GIDS

De complete gids voor ISO 27001 implementatie

Kosten, doorlooptijd, het implementatieproces, een partner kiezen en NIS2-aansluiting. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De belangrijkste cijfers over ISO 27001 implementatie in Nederland.

EUR 15–40K
Totale implementatiekosten voor MKB (<50 medewerkers)
DigiTrust [1]

3–9 mnd
Doorlooptijd implementatie voor MKB met begeleiding
CertificeringsAdvies NL [2]

<0,5%
van alle Nederlandse bedrijven is ISO 27001 gecertificeerd
NormSupport [3]

96.709
ISO 27001 certificaten wereldwijd in 2024 (+99% groei)
ISO Survey 2024 / HEIC [4]

18–36 mnd
Break-even punt van de investering voor MKB
Nieuwhuis Consult [5]

3 jaar
Geldigheid van een ISO 27001 certificaat
DEKRA [6]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2)
Digitale Overheid [7]

100–200 uur
Interne tijdsinvestering voor MKB-organisaties
DigiTrust [1]

1. Wat is ISO 27001?

ISO 27001 is de internationale standaard voor informatiebeveiliging. De norm beschrijft hoe je een Information Security Management System (ISMS) opzet, implementeert, onderhoudt en continu verbetert.

Een ISMS is geen stuk software, maar een samenhangend set van beleid, procedures, technische maatregelen en gedragsregels. Het doel: de vertrouwelijkheid, integriteit en beschikbaarheid van informatie systematisch beschermen. Niet door alles dicht te timmeren, maar door bewuste keuzes te maken op basis van een risicoanalyse.

> **ISO 27001:2022 - de huidige versie**
>
> De meest recente versie dateert uit 2022. Annex A is geherstructureerd van 114 maatregelen in 14 categorieen naar 93 maatregelen in 4 thema's: organisatorisch, menselijk, fysiek en technologisch. Er zijn 11 nieuwe maatregelen toegevoegd, waaronder threat intelligence, cloud security en data masking.

KERNBEGRIPPEN

- **ISMS** - Information Security Management System: het geheel van processen, documenten en maatregelen
- **Annex A** - De 93 beveiligingsmaatregelen (controls) waaruit je kiest op basis van je risicoanalyse
- **Statement of Applicability (SoA)** - Document dat beschrijft welke controls je toepast en waarom
- **Risicobehandelplan** - Hoe je omgaat met geidentificeerde risico's: mitigeren, accepteren, overdragen of vermijden
- **RvA** - Raad voor Accreditatie, toezichthouder op certificerende instellingen in Nederland

ISO 27001 is formeel niet wettelijk verplicht als zelfstandige eis [8]. In de praktijk is het dat indirect wel: overheidsaanbestedingen, contractuele eisen van grote opdrachtgevers, sectorale regelgeving (BIO, NEN 7510) en de aankomende Cyberbeveiligingswet maken certificering steeds vaker een harde voorwaarde.

2. Waarom certificeren?

ISO 27001 certificering is een investering. Maar de voordelen reiken verder dan een certificaat aan de muur.

TOEGANG TOT MARKT EN AANBESTEDINGEN

Bij overheidsaanbestedingen is ISO 27001 vaak een harde eis of gunningscriterium [9]. Grote opdrachtgevers in finance en overheid eisen het van hun leveranciers. Zonder certificaat mis je opdrachten. Uit praktijkonderzoek blijkt dat organisaties na certificering toegang krijgen tot nieuwe klanten en aanbestedingen die eerder niet bereikbaar waren [5].

KLANTVERTROUWEN EN TRANSPARANTIE

Een ISO 27001 certificaat is aantoonbaar bewijs dat je informatiebeveiliging serieus neemt. Het is verifieerbaar via het certificaatregister en geeft opdrachtgevers zekerheid zonder dat zij zelf een audit hoeven uit te voeren [10].

CYBERVERZEKERING

Verzekeraars bieden korting op cyberverzekeringspremies bij ISO 27001 certificering [1]. MKB cyberverzekeringspremies starten vanaf EUR 1.500 per jaar voor basisdekking [11]. Sterke beveiligingsmaatregelen (MFA, backups, ISMS) verlagen de premie.

