ISO 27001
De meest gestelde vragen

Alle antwoorden op de meest gestelde vragen rondom ISO 27001

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Inleiding

Wil je een ISO 27001 certificering behalen met jouw organisatie? Dan heb je ongetwijfeld een heleboel vragen. Bijvoorbeeld over de inhoud, voordelen en eisen van de norm, over het proces op weg naar certificering en over het kostenplaatje. Om die reden hebben wij bij CertificeringsAdvies Nederland een hele reeks aan veel gestelde vragen overzichtelijk gebundeld in deze handige gids. Zo krijg je een indruk van wat een certificeringstraject op weg naar ISO 27001 inhoudt. En mocht je nog meer vragen hebben? Schroom dan niet om contact met ons op te nemen. Onze adviseurs informatiebeveiliging vertellen je er graag meer over!

Inhoudsopgave

CertificeringsAdvies NEDERLAND advies, opleiding & outsourcing

1. Wat is ISO 27001?

Informatie en kennis zijn in principe het belangrijkste bezit van een bedrijf. Daarom is het zaak om dat goed te beveiligen. De ISO 27001 norm is een internationaal erkende norm op het gebied van informatiebeveiliging. Het is nog altijd de snelst groeiende norm van dit moment. In de norm staat beschreven hoe je als organisatie informatiebeveiliging procesmatig in kunt richten. Door het behalen van een ISO 27001 certificering maak je als organisatie aantoonbaar dat je voldoet aan alle eisen en dat je maatregelen hebt getroffen tegen informatiebeveiligingsrisico's.

Definitie

informatiebeveiliging is het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarnaast kunnen ook andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid hierbij een rol spelen.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

2. Wat zijn de voordelen van ISO 27001?

ISO 27001 is steeds vaker een eis bij aanbestedingen. (Potentiële) klanten willen immers voorkomen dat vertrouwelijke informatie op straat komt te liggen en daarom eisen ze dat er zorgvuldig wordt omgegaan met hun gegevens. Een ISO 27001 certificaat is het objectieve en onafhankelijke bewijs waarmee je als organisatie aantoont dat je serieus en structureel bezig bent met informatiebeveiliging. Dit versterkt de vertrouwensband met je (potentiële) klant. Wanneer je in het bezit bent van een ISO 27001 certificaat, versterkt dat tevens je imago. Een certificering biedt dan ook veel commerciële kansen; je onderscheidt jezelf ermee van je concurrentie.

Niet alleen naar buiten toe is een ISO 27001 certificering een groot pluspunt. Een certificering is ook ondersteunend aan je organisatie. Het helpt je bij het bepalen van je beleid en procedures en bij het behalen van je doelstellingen. Je bent in staat om je klanten beter te bedienen en het zorgt voor structuur en professionalisering in je organisatie. Bovendien voldoe je met een ISO 27001 certificaat voor een groot deel aan de relevante wet- en regelgeving op het gebied van informatiebeveiliging. Tot slot verklein je de kans op datalekken waardoor ook de kans op imagoschade afneemt.

3. Hoelang duurt ISO 27001 certificering?

Het is vooraf erg lastig te zeggen hoelang een ISO 27001 certificering precies duurt. De snelheid van implementatie van de norm is namelijk afhankelijk van diverse factoren:

- De huidige stand van zaken binnen de organisatie;
- De aanwezige organisatorische, technische en fysieke beheersmaatregelen;
- De complexiteit van de organisatie;
- De grootte van de organisatie;
- De interne capaciteit en slagkracht van de organisatie.

Wanneer je als bedrijf je bedrijfsprocessen helder in kaart hebt, dan gaat het ISO 27001 traject natuurlijk sneller dan wanneer je vanaf nul moet beginnen.

Daarnaast scheelt het ook weer als er al andere ISO-normen, zoals de ISO 9001 norm, op basis van de High Level Structure (HLS) zijn geïmplementeerd binnen je organisatie waar dan weer verder op gebouwd kan worden. Kortom, hoe meer er al is en des te minder complex de organisatie in elkaar steekt, des te sneller het ISO 27001 traject doorlopen kan worden.

Op basis van onze ervaring kunnen we bij CertificeringsAdvies Nederland wel een indicatie geven van de doorlooptijd. Voor een ISO 27001 certificeringstraject wordt een minimale doorlooptijd van 5 tot 6 maanden aangehouden. Bij grotere organisaties kan het zomaar 8 tot 12 maanden duren.

4. Wat kost ISO 27001?

De kosten van een ISO 27001 certificering worden bepaald aan de hand van een aantal factoren. ISO 27001 trajecten zijn doorgaans de projecten die wat meer kosten met zich meebrengen (dan bijvoorbeeld ISO 9001). Dit komt omdat organisaties steeds afhankelijker worden van hun kennis en informatie. ISO 27001 geeft richtlijnen om die informatie te kunnen beveiligen. Doordat de waarde van kennis en informatie steeds groter wordt, worden anderzijds de risico's ook groter. Wil je de informatiebeveiliging goed op orde hebben, dan moet je als organisatie een complexer traject door dan bijvoorbeeld bij een ISO 9001 certificering. Dat brengt dus ook een ander kostenplaatje met zich mee.

