Audit ISO 27001

Informatiegids

In deze handige informatiegids lees je alles over wat je als Auditee kunt verwachten van de audit ISO 27001.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Wat kun je verwachten van de ISO 27001 audit?

Na het ISO 27001 traject te hebben doorlopen staat de ISO 27001 audit voor de deur, een spannend moment voor velen! Je wil je natuurlijk goed voorbereiden en hoopt op een positieve uitslag. Maar hoe bereid je je nu goed voor? En wat kun je precies verwachten?
In deze informatiegids nemen we je mee door de audit zodat jij straks optimaal bent voorbereid op de audit en je weet wat je te wachten staat. Veel leesplezier!

In deze whitepaper vertellen we je meer over:

- Wat je kunt verwachten tijdens de interne en externe audit;
- De verschillende audit methodes;
- Verschillende rollen tijdens de audit;
- Verschillende vraagstijlen;
- De auditbevindingen.

Inhoudsopgave

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

1. Wat wordt er van jou als auditee verwacht?

Je bent uitgenodigd als ‘auditee’ (iemand die tijdens een audit vragen beantwoordt). Dat betekent dat je een auditor gaat laten zien hoe je (een deel van je werk) doet. Het doel daarvan is om vast te stellen:

- Of dat is volgens de afspraken binnen jouw organisatie (beleid, richtlijnen, procedures, workflows);
- Of die afspraken kunnen voldoen aan een of meerdere eisen van een norm.

Audits zijn er in meerdere vormen: het meest voorkomende verschil is of de auditor je collega is (interne audit) of een externe. In veel normen zijn overigens zowel interne als externe audits verplicht.

1.1. De afspraak

Dat moment van ‘laten zien’ gaat volgens een auditagenda (hoe laat gaat het, met wie, over welk onderwerp op dag x) en volgt een langer auditprogramma (welk thema komt wanneer aan bod in een cyclus van 3 jaar). De verantwoordelijke voor het auditprogramma zorgt er voor dat de relevante onderwerpen voldoende vaak aan bod komen zodat aangetoond kan worden dat de werking van het hele systeem effectief is en aan de totale norm voldoet.

Als het om een interne audit gaat, stelt een interne verantwoordelijke (hierna “Security Officer”) het programma en de specifieke agenda’s op, op basis van risico’s. Bij een externe audit is dit in samenspraak met de certificerende instelling. Je wordt gekozen voor onderwerpen waar je normaliter zelf (mede)uitvoerder van bent. Diezelfde Security Officer helpt jou natuurlijk (al eerder) op pad (en is zelf ook auditee).

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Lees ook het blogartikel ‘KAM-coördinator of Security Officer? Met deze 7 tips bereid je collega’s voor op de ISO-audit’.

Lees het blogartikel

1.2. Het auditdoel

Het doel van de audit kan per norm verschillen. Een detailvoorbeeld uit de ISO 27001 norm (managementsysteem voor informatiebeveiliging):

De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het management-systeem voor informatiebeveiliging

A) overeenkomt met:

1) de eigen eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging; en

2) de eisen van deze Internationale Norm;

B) doeltreffend is geïmplementeerd en onderhouden. (NEN,2015)

Hieruit is terug te lezen dat een audit op zoek is naar opzet, bestaan én doelmatige werking van het managementsysteem. Qua volwassenheid van het systeem is er sprake van:

- Niets (een onderwerp is geheel leeg);
- Opzet (het is beschreven hoe het zou moeten werken);
- Bestaan (naast een beschrijving zijn er middelen en wordt er iets gedaan);
- Werking (het draagt effectief bij aan de doelstellingen).

Een daar nog op volgend niveau van volwassenheid (ook wel 'maturity') is continue verbetering; dit is een algemeen principe van managementsystemen. Continue verbetering is een meer algemene conclusie van een managementsysteem in de breedte, dus niet iets wat voor elk onderwerp expliciet aan bod hoeft te komen. Wel is het van belang om (eerder) geconstateerde afwijkingen bij een onderwerp effectief op te lossen, dus een dergelijk onderwerp zal dan vaker geauditeerd moeten worden.