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet treedt naar verwachting in Q2 2026 in werking [7]. ISO 27001 vormt de beste basis voor compliance. Organisaties die al gecertificeerd zijn, hoeven slechts een beperkt aantal aanvullende stappen te zetten [12].

> **ROI in cijfers**
>
> Het break-even punt voor een MKB-organisatie (25 medewerkers) ligt tussen 18 en 36 maanden [5]. De investering verdient zich terug via nieuwe klanten, lagere verzekeringspremies, minder incidenten en compliance met regelgeving.

3. Het implementatieproces in 6 stappen

Van nulmeting tot certificaat: dit zijn de zes fasen van een ISO 27001 implementatie, met realistische doorlooptijden per fase.

1 Gap-analyse en voorbereiding

1-2 MAANDEN

Inventariseer je huidige situatie: welke beveiligingsmaatregelen heb je al? Waar zitten de gaten? Bepaal de scope van je ISMS en stel een projectplan op. Dit is het fundament voor alle volgende stappen [2].

2 Risicoanalyse

1-2 MAANDEN

Identificeer dreigingen en kwetsbaarheden, beoordeel de risico's en stel een risicobehandelplan op. De risicoanalyse is het hart van ISO 27001. Een oppervlakkige risicoanalyse ondermijnt het hele ISMS [13].

3 ISMS opbouwen en implementeren

2-4 MAANDEN

Schrijf beleid en procedures, implementeer technische en organisatorische maatregelen en train medewerkers. Kies maatregelen uit Annex A die passen bij jouw risicoanalyse en leg dit vast in de Statement of Applicability.

4 Operationele fase

MINIMAAL 3 MAANDEN

Je ISMS moet aantoonbaar operationeel zijn. Minimaal drie maanden draaien volgens het ISMS is een harde eis voor een succesvolle certificeringsaudit [14]. Documenteer incidenten, wijzigingen en metingen.

5 Interne audit en management review

1-2 MAANDEN

Voer een interne audit uit om te toetsen of het ISMS werkt zoals bedoeld. De directie beoordeelt de resultaten in een management review en besluit over corrigerende acties.

6 Certificeringsaudit

1-2 MAANDEN

De externe audit door een certificerende instelling, in twee fasen: Stage 1 (documentatiebeoordeling) en Stage 2 (implementatietoetsing). Bij positief resultaat ontvang je het certificaat, geldig voor drie jaar [6].

DOORLOOPTIJD PER BEDRIJFSGROOTTE

BEDRIJFSGROOTTE	DOORLOOPTIJD
Klein MKB (<50 medewerkers)	3-9 maanden [2]
Middelgroot (50–250 medewerkers)	6-12 maanden [15]
Zonder begeleiding	12-24 maanden [16]

Traditionele trajecten duren 9-12 maanden, vaak door inefficientie en niet door de daadwerkelijke werklast [14]. Een versneld traject is haalbaar mits er al een basis aan beveiliging bestaat, dedicated resources beschikbaar zijn en management commitment volledig is.

Naast de doorlooptijd in maanden kost het intern ook uren. Voor MKB-organisaties schat DigiTrust de interne tijdsinvestering op 100 tot 200 uur [1]. Bij een middelgroot bedrijf zijn 15 tot 30 consultancydagen gebruikelijk, gespreid over 6 tot 12 maanden [15].

> **BELANGRIJK: MINIMALE OPERATIONELE PERIODE**
> Je kunt niet in drie maanden van nul naar certificaat. Het ISMS moet minimaal drie maanden operationeel draaien voor de certificeringsaudit. Een versneld traject van 3 maanden totaal is alleen haalbaar als er al een redelijke basis aan beveiliging bestaat [14].

4. Wat kost het?

De totale kosten van ISO 27001 implementatie bestaan uit drie componenten: externe consultancy, de certificeringsaudit en interne kosten.

