE VERBETERING

ISO 27001 draait om continue verbetering. De auditor verwacht geen perfectie, maar wel bewijs dat je leert van incidenten, auditbevindingen en veranderende risico's [14].

TOP 5 DOCUMENTEN DIE DE AUDITOR ALTIJD OPVRAAGT

1. Risicoanalyse en risicobehandelplan
2. Statement of Applicability (SoA)
3. Interne auditrapport
4. Management review notulen
5. Incidentregistratie

7. Veelgemaakte fouten

Deze fouten zien auditors keer op keer. Herken ze en voorkom ze.

1 **Te veel documentatie die niemand naleeft**

Mooie procedures op papier maar geen bewijs van naleving. Auditors noemen dit een "papiertijger". Schrijf alleen beleid dat je daadwerkelijk uitvoert [15].

2 **Perfectie verwachten voor de audit**

ISO 27001 werkt met continue verbetering. Je hoeft niet met een 10 te starten -- een 6 is voldoende, zolang je kunt aantonen dat je verbetert [16].

3 **Gebrek aan managementbetrokkenheid**

Als het management alles delegeert naar de IT-afdeling, mist de organisatiebrede aanpak die ISO 27001 vereist. De auditor zal vragen naar de rol van de directie [17].

4 **Risicoanalyse te snel of te oppervlakkig**

De risicoanalyse is het fundament. Zonder gedegen analyse kun je niet onderbouwen waarom je bepaalde maatregelen wel of niet hebt genomen [18].

5 **Onvoldoende bewijs van implementatie**

Ontbrekende logbestanden, trainingsregistraties of incidentrapportages. Auditors willen bewijs zien -- niet alleen beleid [10].

6 **Interne audit niet goed uitgevoerd**

Een oppervlakkige of ontbrekende interne audit is een veelvoorkomende major non-conformiteit. De interne audit is verplicht en moet gedegen zijn [10].

7 **ISMS te kort operationeel**

Minimaal 3 maanden operationeel draaien is een harde eis. Te vroeg een audit aanvragen leidt tot uitstel of afwijzing [11].

MEEST VOORKOMENDE NON-CONFORMITEITEN

Geen risicobehandelplan of onduidelijke methodologie (major). Ontbreken van management review of interne audit (major). Verouderde documentatie of ontbrekende trainingsregistraties (minor) [19].

8. NIS2 en de Cyberbeveiligingswet

De Cyberbeveiligingswet (Nederlandse implementatie van NIS2) treedt naar verwachting in Q2 2026 in werking. Circa 10.000 Nederlandse organisaties vallen eronder.

WAT IS HET VERBAND MET ISO 27001?

ISO 27001 is niet verplicht onder NIS2, maar dekt een groot deel van de eisen. NIS2 definieert wat er geregeld moet worden; ISO 27001 definieert hoe [20]. Een ISO 27001 certificaat kan dienen als bewijs van conformiteit richting de toezichthouder.

WAT DEKT ISO 27001 WEL EN NIET?

NIS2-EIS	ISO 27001 DEKKING	AANVULLING NODIG?
Risicoanalyse	Volledig	Nee
Incidentmanagement	Deels	Ja -- meldplicht 24--72 uur
Ketenbeveiliging	Deels	Ja -- uitgebreidere analyse
Registratieplicht	Nee	Ja
Bestuurlijke aansprakelijkheid	Nee	Ja
Continuiteitsplanning	Volledig	Nee

> **Aanbeveling:** Start met ISO 27001 als fundament voor NIS2-compliance. Vul vervolgens de specifieke NIS2-gaps aan (meldplicht, registratie, bestuurlijke aansprakelijkheid). Dit voorkomt dubbel werk en geeft een gestructureerde aanpak [21].

9. Verschil met verwante diensten

De ISO 27001 externe audit wordt vaak verward met andere vormen van beoordeling. Hieronder de verschillen.

