



De ISO 27001 audit

Wat je écht moet weten – Een praktische
gids

Inhoud

1	Waarom een ISO 27001-certificering?	2
2	Ben ik klaar voor de audit?	3
	Wat minimaal op orde moet zijn	3
	Moet alles perfect zijn?	3
3	Hoe lang duurt een audit — en wat kost het?	4
	Het aantal dagen is genormeerd	4
	Kosten van de audit	4
	Jaarlijkse kosten	5
4	Waar vraag je een audit aan?	6
5	Hoe verloopt de audit?	7
	Fase 1: de documentatie-audit	7
	De tussenpauze	7
	Fase 2: de implementatie-audit	7
	Opening en Closing meetings	7
6	Wat verwacht de auditor?	9
	Hoe auditors vragen stellen	9
	Vier lagen documentatie	9
7	Wat is het resultaat van de audit?	11
	Het Corrective Action Plan	11
	Als je het niet eens bent met de auditor	12
8	Uitslag en certificering	13
	De aanbeveling	13
	Wie beslist	13
	Geldigheid	13
9	Hoe verder?	14

Voor wie is dit eBook?

Dit eBook is geschreven voor iedereen die een ISO 27001-certificering overweegt en wil begrijpen hoe het er in een audit écht aan toe gaat. Je leest waar auditors naar op zoek zijn, wat er vaak misgaat, en waarom de 93 maatregelen minder belangrijk zijn dan je denkt.

1. Waarom een ISO 27001-certificering?

ISO 27001 is de internationale standaard voor informatiebeveiliging. Een ISO 27001 certificaat bewijst dat je de beveiliging van informatie structureel managed via een Information Security Management System (ISMS). Dat betekent dat je processen hebt geïmplementeerd waarmee je continu de risico's bewaakt en passende maatregelen treft.

Organisaties kiezen voor ISO 27001 om verschillende redenen. Meestal één van de onderstaande, vaak een combinatie ervan:

Inkoopvoorwaarden van klanten. Met name grote klanten stellen ISO 27001 als harde voorwaarde. Aanvankelijk vooral in de publieke sector, financiële dienstverlening en zorg (NEN 7510), maar als gevolg van ketenverantwoordelijkheid in wet- en regelgeving wordt het steeds meer een 'license to sell'.

Aanbestedingen. In Europa is ISO 27001 (of gelijkwaardige aantoonbare informatiebeveiliging) een standaard eis in overheidstenders.

Wet- en regelgeving. Kaders als de NIS-2, de Cyberbeveiligingswet (Cbw), de Cyber Resilience Act (CRA), DORA en GDPR hebben een grootste gemene deler: robuuste informatiebeveiliging op basis van risicomanagement en een 'all risk approach'. Dit is precies wat je met een ISO 27001 certificering kunt aantonen.

Vertrouwen richting klanten en partners. Het certificaat zegt: wij houden ons verantwoordelijk voor de beveiliging van uw informatie, wij nemen dat serieus, en we laten dat onafhankelijk toetsen – dat is een sterker signaal dan de belofte je best te doen.

Operationele volwassenheid. Het certificeringstraject dwingt je om je eigen huis op orde te brengen: risico's te benoemen, verantwoordelijkheden vast te leggen, en processen herhaalbaar te maken. Je groeit als organisatie van incidentgedreven naar voortdurend verbeterend. Daarnaast zul je onbekende gaten in je beveiligingsproces ontdekken.

Organisaties die de certificering aanvaren als het afvinken van maatregelen en het produceren van overbodige documentatie missen de kern en merken dat tijdens de audit – ze komen meestal niet verder dan Fase I.

VOLGENDE VRAAG: Ben ik klaar voor de audit?

2. Ben ik klaar voor de audit?

Dit is de vraag die begrijpelijker wijs de meeste stress oplevert. We kunnen deze vraag niet beantwoorden met een checklist.