TOTAALKOSTEN PER BEDRIJFSGROOTTE

BEDRIJFSGROOTTE	TOTALE KOSTEN (INCL. CERTIFICERING)
Klein MKB (<50 medewerkers)	EUR 15.000 - EUR 40.000 [1]
Middelgroot (50–250 medewerkers)	EUR 30.000 - EUR 75.000 [15]

KOSTENOPBOUW

KOSTENPOST	BEDRAG
Dagtarief consultant	EUR 800 - EUR 1.500 per dag [17]
MKB totaalproject consultancy	EUR 5.000 - EUR 15.000 [1]
Certificeringsaudit (<10 FTE)	ca. EUR 6.000 [18]
Certificeringsaudit (middelgroot)	EUR 8.000 - EUR 15.000 [1]
Interne uren (MKB)	100-200 uur [1]
Technische aanpassingen	EUR 3.000 - EUR 20.000 [5]

JAARLIJKSE TERUGKERENDE KOSTEN

KOSTENPOST	BEDRAG
Surveillance-audit (jaar 2 en 3)	EUR 2.000 - EUR 7.000/jaar [19]
Hercertificering (elke 3 jaar)	EUR 6.000 - EUR 15.000 [18]
Onderhoud ISMS (intern)	EUR 3.000 - EUR 10.000/jaar [15]

5. Een implementatiepartner kiezen

Een ervaren implementatiepartner kan het verschil maken tussen een traject van 6 maanden en een dat vastloopt na 18 maanden. Zonder begeleiding duurt een implementatie gemiddeld 12 tot 24 maanden [16].

WAAR MOET JE OP LETTEN?

1. **Ervaring in jouw sector en bedrijfsgrootte** - vraag om referenties van vergelijkbare organisaties
2. **Pragmatische aanpak** - een ISMS moet werkbaar zijn, niet alleen op papier staan
3. **Slagingspercentage** - vraag hoeveel klanten bij de eerste audit slagen
4. **Onafhankelijkheid** - de consultant mag niet ook de certificeringsaudit uitvoeren
5. **Vaste prijs vs. nacalculatie** - een vaste projectprijs geeft zekerheid over de kosten

> **De juiste partner vinden?**
>
> Er zijn tientallen ISO 27001 consultancybureaus actief in Nederland, van pragmatische MKB-specialisten tot grote internationale adviesbureaus. De keuze hangt af van je sector, bedrijfsgrootte en budget. Vergelijk minimaal 3 partijen op ervaring, referenties en aanpak. Via IBgids.nl word je vrijblijvend gematcht met aanbieders die passen bij jouw situatie.

6. Het certificeringsproces

De certificeringsaudit wordt uitgevoerd door een onafhankelijke certificerende instelling (CI) en bestaat uit twee fasen.

STAGE 1: DOCUMENTATIEBEOORDELING

Duur: 2-3 dagen. De auditor beoordeelt je ISMS-documentatie tegen de ISO 27001 eisen: scope, beleid, risicoanalyse en Statement of Applicability. Er wordt nog niet getoetst of alles in de praktijk werkt. Het resultaat is een lijst met eventuele gaps voor Stage 2 [20].

STAGE 2: IMPLEMENTATIETOETSING

Duur: 3-5 dagen, enkele weken na Stage 1. De auditor komt op locatie en verifieert de daadwerkelijke implementatie: interviews met medewerkers, procesobservatie, bewijs dat het ISMS niet alleen op papier bestaat. Bij positief resultaat ontvang je het certificaat [21].

NA HET CERTIFICAAT

Het certificaat is 3 jaar geldig [6]. In jaar 2 en 3 volgen surveillance-audits (elk 1-2 dagen) om te controleren dat het ISMS operationeel blijft. Na 3 jaar volgt een volledige hercertificeringsaudit.

CERTIFICERENDE INSTELLINGEN IN NEDERLAND

Kies altijd een CI die geaccrediteerd is door de Raad voor Accreditatie (RvA). Bekende CI's in Nederland: DigiTrust, DEKRA, TUV NORD, BSI, DNV, Kiwa en Brand Compliance [22].

LET OP

Selecteer ook tijdig een certificerende instelling. De wachttijd voor een audit kan 4-8 weken zijn. Plan dit in je tijdlijn mee. Op certificeerwijzer.nl vind je een overzicht van certificerende instellingen en kun je tarieven vergelijken.

7. Veelgemaakte fouten

Deze valkuilen zien we regelmatig bij ISO 27001 implementaties. Voorkom ze.

1. Gebrek aan management commitment

De belangrijkste faalfactor. Zonder actieve steun van de directie strandt elk traject. Het management moet niet alleen budget vrijmaken, maar ook zichtbaar betrokken zijn [23].

