De ultieme toolkit voor

ISO 27001 certificering

Inhoud

ISO 27001: wat is het?

Het is tegenwoordig ondenkbaar dat een onderneming zonder het gebruik van informatietechnologie kan overleven in de veranderlijke en concurrerende wereldmarkt. Informatietechnologie is nodig voor een snelle en accurate verwerking en uitwisseling van data in het kader van zakelijke transacties. Informatiebeveiliging is daarmee uitgegroeid tot een randvoorwaarde voor zakelijk succes. Managers en beveiligingsprofessionals moeten zich aan deze nieuwe situatie aanpassen en de juiste maatregelen treffen om risico's effectief te kunnen identificeren, analyseren en beheren, ongeacht de sector waarin hun organisatie actief is. Laat zien dat uw organisatie de beveiliging van (vertrouwelijke) informatie volledig beheerst door het behalen van de internationaal erkende certificering en het keurmerk van DEKRA. Daarmee geeft u het vertrouwen van klanten, zakelijke partners en stakeholders een boost.

Wat is ISO 27001?

ISO 27001 is een internationale norm voor de toepassing van maatregelen voor informatiebeveiliging binnen organisaties. Deze norm is gepubliceerd door de International Organization for Standardization (ISO) en is uitgegroeid tot een wereldwijd erkende norm.

Voor wie is ISO 27001?

ISO 27001 is geschikt voor organisaties in elke sector, aangezien vrijwel elke onderneming tegenwoordig gebruikmaakt van vertrouwelijke en privacygevoelige informatie. Deze informatie bevindt zich tegenwoordig hoofdzakelijk binnen IT-systemen, waardoor adequate (IT-)beveiliging van groot belang is. De eisen van ISO/IEC 27001 zijn dan ook toepasbaar op bedrijven van elke omvang in elke sector.

De voordelen van ISO 27001

ISO 27001-certificering biedt tal van voordelen:

- U identificeert en reduceert bedreigingen voor uw organisatie;
- U beheert zakelijke en aansprakelijkheids-risico's;
- U houdt vertrouwelijke data en informatie veilig;
- U verzekert zich van het vertrouwen van klanten en zakelijke partners;
- U vergroot uw concurrentievermogen;
- U voldoet aan de eisen van uw stakeholders.

Wat is informatiebeveiliging?

Informatiebeveiliging dient als preventief mechanisme dat data en informatie van organisaties beschermt tegen schade en bedreigingen. In praktijk bewezen technische en organisatorische maatregelen, die in branchenormen zijn vastgelegd, kunnen zwakke punten en beveiligingslekken identificeren. Daarna kunnen deze punten op passende wijze worden verholpen. De drie kerndoelstellingen van informatiebeveiliging zijn:

- **Vertrouwelijkheid**: het beschermen van gevoelige informatie tegen onbevoegde toegang.
- **Integriteit**: het minimaliseren van risico's en waarborgen van de volledigheid en juistheid van data en informatie.
- **Beschikbaarheid**: het waarborgen van betrouwbare toegang tot informatie en informatiesystemen voor bevoegde personen.

Bereid uw organisatie voor op de vijf grootste bedreigingen

- Menselijke fouten: onbedoeld delen van informatie, het kwijtraken van hardware en documenten met gevoelige informatie, etc.;
- Besmetting met malware via het internet;
- De introductie van malware via verwijderbare gegevensdragers, zoals USB-sticks en cd's;
- Social engineering: technieken die (cyber)criminelen gebruiken om mensen te verleiden persoonlijke of bedrijfsgevoelige gegevens prijs te geven;
- Het lamleggen van IT-systemen door cybercriminelen die zogenaamd 'oplossingen voor onderhoud op afstand' bieden.

Met een effectief managementsysteem voor informatiebeveiliging (ISMS) kan uw organisatie zwakke punten in de beveiliging van vertrouwelijke informatie identificeren. Vervolgens kunt u maatregelen ontwikkelen die bescherming bieden tegen deze en andere cyberbedreigingen en die maatregelen in de praktijk toetsen.