Een organisatie is klaar voor de externe audit als ze het ISMS heeft ingericht, èn getoetst op effectieve werking. Meer concreet betekent het dat de volgende stappen moeten zijn afgerond voordat de auditor langskomt.

Wat minimaal op orde moet zijn

Het ISMS is operationeel. De fundamentele processen uit de norm — hoofdstuk 4 tot en met 10 — draaien aantoonbaar. De scope is afgebakend, het informatiebeveiligingsbeleid is ondertekend, en er is een risicoanalyse uitgevoerd die is vertaald naar een risicobehandelplan.

Er is een interne audit uitgevoerd. Voordat de externe auditor komt, vereist de norm dat je het systeem zelf hebt geëvalueerd. Minimaal één interne audit, met een auditrapport als uitkomst. Eventuele afwijkingen zijn gedocumenteerd en worden opgevolgd.

De directiebeoordeling heeft plaatsgevonden. Na de interne audit beoordeelt het topmanagement formeel de prestaties en effectiviteit van het ISMS. Dit is geen formaliteit maar het bewijs dat de directie betrokken is.

De verplichte documentatie is beschikbaar. Denk aan de Verklaring van Toepasselijkheid (de Statement of Applicability of SoA), procedures, en de registraties van de interne audit en directiebeoordeling. Ze moeten bestaan, vindbaar zijn, en beheerd worden.

Kort samengevat: als je het ISMS hebt ingericht én je de Plan-Do-Check-Act cyclus minimaal één keer zelf hebt doorlopen, ben je klaar om een certificeringsinstantie te benaderen.

Moet alles perfect zijn?

Nee. Een auditor verwacht niet dat elke maatregel op dag één 100% is doorgevoerd. Zolang het managementfundament draait, accepteert de norm dat je met een risicobehandelplan werkt. Als een maatregel later wordt geïmplementeerd en de directie het re-strisico (voorlopig) formeel accepteert, is dat toegestaan.

Wees hier wel transparant over: claim niet dat iets is geïmplementeerd terwijl dat in feite nog (deels) moet gebeuren. Een goede auditor prikt hier snel doorheen en het geeft een slechte indruk voor de betrouwbaarheid van het ISMS.

VOLGENDE VRAAG: Hoe lang duurt een audit — en wat kost het?

3. Hoe lang duurt een audit — en wat kost het?

Twee vragen die altijd samen worden gesteld, en waarop het antwoord altijd hetzelfde begint: *het hangt ervan af*. Maar we kunnen wel bandbreedtes geven.

Het aantal dagen is genormeerd

Het aantal auditdagen is niet iets wat een certificeringsinstantie zelf mag verzinnen. Het is gereguleerd door de ISO 27006-norm, op basis van de grootte van de organisatie. Offertes van verschillende instanties zullen daarom vaak op een vergelijkbaar aantal dagen uitkomen.

Ruwe richtlijnen:

Organisatiegrootte	Totaal auditdagen (basis)
1–10 medewerkers	5 dagen
11–15 medewerkers	6 dagen
176–275 medewerkers	14 dagen

Een deel van die dagen zal de auditor bij jou op kantoor of in de fabriek aanwezig zijn.

Voor de minimale audit van 5 dagen ziet de tijdsverdeling er doorgaans zo uit:

- ½ dag: planning en voorbereiding
- 1 dag: Fase 1 (documentatie-audit)
- 3 dagen: Fase 2 (implementatie-audit)
- ½ dag: opstellen auditrapport

De basislijn kan omhoog worden bijgesteld — door complexe IT-omgevingen, meerdere locaties, sterk gereguleerde sectoren of veel uitbestede diensten.

Kosten van de audit

Voor de auditfee alleen kun je grofweg rekenen op:

- Kleine organisaties (tot ~10 FTE): €5.000–€10.000
- Middelgrote organisaties: €10.000–€20.000
- Dagtarieven bij certificeringsinstanties liggen doorgaans tussen de €1.200 en €1.800

De totale kosten kunnen om verschillende redenen hoger zijn, bijv. door verschillen in dagtarieven, doorberekening van reis- en verblijfkosten, en inschatting van complexiteit.

