GIDS

De complete gids voor de ISO 27001 interne audit

Kosten, proces, uitbesteden vs. zelf doen, frequentie, veelgemaakte fouten en NIS2-verband. Met actuele Nederlandse marktdata.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De interne audit is verplicht voor ISO 27001 certificering en bepaalt mede het succes van je externe audit. Hier de feiten.

EUR 1,6K--4K
Kosten uitbestede interne audit voor MKB
Audit Direct [1]

EUR 4K+
Werkelijke kosten bij zelf uitvoeren (incl. risico her-audit)
Audit Direct [1]

1×/jaar
Minimale frequentie interne audit volgens ISO 27001 clausule 9.2
ISO 27001:2022 [2]

20--40 uur
Interne uren voor een MKB interne audit (voorbereiding + uitvoering + rapport)
Audit Direct [1]

EUR 1.500
Extra kosten bij her-audit door gemiste non-conformiteiten
Audit Direct [1]

93
Annex A controls in ISO 27001:2022 die minimaal elke 3 jaar geaudit moeten worden
ISO 27001:2022 [2]

EUR 500--1,5K
Kosten interne auditor training (2--3 dagen klassikaal)
DigiTrust [3]

1--2 wk
Doorlooptijd interne audit voor een MKB-organisatie
Best practice

1. Wat is een ISO 27001 interne audit?

De interne audit is jouw eigen controle op de werking van het ISMS. Het is een verplicht onderdeel van ISO 27001 (clausule 9.2) en een voorwaarde voor certificering.

Bij een interne audit controleer je of jouw Information Security Management System (ISMS) voldoet aan de eisen van ISO 27001:2022 en of het effectief werkt in de praktijk. De audit wordt uitgevoerd door een objectieve auditor -- dat kan een eigen medewerker zijn (mits die niet het eigen werk audited) of een ingehuurde specialist [2].

De interne audit verschilt van de externe audit op een cruciaal punt: bij een interne audit mag de auditor verbetersuggesties doen. Bij een externe audit mag dat niet -- de CI oordeelt alleen [4].

> **Waarom is de interne audit belangrijk?** Zonder interne audit geen certificering. Maar het is meer dan een vinkje: een goede interne audit vindt zwakke plekken voordat de externe auditor ze vindt. Dat bespaart je een her-audit (EUR 1.500+) en reputatieschade [1].

WIE MAG DE INTERNE AUDIT UITVOEREN?

De auditor moet voldoen aan twee eisen: **objectiviteit** (niet je eigen werk auditen) en **competentie** (voldoende kennis van de norm). Bij kleine organisaties is objectiviteit intern lastig te garanderen -- dan is uitbesteden de logische keuze [5].

2. Het auditproces in 7 stappen

Een gestructureerde aanpak maakt het verschil tussen een oppervlakkige afvinkoefening en een audit die echte waarde levert.

1 Auditprogramma opstellen

1--2 DAGEN

Bepaal welke onderdelen je wanneer audited. Kernclausules (4--10) jaarlijks, alle Annex A controls minimaal elke 3 jaar [6].

2 Scope en doelstellingen bepalen

0,5 DAG

Wat is het doel van deze specifieke audit? Conformiteit toetsen, effectiviteit beoordelen, of beide?

3 Auditchecklist voorbereiden

1--2 DAGEN

Stel per clausule en control concrete vragen op. Gebruik de SoA als basis voor Annex A controls [7].

4 Documentreview

1--2 DAGEN

Beoordeel beleid, procedures en registraties op actualiteit, volledigheid en consistentie.

5 Interviews en observaties

1--3 DAGEN

Praat met medewerkers op verschillende niveaus. Stel open vragen. Observeer of procedures in de praktijk worden gevolgd.

6 Auditrapport opstellen

1--2 DAGEN

Classificeer bevindingen als major, minor of observatie. Beschrijf het bewijs en verwijs naar de relevante clausule of control [8].