ISO 27001 in relatie tot **NIS2**

NIS en NIS2: cybersecurity van netwerk en informatiesystemen

NIS en NIS2 stellen eisen aan de cybersecurity van informatie- en IT-systemen. NIS staat voor netwerk- en informatiesystemen. Deze wetgeving heeft betrekking op organisaties die 'essentiële diensten' leveren, zoals zorginstellingen en telecom- en energiebedrijven. De originele richtlijn stamt uit 2016. Met het ingaan van NIS2 in 2023, zijn meer organisaties aangemerkt als aanbieders van essentiële diensten. Hierbij gaat het onder andere om voedselproducenten, post- en koeriersbedrijven en overheidsdiensten.

Organisaties die onder NIS/NIS2 vallen, moeten de risico's op het gebied van cybersecurity in leveranciersrelaties en de toeleveringsketen in kaart brengen en daar adequate beveiligingsmaatregelen voor nemen.

ISO 27001

Om aan de NIS-richtlijn te voldoen, is de ISO 27001-standaard een goed handvat. Hiermee geeft u uw managementsysteem voor informatiebeveiliging op een gestructureerde manier vorm. DEKRA Audit certificeert u graag tegen ISO 27001.

Online training ISO 27001

Leer direct over de nieuwste versie van de norm

De ISO 27001:2022-training van DEKRA is een online training en volledig up-to-date volgens de nieuwste versie van de norm. De training is speciaal ontwikkeld voor managers, security officers, consultants en auditoren die werken met de norm. De training helpt u om de norm ISO 27001 te begrijpen en leert u hoe u op basis van de norm concrete maatregelen neemt om digitale systemen en informatie binnen uw organisatie te beveiligen. Na deze online ISO 27001-training weet u wat er nodig is om maatregelen te nemen voor de beveiliging van vertrouwelijke informatie binnen uw organisatie. Schrijf u via onderstaande button in voor deze training.

ISO 27001 training ›

Certificering in **7 stappen**

Wilt u zeker weten dat u het maximale uit uw informatiebeveiligingsmaatregelen haalt? DEKRA verzorgt graag de ISO 27001-audit van uw informatiebeveiligingsmanagementsysteem. Onze auditoren voeren daarvoor audits uit op de processen en de specifiek voor uw organisatie van toepassing zijnde maatregelen. Zo krijgt u altijd een ISO 27001-certificering op maat. Naast onze gepersonaliseerde aanpak hanteren wij een standaard werkwijze en bestaat het certificeringsproces uit 7 stappen.

Onze werkwijze: **People Based Auditing**

Wat maakt DEKRA uniek? In ons auditproces hebben we altijd aandacht voor de menselijke factor. Want dankzij onze ruime ervaring weten wij; het zijn de mensen in uw organisatie die van doorslaggevend belang zijn als het gaat om invulling geven aan processen, systemen en werkwijzen.

We noemen onze werkwijze **People Based Auditing**. Een werkwijze die al jarenlang zeer hoog gewaardeerd wordt door onze certificaathouders. Het is inmiddels een standaard onderdeel binnen audits. Aspecten als gedrag en bewustwording van medewerkers zijn daarom een belangrijk uitgangspunt tijdens de ISO 27001-certificering.

Zo gaan we samen met u een stap verder dan de standaard normering. U komt te weten of uw organisatiecultuur echt aansluit op de gewenste processen.

Gedrag is de bepalende factor voor succes. Met People Based Auditing krijgt u inzicht in deze factor. Hiermee gaat het managementsysteem (nog meer) leven binnen uw organisatie en onder uw medewerkers.

People Based Auditing in de praktijk

Een ISO 27001-certificering volgens onze unieke People Based Auditing werkwijze betekent voor uw organisatie dat:

- onze auditoren de tijd nemen om zich te verdiepen in uw organisatie, uw unieke wensen en behoeftes;
- u gedurende het gehele proces een vast aanspreekpunt heeft;
- we u zo goed mogelijk voorbereiden op het certificeringstraject;
- er meer bewustwording is in de kwaliteit van dienstverlening.

Uw ISO 27001-certificering in **7 stappen**

1 Kennismaking

We komen graag bij u op bezoek, of nemen contact op via Teams óf telefonisch. Tijdens de kennismaking bespreken we het proces van een ISO 27001-certificering. Hierna bereidt u uw organisatie voor op de ISO 27001 audit.