Dit is dus exclusief de implementatiekosten: interne uren, tooling en consultancy. Met name die laatste twee kunnen de kosten behoorlijk opjagen.

Jaarlijkse kosten

Het ISO 27001 certificaat is drie jaar geldig, maar de auditor komt jaarlijks terug voor een surveillance audit (ook wel controle-audit of onderhoudsaudit. Deze is kleiner dan de initiële audit — reken op ongeveer 30–50% van de initiële auditkosten, of €2.000–€5.000 per jaar voor kleinere organisaties. In het derde jaar volgt een hercertificeringsaudit.

VOLGENDE VRAAG: Waar vraag je een audit aan?

4. Waar vraag je een audit aan?

Een ISO 27001-certificeringsaudit vraag je aan bij een zogenaamde *certification body* — niet bij een consultant, en niet bij een interne auditor. Consultants kunnen je ondersteunen bij de voorbereiding, maar zij mogen geen officiële certificering afgeven.

De certification body is een instantie die geaccrediteerd is voor ISO 27001 door de Raad voor Accreditatie (RvA). In Nederland zijn dat onder andere partijen als Kiwa, DNV, BSI en DigiTrust. Controleer altijd of de accreditatie actueel is in het register van de Raad voor Accreditatie. Niet-geaccrediteerde instellingen kunnen geen geldig ISO 27001 certificaat afgeven.

Kies een partij met ervaring in jouw type organisatie. Een auditor die gewend is aan grote industriële bedrijven of ziekenhuizen kijkt anders naar het ISMS, dan iemand die regelmatig kleinere dienstverleners of SaaS-aanbieders auditeert. Dat maakt het verschil tussen een audit die daadwerkelijk waarde toevoegt en een audit die voelt als een bureaucratische verplichting.

VOLGENDE VRAAG: Hoe verloopt de audit?

5. Hoe verloopt de audit?

De initiële certificeringsaudit bestaat altijd uit twee fasen — dat wordt voorgeschreven door de norm. Deze tweedeling in de audit weerspiegelt de tweedeling in de ISO 27001 zelf: een fundament van processen (clausules 4 tot en met 10) en een bijlage met 93 mogelijk toepasbare beveiligingsmaatregelen (de Annex A controls).

Fase 1: de documentatie-audit

In Fase 1 kijkt de auditor naar het ontwerp van het managementsysteem. Begrijpt de organisatie de standaard? Hoe ziet het beveiligingsbeleid eruit? Is de scope duidelijk gesteld? Is er een risicoanalyse uitgevoerd? Is er een Statement of Applicability opgesteld? Zijn de interne audit en de directiebeoordeling afgerond? Zijn er plannen voor verbetering? Is dit consistent gedocumenteerd?

Fase 1 neemt meestal zo'n 30% van de totale audittijd in beslag. Het belang van deze fase wordt vaak onderschat, vooral door organisaties die de focus leggen op een checklist met maatregelen. Als de basis van het ISMS onvoldoende op orde is, kan de auditor besluiten dat het op dit moment geen zin heeft om naar Fase 2 te gaan.

De uitkomst van Fase 1 is een rapport met eventuele aandachtspunten. Sommige daarvan moeten zijn opgelost voordat Fase 2 begint. Daarvan zal de auditor bewijs willen zien. Vaak gebeurt dat door het overleggen van gecorrigeerde documentatie of in een externe bespreking (bijv. een Teams-call).

De tussenpauze

Tussen Fase 1 en Fase 2 zitten doorgaans twee tot vier weken, met een maximum van twaalf. In die tijd kunnen de aandachtspunten uit het Fase 1 rapport worden aangepakt.