Een specifiek audit-onderwerp kan bijvoorbeeld zijn hoe een organisatie omgaat met back-ups (wat, waarom, hoe, hoe lang, waarheen, hoe vaak, is er monitoring op, worden er restore tests gedaan, enz. enz.). Daarvoor kan een audit(or) o.a. kijken naar:

1. Beleid voor back-ups, met verantwoordelijken;
2. Een procesbeschrijving voor de back-ups, of inrichting daar van via een automatische tool met automatisch meldingen via e-mails;
3. De uitvoering (en vastlegging daarvan) van de back-ups én restore-testen daarvan, inclusief eventuele opvolging bij afwijkingen en of deze conform de eigen processen is, en;
4. Of door middel van het uitgevoerde werk het doel, bijvoorbeeld of voor een informatiesysteem het recovery point objective, behaald wordt.

De auditee verstrekt de auditor informatie waarmee de auditor constateert in welke mate dit voldoet. Daarbij is de auditor neutraal. Als de organisatie stelt dat de best mogelijke methode methodeX is, en methodeX voldoet aan de norm, dan is de persoonlijke mening van de auditor over die methode niet relevant. Wel kan de auditor aangeven als iets niet consistent is. Belooft de organisatie via contract aan al haar klanten methodeY, of eist een wet methodeY, dan is er een afwijking als de organisatie in plaats daarvan methodeX toepast.

Naast het bovengenoemde 'uitvoerende' doel van elk auditonderdeel is er het hogere doel. Dat ontstaat uit de eindconclusie en wordt dus meestal per individueel onderwerp besproken:

- zijn we als organisatie in control en hoe verbeteren we? (interne audits);
- voldoet de organisatie dermate dat een onafhankelijk certificaat hiervan afgegeven kan worden (externe audits).

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

2. De auditmethode

Uit de doelstelling en het voorbeeld-bewijs in voorgaand hoofdstuk blijkt al dat auditoren op zoek zijn naar verschillende soorten bewijs. Daar horen dus ook verschillende manieren van onderzoeken bij. De geaccrediteerde certificerende instellingen die externe audits uitvoeren, hebben hier formele spelregels voor (en worden op hun beurt gecontroleerd door de Raad voor Accreditatie).

De principes van de externe audit kunnen ook worden toegepast bij de interne audit. Een verschil daarbij is zoals al genoemd dat er bij een interne audit wél ruimte is voor verbetersuggesties (voor zover er tijd is binnen de planning). Bij externe audit kan de auditee hier beter niet om vragen.

2.1 Bewijsvorming

In principe is een auditor altijd op zoek naar meerdere vormen van bewijs voor elk onderwerp. Neem bijvoorbeeld een onderwerp als "periodieke controles" (vaak geborgd door een operationele planning / actielijst). Daarbij kan hij of zij kijken naar bewijsvormen als:

1. Documenten en registraties

- Document (opzet): Is er een operationele planning en een beschrijving hoe deze aangestuurd en uitgevoerd moet worden?
- Registratie (bestaan): is zichtbaar dat de acties uit de operationele planning zijn uitgevoerd (mogelijk door rapportage) en wordt de planning goed bijgehouden.
- Registratie (werking): waren de acties op tijd? Waren ze effectief (leverden ze nuttige informatie of vervolgmogelijkheden op)?

2. Interviews

- Vertelt de voor de operationele planning verantwoordelijke medewerker dat er "weliswaar een ingevulde planning is, maar dat deze in de laatste maand voor de audit pas ingevuld en uitgevoerd wordt"?
- Geven directie en technisch systeembeheerder dezelfde informatie over het belang van de handelingen op de operationele planning?

3. Observaties

- Wordt één van de acties op de operationele planning, bijvoorbeeld de restore-test van een back-up, uitgevoerd naar een fysiek medium (NAS) in het kantoor, maar ziet de auditor dat deze niet meer aanwezig is in het serverrack waar deze moet staan?

Het bovenstaande voorbeeld van operationele planning is niet toevallig gekozen. Een interne audit is namelijk een hulpmiddel voor een organisatie om te controleren of ze 'in control is'. Het gaat te ver om bij een (ISO) interne audit op alle details uitputtend onderzoek te doen. Het is juist aan de organisatie om die details als onderdeel van het normale werk operationeel te beheersen, want anders gaat er iets mis met de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(systemen). De audit kan controleren of dat proces goed loopt en zal dat ook op basis van steekproeven checken.

Stel een organisatie heeft bijvoorbeeld honderden IT-systemen of applicaties (denk aan een ziekenhuis of een overheidsonderdeel). Dan doet die organisatie bijvoorbeeld zelf op meerdere moment in het jaar controle of er niet te veel toegangsrechten zijn verstrekt of nog actief zijn (en legt dat vast). De audit kan dat dan verifiëren.