2. Onderschatting van tijd en resources

Organisaties plannen vaak 6 maanden terwijl 9-12 maanden realistischer is. Tijdsdruk leidt tot haastige implementaties waarbij belangrijke stappen worden overgeslagen [24].

3. Papieren tijger: documentatie zonder implementatie

Een overmaat aan documentatie die niet aansluit op de werkwijze. Auditors herkennen dit direct. Het ISMS moet leven in de organisatie [25].

4. Informatiebeveiliging = alleen IT

ISO 27001 raakt de hele organisatie: HR, facilities, juridisch, operations. Het delegeren naar "iemand met wat vrije tijd" bij IT is een recept voor falen [26].

5. Onvolledige risicoanalyse

De risicoanalyse is het fundament. Een oppervlakkige of onvolledige risicoanalyse ondermijnt het hele ISMS en leidt tot verkeerde maatregelen [13].

6. Scope te breed of te smal

Te breed maakt het onnodig complex en duur. Te smal betekent dat het certificaat niet dekt wat klanten verwachten [27].

8. ISO 27001 en NIS2

De Cyberbeveiligingswet (de Nederlandse implementatie van NIS2) treedt naar verwachting in Q2 2026 in werking [7]. ISO 27001 vormt de beste basis, maar is niet volledig voldoende.

WAT ISO 27001 WEL DEKT

Risicoanalyse en passende maatregelen, beleid en procedures, interne audits en periodieke evaluaties, training en bewustwording van medewerkers [12].

WAT ISO 27001 NIET DEKT

NIS2-EIS	ISO 27001	TOELICHTING
Bestuurdersaansprakelijkheid	Niet gedekt	Bestuurders worden persoonlijk verantwoordelijk
Incidentmeldplicht	Gedeeltelijk	NIS2 eist melding aan autoriteiten binnen strikte termijnen
Supply chain security	Gedeeltelijk	NIS2 eist juridisch vastgelegde leveranciersbeveiliging
Sancties	Niet van toepassing	NIS2 voorziet in boetes tot EUR 10M of 2% omzet

> **Advies**
>
> ISO 27001 vormt de beste basis voor NIS2-compliance. Organisaties die al gecertificeerd zijn, hoeven slechts een beperkt aantal aanvullende stappen te zetten. Begin nu met ISO 27001 zodat je voorbereid bent wanneer de Cyberbeveiligingswet in werking treedt [28].

9. ISO 27001 vs SOC 2 vs NEN 7510

Welke standaard past bij jouw organisatie? Dit zijn de belangrijkste verschillen.

KENMERK	ISO 27001	SOC 2	NEN 7510
Scope	Alle sectoren, wereldwijd	SaaS, cloud providers	Zorgsector NL
Type bewijs	Certificaat (3 jaar)	Attestatierapport	Certificaat
Marktfocus	Europa, internationaal	VS, Anglo-Saksisch	Nederland, zorg
Verplicht?	Nee (indirect wel)	Nee (klanteis)	Ja, voor zorg
Kosten (MKB)	EUR 15-40K	EUR 20-50K	EUR 15-45K
Doorlooptijd	6-12 maanden	3-9 maanden	6-14 maanden

Kies ISO 27001 als: je opereert op de Europese markt, opdrachtgevers (overheid, finance) het eisen, je NIS2/Cbw compliance als doel hebt, of je internationaal wilt groeien.

Kies NEN 7510 als: je organisatie gezondheidsgegevens verwerkt of levert aan zorginstellingen. NEN 7510 is wettelijk verplicht in de zorg. Het is een superset van ISO 27001: wie NEN 7510 heeft, voldoet grotendeels ook aan ISO 27001 [29].

10. Aan de slag

Klaar om te beginnen? Dit zijn de concrete eerste stappen.