Fase 2: de implementatie-audit

In Fase 2 gaat de auditor de organisatie in — op locatie of remote. Hij wil bewijs zien voor de daadwerkelijke implementatie en effectiviteit van de beveiligingsmaatregelen. Dat gebeurt o.a. door het bekijken van systemen, log- en configuratiebestanden, het interviewen van medewerkers, en een doorloop van het pand voor de fysieke beveiligingsmaatregelen.

Let op dat de audit al informeel begint als de auditor het terrein opkomt en het pand binnengaat: als hij zonder ooit bevraagd of gecontroleerd te worden een afdeling op kan lopen, zal hij willen weten of dat is voorzien in de risicoanalyse.

Aan het einde van Fase 2 — vaak tijdens de **closing meeting** — bespreekt de auditor zijn conclusies met het management.

Opening en Closing meetings

Aan het begin van zowel Fase 1 als Fase 2 houdt de auditor een **opening meeting** met het management en de relevante betrokkenen. Het doel is de scope en aanpak van de audit bevestigen, de agenda doornemen, en praktische afspraken maken over toegang,

begeleiding en communicatie. Dit is voor de organisatie ook het moment om vragen te stellen over het verloop.

Aan het einde van Fase 2 presenteert de auditor zijn bevindingen in de **closing meeting** — opnieuw met het management erbij. Alle non-conformiteiten en observaties worden mondeling toegelicht voordat ze in het rapport verschijnen. Dit is het moment waarop de organisatie kan reageren, verduidelijken, of — als ze het er niet mee eens zijn — bezwaar aantekenen.

De closing meeting is een samenvatting van de audit en zal geen verrassingen bevatten. Een goede auditor communiceert zijn bevindingen doorlopend tijdens de audit.

VOLGENDE VRAAG: Wat verwacht de auditor?

6. Wat verwacht de auditor?

Niet weten wat de auditor gaat vragen, is waar voor organisaties de meeste zorgen zitten. Alle clausules uit hoofdstuk 4 tot en met 10 — de fundamentele processen — moeten geïmplementeerd zijn, dus daar wordt je op bevraagd. Van de maatregelen die je via het SoA van toepassing hebt verklaard, zal hij de implementatie en de effectiviteit willen vaststellen, en van de maatregelen die je niet van toepassing hebt verklaard, wil hij weten wat daarvoor de reden is.

In de meeste audits die ik heb begeleid, loopt de auditor de onderdelen af in de volgorde waarin ze in de norm zijn beschreven. Sommige auditors doen het aan de hand van enkele belangrijke bedrijfsprocessen. Iedere auditor heeft zijn eigen stijl en stokpaardjes. Sommigen leunen zwaarder op formele documentatie dan anderen – daarin spelen ook de voorkeuren van de certificerende instantie waarvoor ze werken mee. Ik heb vanuit de klant audits begeleid, waarbij ik vooraf aanraadde de documentatie meer uit te breiden, en de auditor vervolgens aangaf dat het 'best wat minder had gemogen'. En andersom ook. Gelukkig ken ik weinig voorbeelden waarin de auditor zich onredelijk opstelt, zolang de basisprocessen op orde zijn en de organisatie oprecht streeft naar voortdurende verbetering. Een goede auditor heeft hier een neus voor.

Hoe auditors vragen stellen

Auditors geven de voorkeur aan open vragen en stellen zelden ja/nee-vragen. Zo krijgen ze meer informatie en is het risico op het geven van wenselijke antwoorden kleiner. Ze zullen de beweringen niet als feit aannemen, maar willen weten waaróm je iets zegt en op zoek gaan naar objectief bewijs om de bewering te ondersteunen of, bij redelijke twijfel, eventueel te weerleggen.

Je kunt bijvoorbeeld een reeks vragen verwachten als de volgende:

- Kun je me uitleggen hoe jullie omgaan met back-ups?
- Is dat ergens opgeschreven?
- Geldt het alleen voor dit systeem, of voor alle systemen?
- Hoe is de keuze gemaakt om het op die manier te doen?
- Welke specifieke risico's worden hiermee afgedekt?
- Kun je laten zien dat die back-ups ook volgens die procedure zijn uitgevoerd?
- Hoe gaan jullie om met uitzonderingen en foutmeldingen?
- Doen jullie regelmatig een restore test?
- Zijn daar verslagen van?