In de praktijk betekent dit dat de auditor de auditee vraagt ‘hoe iets werkt’. Het antwoord op een vraag is daarmee gelijk een stukje ‘interview’ en kan uitgediept worden. De auditee laat op een gegeven moment uit zichzelf bewijs zien (“daar hebben we beleidsstuk XYZ” voor” of “kijk, dat doe ik zo”) of de auditor vraagt daar expliciet naar. In een goed ingericht managementsysteem is de auditee bewust van zijn verantwoordelijkheid en taak, dus zal deze eenvoudig op een vraag kunnen reageren met bewijs.

2.2 Vraagstelling

Omdat de audit kijkt naar zowel de norm als de manier waarop een organisatie handelt (zie onderdeel ‘doel’ hierboven) kan een auditor de vraag op verschillende manieren stellen. Zo kan een auditor zeggen:

- “Hoe doen jullie back-ups?” (organisatiegericht) of
- “Hoe ga je om met A.12.3.1?” (de specifieke norm-paragraaf over back-ups).

Een ander voorbeeld van verschillende vraagstijlen is:

- “Hoe hebben jullie bepaald wat meer of minder belangrijk is voor jullie managementsysteem?”. Dat is organisatiegericht en dekt meerdere management-paragrafen uit een norm zoals belangrijke issues, belangen van stakeholders en risicoanalyse.
- “Waarom sluit je paragraaf A.11.1.6 (laad en loslocaties) uit in je verklaring van toepasselijkheid?”. Dit stuurt heel norm gericht op begrip van 6.1.3.e.

Lees ook het blogartikel ‘Hoe gaat een ISO 27001 audit in zijn werk’.

Lees het blogartikel

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Bij een interne audit zijn de vragen vaak meer organisatiegericht, bij een externe audit varieert het tussen organisatie- en normgericht.

De manier waarop de vraag gesteld wordt, kan het best worden aangepast aan de rol en verantwoordelijkheid van de auditee.

2.3. De Security Officer als auditee

Als de Security Officer de auditee is, dan wordt van hem of haar verwacht dat hij de formele normeisen (her)kent en kan een auditvraag open en algemeen gehouden worden. Het antwoord geeft daarmee hopelijk de meest direct relevante en praktische informatie (en mogelijk gelijk antwoord op meerdere punten). De vragen zullen algemeen gesproken gaan over managementprincipes en - hoe groter de organisatie – minder over de technische uitvoering. Een Security Officer (of Security Team) kent de norm en de manier waarop de organisatie die invult. Waarbij dit 'kennen' uiteraard ondersteund kan worden door het eigen systeem: een wandelende encyclopedie is niet nodig. En een Security Officer heeft specialisten in de eigen organisatie om bepaalde thema's uit te leggen (bijvoorbeeld waarom een bepaald niveau van encryptie wordt toegepast).

2.4. De Technisch Beheerder als auditee

Als de (technisch) beheerder van een belangrijk informatiesysteem geauditeerd wordt, dan is A tot Z kennis van alle onderdelen van een norm en het managementsysteem minder belangrijk. De auditee moet wel weten dat er een managementsysteem is waarin hij de zaken die hij niet dagdagelijks doet op kan zoeken (of collega's als de security officer waar hij dingen aan kan vragen), bijvoorbeeld een procedure voor vernietigen van harde schijven. Het gaat er met name om: is duidelijk welke uitvoerende activiteiten hij (voor zover relevant voor informatiebeveiliging) moet doen, hoe, wat het gewenste resultaat is, en wordt het resultaat gehaald.

Hoe kleiner de organisatie, hoe meer rollen of onderwerpen binnen 1 persoon samenkomen, dus hoe meer vragen er aan die persoon gesteld kunnen worden.

3.1 Algemene regels

Daarnaast gelden er natuurlijk algemene regels, bijvoorbeeld:

- Dat incidenten gemeld moeten worden;
- Dat je voorzichtig bent met verdachte e-mails en hoe iemand omgaat met zijn laptop. Laptop van directeur, receptie en soft wareontwikkelaar moeten allemaal veilig zijn;
- Dat medewerkers op de hoogte worden gesteld van de doelen van het managementsysteem.

Die vragen kunnen dus aan iedereen gesteld worden.

Lees ook het blogartikel 'Het verschil tussen interne en externe audit?