1. **Bepaal je scope** - welke processen, systemen en locaties vallen onder het ISMS?
2. **Zorg voor management commitment** - formeel akkoord van de directie, inclusief budget
3. **Inventariseer je huidige situatie** - wat heb je al aan beveiliging? Waar zitten de gaten?
4. **Stel een projectteam samen** - wijs een projectleider aan, betrek IT, HR en management
5. **Stel budget en planning op** - reken op EUR 15.000-40.000 totaal voor MKB, plan 6-12 maanden
6. **Selecteer een implementatiepartner** - vergelijk minimaal 3 bureaus op ervaring en referenties
7. **Selecteer een certificerende instelling** - kies een RvA-geaccrediteerde CI, plan de audit vroegtijdig

Bronnenlijst

[1] **DigiTrust** - Is ISO 27001 betaalbaar voor het MKB? Kosten, interne uren, certificeringsaudit. digitrust.nl

[2] **CertificeringsAdvies NL** - Hoelang duurt ISO 27001 certificering? Doorlooptijd per bedrijfsgrootte. certificeringsadvies.nl

[3] **NormSupport** - De uitdaging van ISO 27001 certificering voor Nederlandse bedrijven. <0,5% gecertificeerd. normsupport.nl

[4] **ISO Survey 2024 / HEIC** - ISO 27001 certifications nearly double in 2024. 96.709 certificaten wereldwijd. heic.eu

[5] **Nieuwhuis Consult** - ISO 27001 voor MKB: is het de investering waard? ROI, break-even 18-36 maanden. nieuwhuisconsult.nl

[6] **DEKRA** - ISO 27001 certificatie. Geldigheid 3 jaar, surveillance-audits. dekra.nl

[7] **Digitale Overheid** - Cyberbeveiligingswet. Verwachte inwerkingtreding Q2 2026. digitaleoverheid.nl

[8] **Nieuwhuis Consult** - Is ISO 27001 verplicht voor mijn bedrijf? nieuwhuisconsult.nl

[9] **Ondernemersplein** - ISO en NEN certificering voor uw bedrijf. Aanbestedingseisen. ondernemersplein.overheid.nl

[10] **TUV NORD** - ISO 27001 certificering. Klantvertrouwen en transparantie. tuv.nl

[11] **Verzekercyber.nl** - Wat kost een cyberverzekering? MKB premies vanaf EUR 1.500/jaar. verzekercyber.nl

[12] **Cyberbeveiligingswet.info** - Cyberbeveiligingswet en ISO 27001. Overlap en aanvullingen. cyberbeveiligingswet.info

[13] **Nieuwhuis Consult** - Kosten ISO 27001 implementatie. Belang risicoanalyse. nieuwhuisconsult.nl

[14] **Audit Direct** - ISO 27001 certificering binnen 3 maanden: is een versneld traject haalbaar? auditdirect.nl

[15] **Nieuwhuis Consult** - Hoe lang duurt een ISO 27001 implementatietraject? Tijdlijnen en verwachtingen. nieuwhuisconsult.nl

[16] **DigiTrust** - How long does ISO 27001 implementation take? Zonder begeleiding 12-24 maanden. digitrust.nl

[17] **Diks Process Support** - Hoeveel kost ISO 27001 consultancy? Dagtarieven EUR 800-1.500. diksprocesssupport.nl

[18] **Diks Process Support** - Wat zijn de kosten van een ISO 27001 audit? diksprocesssupport.nl

[19] **Diks Process Support** - Wat zijn de jaarlijkse kosten van ISO 27001? Surveillance-audit kosten. diksprocesssupport.nl

[20] **TUV NORD** - Certificeringsproces ISO 27001. Stage 1 en Stage 2 uitleg. tuv.nl

[21] **ProActive Compliance Tool** - ISO 27001 certificering: hoe werkt een audit? proactivecompliancetool.nl

[22] **ISO Register** - Overzicht certificatie-instellingen in Nederland. isoregister.nl

[23] **DigiTrust** - Waarom falen sommige ISO 27001 projecten? Management commitment. digitrust.nl

[24] **DigiTrust** - Wat zijn de grootste uitdagingen bij ISO 27001? Tijdsonderschatting. digitrust.nl

[25] **Fendix** - Veelgemaakte ISO 27001 implementatiefouten. Papieren tijger. fendix.nl

[26] **Equans** - ISO 27001 certificering: voorkom deze 3 cruciale valkuilen. equans.nl

[27] **CertificeringsAdvies NL** - ISO 27001 checklist in 15 stappen. Scope-problemen. certificeringsadvies.nl

[28] **CertificeringsAdvies NL** - NIS2 stappenplan voor NIS2 en ISO 27001 mapping. certificeringsadvies.nl

[29] **Fendix** - ISO 27001 vs NEN 7510: de verschillen. fendix.nl

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief en gebaseerd op de Nederlandse markt (peildatum: maart 2026).