De auditor wil weten of wat er gezegd wordt ook klopt met wat er werkelijk gebeurt.

Vier lagen documentatie

Een auditor kijkt naar documentatie op vier niveaus:

Niveau 1 — Strategisch. Documenten ondertekend door het management: het ISMS-beleid, de scope, de SoA. Dit is het bewijs dat de top van de organisatie betrokken is en

verantwoordelijkheid neemt.

Niveau 2 — Risicobeheersing. Het formele proces: hoe voer je risicoanalyses uit, hoe behandel je risico's, hoe documenteer je risicoacceptatie?

Niveau 3 — Procedures. Hoe worden specifieke maatregelen uitgevoerd? Wachtwoord-beheer, patch-management, toegangsreviews — niet als abstracte beschrijving, maar als werkende procedure.

Niveau 4 — Records. De harde bewijsvoering: systeemlogs, incident-tickets, verslagen van vergaderingen, resultaten van access reviews. Records bewijzen dat het proces daadwerkelijk is gevolgd — niet dat het bestaat, maar dat het werkt.

Niveau 4 is waar de meeste organisaties tekortkomen. Ze hebben het beleid. Ze hebben de procedure. Maar de registratie — het bewijs dat de procedure werd gevolgd — ontbreekt of is inconsistent.

In de praktijk zien we vaak de volgende non-conformities (punten waarop niet aan de eis wordt voldaan):

- Onvolledige of verouderde risicoanalyses
- Access reviews die wel zijn uitgevoerd, maar niet zijn vastgelegd
- Incident response plannen die nooit zijn getest
- Patch-management zonder vaste procedures of rapportage
- Niet uitgevoerde en ongedocumenteerde leveranciersbeoordelingen
- Een SoA die niet klopt met de daadwerkelijke implementatie

Het gaat dus vaak niet om het ontbreken van maatregelen an sich, maar aan het ontbreken van structuur, herhaalbaarheid, documentatie en goede risicoanalyses.

VOLGENDE VRAAG: Wat is het resultaat van de audit?

7. Wat is het resultaat van de audit?

Als een auditor vaststelt dat niet aan een eis van de norm wordt voldaan, resulteert dat in een auditbevinding. Er zijn drie classificaties.

Observatie / afwijking. Een punt voor verbetering of een kleine incidentele afwijking. Het managementsysteem als geheel loopt geen gevaar.

Minor non-conformiteit. Een gedeeltelijk falen van een eis. Het werpt twijfels op, maar bedreigt het ISMS niet in zijn kern. Met een goed actieplan is dit oplosbaar zonder dat de certificering in gevaar komt.

Voorbeelden van minor non-conformities zijn:

- een wel uitgevoerde, maar niet gedocumenteerde access review
- een controle die volgens de procedure halfjaarlijks plaats moet vinden, maar die al zeven maanden niet is uitgevoerd
- het ontbreken van een verwerkersovereenkomst met een leverancier.

Major non-conformiteit. Een volledig falen van een eis, of een onacceptabel risico.

Voorbeelden van major non-conformities zijn:

- een geïdentificeerd risico dat niet geaccepteerd is, en waarvoor geen behandelplan bestaat
- het ontbreken van controls die essentieel zijn voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen jouw specifieke scope (denk aan toegangscontrole op systemen of het ontbreken van een incident response procedure)
- interne audits zijn niet uitgevoerd (de PDCA cyclus is onvolledig)
- de directiebeoordeling heeft niet plaatsgevonden (de directie is onvoldoende betrokken)
- belangrijke bedrijfsactiviteiten zijn buiten de scope van de audit verklaard – wat gecertificeerd wordt is niet representatief voor de daadwerkelijke bedrijfsvoering.