7 Bevindingen bespreken en opvolgen

0,5--1 DAG

Bespreek het rapport met management. Wijs eigenaren aan voor corrigerende acties. Plan opvolging.

TIP

Plan de interne audit minimaal 1 maand voor de externe audit. Zo heb je voldoende tijd om bevindingen op te lossen en corrigerende acties te implementeren.

3. Wat kost het?

De kosten van een interne audit hangen af van je keuze: uitbesteden of zelf doen. Uitbesteden is vaak goedkoper dan gedacht -- zelf doen duurder.

KOSTEN BIJ UITBESTEDEN

BEDRIJFSGROOTTE	KOSTEN
Klein MKB (<25 mdw)	EUR 1.600 -- EUR 2.500
Middelgroot (25--100 mdw)	EUR 2.500 -- EUR 4.000
Groot (100+ mdw)	EUR 3.000 -- EUR 6.000

Bron: Audit Direct [1]

KOSTEN BIJ ZELF UITVOEREN

KOSTENPOST	BEDRAG
Interne uren (20--40 uur x EUR 85)	EUR 1.700 -- EUR 3.400
Risico her-audit (bij gemiste bevindingen)	EUR 1.500
Geschatte totaalkosten	EUR 3.200 -- EUR 4.900

> **VERBORGEN KOSTEN BIJ ZELF DOEN**
> Het risico dat een ongetrainde collega fouten mist is groot. Als de externe auditor deze fouten vindt, volgt een her-audit van circa EUR 1.500 extra. De totale geschatte impact is EUR 4.050 [1].

KOSTEN INTERNE AUDITOR OPLEIDEN

OPLEIDING	KOSTEN	DUUR
Online awareness	EUR 200 -- EUR 800	1 dag
Interne auditor training	EUR 500 -- EUR 1.500	2--3 dagen
Lead Auditor training	EUR 2.000 -- EUR 4.000	5 dagen

Bron: DigiTrust [3], IAS [9]

4. Uitbesteden vs. zelf doen

De meeste MKB-organisaties besteden de interne audit uit -- niet vanwege de kosten, maar vanwege objectiviteit en expertise.

VERGELIJKING

FACTOR	UITBESTEDEN	ZELF DOEN
Directe kosten	EUR 1.600 -- EUR 4.000	EUR 1.700 -- EUR 3.400
Objectiviteit	Hoog (geen bedrijfsblindheid)	Risico op bias
Kwaliteit	Hoog (specialist)	Wisselend
Risico her-audit	Laag	Hoger (+EUR 1.500)
Kennis in de organisatie	Minder opbouw	Meer interne kennis
Capaciteitsbeslag	Minimaal	20--40 uur

WANNEER UITBESTEDEN?

- Geen medewerker met ISO 27001-kennis beschikbaar
- Onafhankelijkheid intern niet te garanderen (kleine organisatie)
- Eerste interne audit (geen ervaring met het proces)
- Extra zekerheid voor een belangrijke externe audit

HET HYBRIDE MODEL

Veel organisaties kiezen een groeipad: jaar 1 volledig extern, jaar 2 samen met extern (kennisoverdracht), jaar 3 intern met externe review van het rapport [5].

TIP

Op certificeerwijzer.nl vind je aanbieders die interne ISO 27001 audits uitvoeren. Vergelijk op ervaring, tarieven en sector.

5. Frequentie en planning

ISO 27001 schrijft geen vaste frequentie voor, maar geeft richtlijnen. De praktijk wijst uit: minimaal jaarlijks, met een slim auditprogramma.