Daarnaast speelt in het kostenplaatje natuurlijk ook mee wat de huidige stand van zaken is en wat het doel is van de certificering. Heb je al een managementsysteem met de vereiste onderdelen van de High Level Structure (HLS), omdat je bijvoorbeeld al ISO 9001 gecertificeerd bent, of moet je vanaf de basis beginnen? En heb je jouw processen al in kaart gebracht of sta je nog aan het begin van dat proces? Allemaal vragen die van invloed zijn op de uiteindelijke kostenbepaling. Verder spelen ook de complexiteit van de organisatie en de bijbehorende processen een grote rol in het bepalen van de kosten voor ISO 27001. Een klein bedrijf zit immers eenvoudiger in elkaar dan een grote organisatie.

Dan komen we bij de laatste set factoren die van invloed zijn op de kosten, namelijk de mate van begeleiding van een adviesbureau en de keuze voor de certificerende instantie. De ene organisatie wil graag intensieve begeleiding van een adviesbureau, waar een andere organisatie voldoende heeft aan coaching op hoofdlijnen. Tot slot spelen de kosten van de certificerende instantie een rol. Je dient een dergelijke instantie in te schakelen, omdat zij de audit uit mogen voeren (en dat mag het adviesbureau niet). De ene instantie is echter de andere niet; de kosten verschillen per instantie. Vraag daarom altijd een aantal offertes op ter vergelijking.

5. Welke stappen moet ik doorlopen voor ISO 27001?

Het ISO 27001 traject bestaat uit twee fasen met in beide fasen een aantal te doorlopen stappen:

Fase	Stap	Activiteit
Fase 1	1	Algemene inventarisatie van de organisatie (werkwijze, beschikbare informatie, infrastructuur, etc.) + scope bepaling.
	2	Uitvoeren contextanalyse (in kaart brengen van stakeholders en relevante risico's/ kansen)
	3	Uitvoeren risicoanalyse o.b.v. de ISO 27001/NEN7510-normelementen (zie o.a. Annex A van de norm)
	4	Opstellen Plan van Aanpak (vaststellen benodigde maatregelen en eisen aan het managementsysteem, afstemmen actieplan)
Fase 2	5	Aanscherpen contextanalyse
	6	Beleidscyclus: vaststellen proces van bepalen beleid/ doelstellingen, vertaling naar organisatie en bewaking hiervan.
	7	Uitvoeren Plan van Aanpak
	8	Borging en Implementatie: gemaakte afspraken en procedures vastleggen in het managementsysteem en implementeren binnen de organisatie.
	9	Interne audit: uitvoeren interne audit ter controle van een effectieve implementatie en ter voorbereiding op de certificeringsaudit.
	10	Certificering: de certificering wordt uitgevoerd door een erkende certificerende instantie.

6. Wat houdt de risicoanalyse in ISO 27001 in?

In de ISO 27001 norm speelt de risicoanalyse een belangrijke rol. Met de ISO 27001 risicoanalyse kun je perfect beoordelen in hoeverre de beveiliging binnen je organisatie op een acceptabel niveau is. Daarvoor is het wel noodzakelijk dat je jouw processen in kaart hebt gebracht en weet waar de risico's liggen. Daarnaast is het makkelijk als je de scope al hebt bepaald en als het informatiebeveiligings-beleid is vastgesteld. De ISO 27001 risicoanalyse wordt uitgevoerd met behulp van een zogenaamde 'uitleg op de ISO 27001 norm', ofwel de ISO 27002. Deze ISO 27002 norm is een lijst met veelvoorkomende risico's, referentiebeheerdoelstellingen en maatregelen. Om een goede risicobeoordeling uit te voeren loop je deze lijst door en bepaal je welke risico's op je organisatie van toepassing zijn. Het is cruciaal om passende maatregelen te nemen voor specifieke risico's binnen jouw organisatie. Deze maatregelen zijn gebaseerd op best practices, waardoor ze gemakkelijk in de praktijk toe te passen zijn.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

7. Wat is een ISMS?

ISMS staat voor Information Security Management System, ofwel een managementsysteem voor informatiebeveiliging. Een ISMS sluit aan bij het beleid en de strategie van de organisatie en dient geïntegreerd te worden in de huidige processen. Het doel van het ISMS is (vertrouwelijke) informatie beter beveiligen. Een ISMS is geen softwaretool, maar een continu verbeterproces. Het is een manier van werken waarbij een systematische aanpak wordt gehanteerd om (vertrouwelijke) informatie te managen, zodat de veiligheid ervan wordt geborgd.
Uiteindelijk leg je in een ISMS je complete set aan beheersmaatregelen, processen en procedures vast met betrekking tot informatiebeveiliging om zo de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie te controleren. Het ISMS bevat controles waarmee je de risico's die voortkomen uit de risicoanalyse en die gerelateerd zijn aan mensen, processen en systemen beheersbaar maakt.