Bij een major non-conformiteit wordt de certificering direct stilgelegd. Als de non-conformiteit niet afdoende gecorrigeerd wordt, kan het certificaat niet worden afgegeven.

Het Corrective Action Plan

Als er non-conformiteiten zijn vastgesteld, moet je een Corrective Action Plan (CAP) indienen. Doorgaans krijg je daar 10 tot 60 dagen de tijd voor.

Een goed CAP bevat per non-conformiteit:

1. **Root cause analyse** — waarom is dit misgegaan?
2. **Correctie** — hoe is de directe tekortkoming tijdelijk opgelost?
3. **Correctieve actie** — hoe zorgen we dat dit structureel niet meer kan gebeuren?
4. **Tijddlijn** — wanneer is dit volledig afgerond?

Wordt het CAP niet geleverd, dan zal de auditor geen positieve certificeringsaanbeveling doen.

Als je het niet eens bent met de auditor

Meningsverschillen kun je uitpraten tijdens de audit of in de afsluitende bijeenkomst. Kom je er niet uit, dan heb je het recht om bevindingen niet te accepteren en een formeel beroepsproces op te starten bij de certificeringsinstantie. Dat is een serieuze stap, maar het recht daarop is er.

VOLGENDE VRAAG: Uitslag en certificering

8. Uitslag en certificering

De aanbeveling

Aan het einde van Fase 2 — vaak tijdens de closing meeting — bespreekt de auditor zijn conclusies met het management. Er zijn vier mogelijke uitkomsten:

1. **Aanbeveling voor certificering.** Alles is in orde.
2. **Voorwaardelijke aanbeveling zonder extra bezoek.** Je krijgt het certificaat mits je op afstand een goedgekeurd actieplan voor je minor non-conformiteiten aanlevert.
3. **Voorwaardelijke aanbeveling met extra bezoek.** Een follow-up audit op locatie is nodig om herstelwerkzaamheden fysiek te bewijzen — dit speelt vaak bij een major.
4. **Onvoldoende.** De audit is niet behaald.

Wie beslist

Het rapport en de aanbeveling van de auditor worden door de certificerende instantie beoordeeld op kwaliteit. Pas als zij vaststellen dat de audit correct is uitgevoerd en zij akkoord gaan met de aanbeveling van de auditor, neemt de certificatie-instelling de officiële certificeringsbeslissing. Zij zijn degenen die uiteindelijk het ISO 27001-certificaat aan jouw organisatie verstrekt.

Als er correctieplannen nodig waren, ontvang je het certificaat nadat die plannen zijn ingediend én goedgekeurd.

Geldigheid

Het certificaat is drie jaar geldig. Maar achterover leunen is er niet bij. Jaarlijks komt de auditor terug voor een surveillance audit — een kleinere toets of het managementsysteem nog effectief wordt onderhouden. In het derde jaar volgt de hercertificeringsaudit.

ISO 27001 is geen eenmalige exercitie. Het is een cyclus. Wie het managementsysteem na de certificering laat versloffen, betaalt daar bij de eerste surveillance audit de prijs voor.

VOLGENDE VRAAG: Hoe verder?

9. Hoe verder?

Een ISO 27001-certificering halen begint niet bij de audit. Het begint bij het bouwen van een managementsysteem dat stevig genoeg is om de audit te doorstaan, en het implementeren van de maatregelen die passen bij jouw organisatie. Dat is waarvoor we **ISO27DIY** hebben gebouwd. Een praktische methode waarmee je — stap voor stap, in een logische volgorde — een audit-waardig ISMS inricht, maatregelen kiest, implementeert en documenteert. Ondersteund door simpele tooling en deskundige mensen. Met alles wat je nodig hebt om je succesvol op de audit voor te bereiden.

Meer weten?

Ga naar <https://iso27diy.com> en bekijk hoe je kunt starten.