FREQUENTIE-EISEN

ONDERDEEL	FREQUENTIE
Kernclausules (4--10)	Jaarlijks
Annex A controls (93 stuks)	Alle minimaal elke 3 jaar
Risicogebieden	Jaarlijks of vaker bij hoog risico
Na significante wijzigingen	Direct

Bron: ISO 27001:2022 clausule 9.2 [2], Hightable [6]

SLIMME PLANNING

Verdeel de 93 Annex A controls over 3 jaar. Audit elk jaar circa 31 controls plus alle kernclausules. Focus op risicogebieden en gebieden waar eerder bevindingen waren.

> **Planning voorbeeld MKB:** Jaar 1: clausules 4--10 + organisatorische controls (A.5). Jaar 2: clausules 4--10 + mensgerichte (A.6) en fysieke controls (A.7). Jaar 3: clausules 4--10 + technologische controls (A.8). Zo zijn in 3 jaar alle controls aan bod geweest.

6. Waar kijkt de auditor naar?

Een goede interne audit gaat verder dan afvinken. De auditor zoekt bewijs dat het ISMS werkt in de praktijk.

CLAUSULES 4--10 (HET MANAGEMENTSYSTEEM)

- **Clausule 4:** Context -- zijn stakeholders en scope geidentificeerd?
- **Clausule 5:** Leiderschap -- is het management actief betrokken?
- **Clausule 6:** Planning -- zijn risico's en kansen geadresseerd?
- **Clausule 7:** Ondersteuning -- zijn competenties en bewustzijn op orde?
- **Clausule 8:** Uitvoering -- werkt het risicobehandelplan?
- **Clausule 9:** Evaluatie -- monitoring, meting, interne audit, management review
- **Clausule 10:** Verbetering -- worden non-conformiteiten opgelost?

ANNEX A CONTROLS (93 CONTROLS)

CATEGORIE	AANTAL CONTROLS	VOORBEELDEN
Organisatorisch (A.5)	37	Beleid, rollen, leveranciersbeheer
Mensgericht (A.6)	8	Screening, awareness, disciplinair
Fysiek (A.7)	14	Toegang, apparatuur, clear desk
Technologisch (A.8)	34	Toegangsbeheer, encryptie, logging

MEEST VOORKOMENDE BEVINDINGEN

- Verouderde of ontbrekende risicoanalyse
- Inactieve accounts niet opgeschoond
- Ontbrekende trainingsregistraties
- Incidenten niet geregistreerd of niet afgehandeld
- Geen testresultaten van back-upherstel
- Leveranciers niet beoordeeld op beveiligingsniveau

7. Veelgemaakte fouten

Deze fouten ondermijnen de waarde van je interne audit en verhogen het risico op problemen bij de externe audit.

1. **Eigen werk auditen**
   De objectiviteitseis is strikt: je mag niet je eigen implementatie controleren. De CI kan dit als non-conformiteit rapporteren [5].

2. **Te oppervlakkig auditen**
   Alleen afvinken zonder doorvragen levert weinig op. Stel "waarom"- en "hoe"-vragen. Vraag om bewijs [1].

3. **Geen auditprogramma**
   De externe auditor verwacht een gepland en gedocumenteerd auditprogramma. Zonder programma is clausule 9.2 niet vervuld [6].

4. **Alleen documentatie checken**
   De interne audit moet ook interviews en observaties bevatten. Documentatie alleen zegt niets over de praktijk [10].

5. **Geen follow-up op bevindingen**
   Bevindingen zonder corrigerende acties zijn waardeloos. Wijs eigenaren aan en plan opvolging [6].

6. **Te laat auditen**
   Als de interne audit te kort voor de externe audit plaatsvindt, is er geen tijd om bevindingen op te lossen.

7. **Bevindingen niet classificeren**
   Onderscheid maken tussen major, minor en observatie is belangrijk voor prioritering en opvolging [8].

8. NIS2 en de Cyberbeveiligingswet

De interne audit wordt nog belangrijker met de komst van NIS2. Het is je instrument om aantoonbaar "in control" te zijn.