Lees het blogartikel

3. De auditbevindingen

Hoe meer en makkelijker de auditee weet wat het doel van de vraag of het onderwerp is, hoe makkelijker hij of zij vertelt, en hoe makkelijker het duidelijk wordt hoe het systeem werkt en hoe doeltreffend het is. Dat kan een hoop detailvragen en gezoek schelen. En, niet onbelangrijk, dit leidt in de praktijk van elke dag tot het juiste gedrag.

Als de auditee bijvoorbeeld een beleid en procesbeschrijving laat zien, voordoet hoe een handeling gaat en de bijbehorende registratie volledig en consistent is, dan zal de auditor waarschijnlijk bedanken voor het antwoord (de bevinding is dan “voldoet”) en doorgaan naar het volgende onderwerp.

Wat als dat niet zo makkelijk loopt? In eerste instantie kan dat. Mensen worden niet dagelijks geaudit, dus enige onwennigheid kan er zijn, dus daar houdt de planning rekening mee.
Als het alsnog niet lukt: een verwacht beleidsstuk is, ook met navragen bij een collega, geheel niet te vinden. Of het beleid is er wel maar de back-up wordt in de praktijk nooit uitgevoerd. Dan is er een negatieve bevinding of te wel een afwijking.
Dat kan een kleine bevinding zijn (het onderdeel van het systeem bestaat en wordt uitgevoerd, maar niet helemaal volgens de regels) of een grote (een belangrijk onderdeel ontbreekt bijvoorbeeld
helemaal, zoals een directiebeoordeling). Bij een kleine bevinding wordt doorgevraagd of er een onderliggende oorzaak is. Het is belangrijk om te duiden of er iets misgaat op een uitvoerend detail of dat de gekozen werkwijze geheel niet aansluit bij het te beheersen risico voor de organisatie.

Bevindingen worden tijdens de audit teruggekoppeld aan de auditee zodat deze de logica van de auditor snapt en eventueel kan corrigeren. Dit is dus ook zeker een moment waar je als auditee aan kan geven als die logica niet klopt, of dat er misschien nog andere feiten zijn die meegenomen moeten worden.

Het lijkt voor de hand liggend, maar voor auditees is het goed om te weten: er wordt gezocht naar feiten, niet fouten. Een (goede) auditor is niet op zoek naar zoveel mogelijk afwijkingen, maar geeft weer wat goed en niet goed gaat. Het is wel een gemiste kans (en opmerkelijk) als er geen enkele afwijking of verbetersuggestie uit een audit komt.
Voor organisaties die al lange tijd een stabiel systeem hebben (of uit willen gaan van het positieve) is een
nieuwe trend het ‘waarderend auditen’. Dit zoekt
positieve punten en probeert deze te versterken.

Meer weten over waarderend auditen?

Lees het blogartikel ‘Training waarderend auditen, een nieuw perspectief’

Lees het blogartikel

4. Na de audit

Logischerwijs zal bij het opvolgen van bevindingen na de audit, de auditee ook betrokken worden. De auditor maakt zijn rapport en deelt het met de organisatie - in ieder geval de Security Officer. Deze volgt de auditbevindingen op. Logischerwijs zullen de auditees (en hun teams / afdelingen) hierbij ook betrokken worden. Afhankelijk van de aard van de bevindingen en de soort audit kan het nodig zijn dat er een aanvullende audit volgt. Deze zal dan controleren of de getroffen maatregelen effectief zijn. Door deze opvolging wordt de prestatie van de organisatie beter - en is informatie dus beter beschikbaar, integer en vertrouwelijk.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

CERTIFICERINGSADVIES NEDERLAND

JOUW PARTNER IN CERTIFICEREN

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Heb je interesse in begeleiding naar de ISO 27001 audit of wil je een interne audit door ons laten uitvoeren? Wil je graag meer weten over de mogelijkheden en bijbehorende kosten? Neem dan gerust contact met ons op. Wij vertellen je graag meer!

CertificeringsAdvies Nederland is de partner in certificeren. Wij ondersteunen mensen en organisaties in hun ontwikkeling. Zo helpen wij jou met je organisatie slim in te richten en zijn we een inspiratiebron voor de mensen binnen je organisatie. Dat doen we door advies-, opleidings- en outsourcingsdiensten aan te bieden binnen de thema's Kwaliteit, Arbo & Veiligheid, Milieu & MVO, Voedselveiligheid en Informatiebeveiliging.

Meer weten?

Kijk op www.certificeringsadvies.nl
T 085 4879972
E info@certificeringsadvies.nl