2 Audit op uw locatie

Onze auditoren voeren een audit uit bij u op locatie. Hierbij beoordelen en toetsen we de werking van het managementsysteem. We controleren of deze werkt zoals beschreven in het managementsysteem van uw organisatie. Uw organisatie dient aantoonbaar te maken dat u hierover zelf in controle bent. Is dit niet aantoonbaar, dan kan het nodig zijn om de corrigerende maatregelen vervolgens te toetsen.

3 Verslag en evaluatie

Onze lead-auditor deelt het auditverslag. Hierin vindt u alle resultaten van de audit.

4 ISO 27001-certificering

Na succesvolle afronding ontvangt u uw ISO 27001 certificaat. Het certificaat is maximaal drie jaar geldig.

5 Eerste vervolgaudit

Binnen een jaar houden we een vervolgaudit. Daarin beoordelen we of uw managementsysteem nog steeds werkt volgens de norm.

6 Tweede vervolgaudit

Ongeveer een jaar later houden we een tweede vervolgaudit. We beoordelen opnieuw of uw managementsysteem volgens de norm werkt.

7 Hercertificering

In het derde jaar na de ISO 27001-certificering plannen we een audit voor hercertificering. In het geval de hercertificering met een positief resultaat wordt afgerond, wordt het certificaat opnieuw voor een periode van drie jaar verlengd. Na hercertificering volgt de jaarlijkse auditcyclus.

☑ ISO 27001 **checklist**

Met onze checklist komt u er snel en eenvoudig achter of uw organisatie goed is voorbereid op certificering volgens ISO/IEC 27001. De lijst is gerangschikt volgens de basisstructuur van managementsysteemnormen.

Als u een vraag met ja kunt beantwoorden, markeer deze dan met een vinkje. Zo kunt u direct zien welke onderdelen van uw organisatie al voldoen aan de ISO 27001-certificeringseisen, en welke onderdelen nog meer aandacht vereisen.

Context van de organisatie

- ☐ U hebt de structuur van uw organisatie in kaart gebracht (bijv. in de vorm van een organigram).
- ☐ U hebt het toepassingsgebied van uw ISMS (Information Security Management System) gedefinieerd (in het bijzonder voor stakeholders).
- ☐ U hebt een verklaring van toepasselijkheid opgesteld die de beslissingen ten aanzien van het treffen van maatregelen documenteert, evenals de redenen voor deze beslissingen.
- ☐ U hebt een omgevingsanalyse uitgevoerd voor de integratie van het ISMS binnen uw organisatie.
- ☐ U hebt een behoefteanalyse uitgevoerd voor de verschillende groepen stakeholder.
- ☐ U hebt een overzicht samengesteld van alle relevante juridische, wettelijke en contractuele eisen die van invloed zijn op uw strategie voor informatiebeveiliging en het ISMS.

Management

- ☐ U hebt de zakelijke doelstellingen en eisen ten aanzien van het interne beleid voor informatiebeveiliging duidelijk gedefinieerd en gedocumenteerd.
- ☐ U hebt een concrete strategie voor informatiebeveiliging gedefinieerd.
- ☐ U hebt uw topkader gedefinieerd: deze groep is verantwoordelijk voor het beheer van het ISMS van uw organisatie en bepaalt de manier waarop mensen en middelen worden ingezet.
- ☐ U hebt een beleid voor informatie-beveiliging geïmplementeerd.

Planning

- [ ] U beschikt over een gedocumenteerde procedure voor risicobeoordeling.
- [ ] U beschikt over uitgebreide documentatie over het proces voor risicobeoordeling en het plan/proces voor risicobeheer.
- [ ] U beschikt over alle gegevens en resultaten van uw risicobeoordelingen en -analyses.
- [ ] U hebt alle gegevens en resultaten voor het risicobeheer gedocumenteerd.
- [ ] U hebt alle veiligheidsdoelstellingen voor uw organisatie en stakeholders gedefinieerd.

Support

- [ ] U beschikt over een strategie voor de omgang met de gedocumenteerde informatie.
- [ ] U bent in staat om het personeel en de infrastructuur beschikbaar te stellen die nodig zijn voor de implementatie en het beheer van het ISMS.
- [ ] U hebt een procedure voor interne en externe communicatie gedefinieerd.
- [ ] U hebt documentatie opgesteld voor het bewustwordings- en trainingsconcept voor het ISMS.
- [ ] U beschikt over trainingsdocumenten voor het ISMS en bewijs dat uw werknemers hebben deelgenomen aan relevante training.
- [ ] U beschikt over een communicatieplan of -matrix voor het documenteren van alle communicatie binnen uw onderneming die betrekking heeft op de informatiebeveiliging.
- [ ] U hebt gedetailleerde beschrijvingen opgesteld van de rollen van medewerkers op wie het ISMS van toepassing is (zoals de information security board, de CISO of de data security board) en kunt bewijzen dat u hun competenties hebt geverifieerd.