WAAROM DE INTERNE AUDIT ESSENTIEEL IS VOOR NIS2

NIS2 vereist dat organisaties kunnen aantonen dat hun cyberbeveiligingsmaatregelen effectief zijn. De interne audit levert dit bewijs. Zonder interne audit geen certificering, en zonder certificering een zwakkere positie bij NIS2-toezicht [11].

AANVULLENDE AUDITONDERWERPEN VOOR NIS2

- **Meldprocedure:** 24 uur vroegtijdige waarschuwing, 72 uur volledige melding bij CSIRT
- **Ketenbeveiliging:** beoordeling van leveranciers en hun beveiligingsniveau
- **Business continuity:** crisisbeheersing en herstelplannen
- **Bestuurlijke betrokkenheid:** aantoonbare rol van de directie

Bron: Fendix [12]

> **Aanbeveling:** Neem de NIS2-specifieke onderwerpen op in je auditprogramma. Zo bereid je je organisatie voor op zowel de externe audit als het NIS2-toezicht.

9. Verschil met verwante diensten

De interne audit wordt regelmatig verward met andere vormen van beoordeling. Hieronder de belangrijke verschillen.

INTERNE AUDIT VS. EXTERNE AUDIT

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

INTERNE AUDIT VS. GAP-ANALYSE

ASPECT	INTERNE AUDIT	GAP-ANALYSE
Wanneer	Jaarlijks, na implementatie	Voor implementatie
Formeel	Ja -- ISO 27001-eis	Nee -- geen normatieve eis
Output	Non-conformiteiten	Gap-rapport met actieplan

INTERNE AUDIT VS. MANAGEMENT REVIEW

ASPECT	INTERNE AUDIT	MANAGEMENT REVIEW
Uitvoerder	Interne auditor	Top management
Doel	Conformiteit en effectiviteit	Strategische geschiktheid
Relatie	Levert input voor management review	Bepaalt prioriteiten

10. Volgende stappen

Of je de interne audit uitbesteedt of zelf doet -- begin met een helder plan.

1. **Bepaal je aanpak**
   Uitbesteden, zelf doen of hybride? Weeg objectiviteit, kosten en interne capaciteit tegen elkaar af.

2. **Stel een auditprogramma op**
   Bepaal welke clausules en controls je dit jaar audited. Verdeel Annex A controls over 3 jaar.

3. **Plan de timing**
   Plan de interne audit minimaal 1 maand voor de externe audit. Zorg voor voldoende tijd om bevindingen op te lossen.

4. **Bij uitbesteden: vergelijk aanbieders**
   Vraag minimaal 3 offertes aan. Vergelijk op ervaring, tarief en sectorkennis. Gebruik certificeerwijzer.nl voor een overzicht.

5. **Bij zelf doen: zorg voor opleiding**
   Investeer in een interne auditor training (EUR 500--EUR 1.500). De investering betaalt zich terug in kwaliteit.

Bronnenlijst

[1] **Audit Direct** -- Interne audit ISO 27001 uitbesteden vs. zelf doen (auditdirect.nl)

[2] **ISO/IEC 27001:2022** -- Clausule 9.2 Internal Audit

[3] **DigiTrust** -- Internal Auditor ISO 27001 training (digitrust.nl)

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

[5] **CertificeringsAdvies NL** -- De interne audit uitbesteden of niet (certificeringsadvies.nl)

[6] **Hightable** -- ISO 27001 Internal Audit: The Lead Auditor's Guide (hightable.io)

[7] **Advisera** -- Checklist Interne Audit sjabloon (advisera.com)

[8] **DigiTrust** -- Hoe los je ISO 27001 non-conformiteiten op (digitrust.nl)

[9] **IAS** -- ISO 27001 interne auditor opleiding in Nederland (iasiso-europe.com)

[10] **Vanta** -- 7 steps to an effective ISO 27001 internal audit (vanta.com)

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

[12] **Fendix** -- NIS2 & ISO 27001: de overlap en verschillen (fendix.nl)