Meer informatie over een ISMS?

Lees het artikel 'Wat is een ISMS'

8. Hoe bepaal je een ISO 27001 scope?

Het bepalen van de ISO 27001 scope is erg belangrijk. Het bepalen van het doel en de scope is doorgaans vaak de eerste stap die je uitvoert als je aan de slag gaat met ISO 27001. De scope duidt in algemene zin de aard, de grootte en kaders van het project aan. De scope maakt dus duidelijk wat er wel en wat er niet binnen het project en de certificering valt. Bij een ISO 27001 scope kader je af welke informatietypen en bedrijfsonderdelen binnen het informatiebeveiligingssysteem (ISMS) vallen. Een goed afgebakende scope zorgt voor duidelijkheid, richting en focus. Als organisatie ben je verantwoordelijk voor het beschermen van alle informatie die binnen de scope valt.

Meer informatie over de scope?

Lees het artikel ‘De ISO 27001 scope bepalen’

9. Is ISO 27001 verplicht?

Voldoen aan de ISO 27001 norm is geen wettelijke verplichting vanuit de Nederlandse of de Europese wetgeving. Wat wel verplicht is vanuit de wetgeving, is voldoen aan de Algemene Verordening Gegevensbescherming. Deze twee zaken moeten echter niet door elkaar gehaald worden. Voor meer informatie over de relatie tussen ISO 27001 en de AVG zie vraag 11 in dit document.

Wanneer je als organisatie met de ISO 27001 norm aan de slag gaat om uiteindelijk gecertificeerd te worden, dan dien je te voldoen aan de eisen die gesteld worden in de norm. Eén van die eisen is dat er een procedure wordt geïmplementeerd die beschrijft hoe er om wordt gegaan met datalekken. Vanuit de AVG-wet ben je als organisatie verplicht om een datalek te melden.

Het is overigens niet helemaal waar dat ISO 27001 niet verplicht is. Voor rijksoverheid, waterschappen en gemeenten is hetnamelijk wel verplicht om de informatiebeveiliging op orde te hebben. Dit is een zogenaamd BIO-traject dat gebaseerd is op ISO 27002. Per 1 januari 2020 moeten alle overheidsorganisaties voldoen aan aan de Baseline Informatiebeveiliging Overheid - BIO. Daarnaast moeten zorgorganisaties wettelijk voldoen aan de van ISO 27001 afgeleide NEN 7510 norm. Voor meer informatie over ISO 27002, zie vraag 10 in dit document.

10. Het verschil tussen ISO 27001 en 27002, hoe zit dat?

Wanneer je met ISO 27001 aan de slag gaat, dan kom je automatisch ook in aanraking met ISO 27002. Beide normen zijn weliswaar normen voor informatiebeveiliging, maar je kunt je als bedrijf enkel laten certificeren voor ISO 27001. ISO 27002 is een verdieping op ISO 27001. Met behulp van de ISO 27002 norm wordt de risicoanalyse die je verplicht dient uit te voeren voor de ISO 27001 norm uitgevoerd. Deze ISO 27002 norm bestaat uit een lijst met veel voorkomende risico's, referentiebeheer-doelstellingen en -maatregelen. Je loopt door de lijst om te bekijken welke risico's van toepassing zijn op jouw organisatie. Vervolgens dien je daarvoor passende maatregelen te nemen.

11. Wat is de relatie tussen ISO 27001 en de AVG?

ISO 27001 is de norm voor informatiebeveiliging, waar de Algemene Verordening Gegevensbescherming (AVG) de wet is voor bescherming van persoonsgegevens. In feite kun je stellen dat de ISO 27001 norm met de komst van de AVG naar een hoger niveau is getild. Privacy en informatiebeveiliging gaan namelijk hand in hand. ISO 27001 is een uitstekende manier om de veiligheid van kennis en informatie te borgen, maar het is niet zo dat wanneer je ISO 27001 gecertificeerd bent, dat je dan ook voldoet aan de AVG. Het ISMS is echter wel een goed hulpmiddel. Wanneer het je lukt om de regels van de AVG-wet te borgen in een Information Security Management System (ISMS), dan sla je twee vliegen in één klap. . Dit kan o.a. door het invoeren van een ISO 27701 (Privacy Information Management) Systeem.

CERTIFICERINGSADVIES NEDERLAND

JOUW PARTNER IN CERTIFICEREN

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Heb je vragen over ISO 27001 of informatiebeveiliging? Of wil je hier graag meer over weten? Neem dan contact op met CertificeringsAdvies Nederland.

Deze whitepaper is geschreven door CertificeringsAdvies Nederland. Als Partner In Certificeren helpen wij organisaties met advies, opleiding en outsourcing binnen de thema's Kwaliteit, Arbo en Veiligheid, Milieu en MVO, Informatiebeveiliging en Voedselveiligheid.

Meer weten?

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