Operatie

- [ ] U beschikt over documentatie over interne auditprogramma's en auditresultaten.
- [ ] U beschikt over uitgebreide documentatie over de structuur voor het meten van alle key performance indicators (KPI's), de meetresultaten en managementverslagen over de escalatie van problemen.
- [ ] U hebt een Incident Response Plan (IRP) opgesteld dat een actuele lijst van contactpersonen en escalatieplannen omvat.
- [ ] U beschikt over bewijs van het feit dat de processen rond het ISMS correct zijn uitgevoerd, dat het ISMS wordt beheerd en dat de prestaties ervan worden gemeten.
- [ ] U beschikt over bewijs van vormen van niet-naleving, van alle toegepaste reactieve maatregelen en van de resultaten van alle toegepaste corrigerende maatregelen.
- [ ] U beschikt over een overzicht van de resultaten van risicobeoordelingen (zoals risicobeoordelingsverslagen en belangrijke risicocijfers) en het risicobeheer (zoals testrapporten en verslagen van penetratietests).
- [ ] Uw documentatie omvat gedragsregels ten aanzien van onregelmatigheden die relevant zijn voor de beveiliging, procesbeschrijvingen en werkinstructies voor het verkrijgen van bewijsmateriaal en rapportage over incidenten op het gebied van informatiebeveiliging.

Meer weten over **ISO 27001?**

Onze experts informeren u graag over de introductie van een informatiebeveiliging managementsysteem dat voldoet aan alle eisen van ISO 27001. Vraag eenvoudig online een informatief gesprek aan, vraag direct een offerte aan, of bezoek onze website voor meer informatie over een ISO 27001-certificering.

ISO 27001 offerte ›

DEKRA Audit
Meander 1051
6825 MJ Arnhem
salesaudit.nl@dekra.com
+31 88 96 83016

Over **DEKRA Audit**

Proactief. Zorgvuldig. Visionair. Of u nu behoefte hebt aan efficiëntere bedrijfsprocessen, betrouwbaardere producten en systemen voor internationaal marktsucces of gekwalificeerde auditoren, met ruim duizend specialisten in alle delen van de wereld kan DEKRA Audit u voorzien van uitgebreide diensten.

Onze dienstverlening beslaat alle aspecten van kwaliteit en prestaties, veiligheid en gezondheid, duurzaamheid en verantwoord ondernemen. Circa 30.000 bedrijven in ruim 50 landen maken al gebruik van onze certificeringen, tests en inspecties om hun doelstellingen snel en soepel te realiseren.

Lees meer over ons op **dekra.nl**

Alle audits & keurmerken ›

Onze werkwijze ›

Alle diensten van DEKRA ›

Certificeringen en keurmerken **DEKRA Audit**

Voor welke audits kunt u bij ons terecht? Bekijk hier een greep uit ons portfolio:

- Amusementcentra
- AQAP
- Assessment Services
- Better Biomass
- BORG E
- BRL 100
- BRL 6000
- BRL 6000-25
- CCV Pentesten
- CO2-Prestatieladder
- CO2-Reductiemanagement
- Dubbeltellingverificatie
- HKZ
- IACS QSCS
- Inboekverificatie
- ISAE 3402 / 3000
- ISCC Corsia
- ISCC EU
- ISCC Plus
- ISO 27701
- ISO 45001
- ISO 55001
- ISO 9001
- ISO/IEC 2000-1
- Keurmerk beveiliging
- MedMij
- MVO Prestatieladder
- NEN-EN 15224
- NEN 7510
- NTA 8009
- NTA 8080
- NVKL kwaliteitslabel
- Prestatieladder Socialer Ondernemen
- Regeling brandmeldinstallaties
- Regeling Ontruimingsinstallaties
- Safety Culture Ladder
- SCIOS
- SERMI
- TX-Keur
- VCA