EXTERNE AUDIT VS. INTERNE AUDIT

ASPECT	EXTERNE AUDIT	INTERNE AUDIT
Uitgevoerd door	Geaccrediteerde CI	Eigen medewerker of ingehuurde specialist
Doel	Certificaat afgeven of behouden	ISMS controleren en verbeteren
Mag adviseren?	Nee	Ja
Kosten (MKB)	EUR 5.000 -- EUR 15.000	EUR 1.600 -- EUR 4.000
Frequentie	Jaarlijks + elke 3 jaar	Minimaal jaarlijks

EXTERNE AUDIT VS. IMPLEMENTATIEBEGELEIDING

ASPECT	EXTERNE AUDIT	IMPLEMENTATIEBEGELEIDING
Fase	Na implementatie	Tijdens implementatie
Rol	Beoordelaar	Adviseur
Resultaat	Certificaat of afwijkingen	Werkend ISMS
Kan door dezelfde partij?	Nee -- CI en consultant moeten gescheiden zijn	

ISO 27001 VS. SOC 2

ASPECT	ISO 27001	SOC 2
Type	Certificering tegen internationale norm	Attestation report door CPA
Geldigheid	3 jaar (met surveillance)	12 maanden
Erkenning	Wereldwijd (IAF MLA)	Vooral VS en SaaS

10. Volgende stappen

Klaar om een ISO 27001 externe audit aan te vragen? Volg dit stappenplan.

1. **Check je gereedheid**
   Is je ISMS minimaal 3 maanden operationeel? Heb je een interne audit en management review uitgevoerd? Is je risicoanalyse actueel?

2. **Vergelijk certificerende instellingen**
   Vraag minimaal 3 offertes aan bij RvA-geaccrediteerde CI's. Vergelijk op ervaring, tarief en beschikbaarheid. Gebruik certificeerwijzer.nl voor een actueel overzicht.

3. **Plan de audit**
   Plan Stage 1 en Stage 2 met maximaal 3 maanden ertussen. Zorg dat key stakeholders beschikbaar zijn voor interviews.

4. **Bereid je evidence pack voor**
   Verzamel alle documenten die de auditor waarschijnlijk opvraagt. Denk aan risicoanalyse, SoA, auditrapport, incidentregistratie en trainingsregistraties.

5. **Doorloop de audit met vertrouwen**
   Wees eerlijk en transparant. Toon bewijs van continue verbetering, niet van perfectie. Auditors waarderen openheid.

HULP NODIG BIJ HET KIEZEN?

Op ibgids.nl/word-gematcht vind je onafhankelijk advies en kun je je laten matchen met geschikte aanbieders voor een ISO 27001 externe audit.

Bronnenlijst

[1] **NormSupport** -- De uitdaging van ISO 27001 certificering voor Nederlandse bedrijven (normsupport.nl)

[2] **ISO Survey 2024 / HEIC** -- ISO 27001 certifications nearly double in 2024 (heic.eu)

[3] **DigiTrust** -- How much does an ISO 27001 audit cost (digitrust.nl)

[4] **Diks Process Support** -- Wat zijn de kosten van een ISO 27001-audit (diksprocesssupport.nl)

[5] **ISO/IEC 27001:2022** -- International standard for information security management

[6] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2-richtlijn) (digitaleoverheid.nl)

[7] **BSI Group** -- ISO/IEC 27001 voor het MKB (bsigroup.com)

[8] **CertificeringsAdvies NL** -- Hoelang duurt ISO 27001 certificering (certificeringsadvies.nl)

[9] **RvA** -- Geaccrediteerden overzicht (rva.nl)

[10] **CertificeringsAdvies NL** -- Hoe gaat een ISO 27001 audit in zijn werk (certificeringsadvies.nl)

[11] **Audit Direct** -- ISO 27001 certificering binnen 3 maanden (auditdirect.nl)

[12] **DigiTrust** -- Hoe werkt het ISO 27001 auditproces (digitrust.nl)

[13] **ISO Register** -- Overzicht certificatie instellingen (isoregister.nl)

[14] **Nieuwhuis Consult** -- ISO 27001 audit voorbereiden (nieuwhuisconsult.nl)

[15] **Fendix** -- Veelgemaakte fouten bij ISO 27001 implementatie (fendix.nl)

[16] **Equans** -- ISO 27001 certificering: voorkom deze 3 valkuilen (equans.nl)

[17] **Compleye** -- ISO 27001 certificering: veelvoorkomende valkuilen (compleye.io)

[18] **Normwijzer** -- Risicoanalyse voor ISO 27001 (normwijzer.nl)

[19] **Cyberday** -- 10 meest voorkomende non-conformiteiten bij ISO 27001 (cyberday.ai)

[20] **FidelSec** -- Het verschil tussen de Cyberbeveiligingswet (NIS2) en ISO 27001 (fidelsec.nl)

[21] **Kiwa** -- ISO 27001 and NIS2: Making Compliance Manageable (kiwa.com)