Step-by-step Guide

ISO 27001 Certification.

Inhoud

Kennismaken met de ISO 27001 Norm

In deze whitepaper geven we u de nodige informatie over de ISO 27001 norm. De whitepaper bestaat uit informatie over de ISO 27001 norm, de projectfasen van de ISO 27001 certificering en de voordelen van de ISO 27001 norm voor uw organisatie.

Als professioneel Risk Management Governance en Compliance bedrijf bieden wij u graag ondersteuning bij het ISO 27001 certificeringstraject binnen uw organisatie. We beantwoorden graag uw vragen over de ISO 27001 norm.

ISO 27001

Informatiebeveiliging

ISO 27001 is een internationaal erkende norm voor beheersystemen voor informatiebeveiliging (ISMS). De norm specificeert de vereisten voor het opzetten, implementeren, onderhouden en continu verbeteren van een ISMS. De norm biedt een kader voor het beheren van risico's voor informatiebeveiliging en omvat mensen, processen en technologie.

ISO 27001 certificering toont aan dat een organisatie zich inzet voor informatiebeveiliging en in staat is gevoelige gegevens te beschermen. Deze certificering wordt bereikt door middel van een onafhankelijk auditproces dat wordt uitgevoerd door een geaccrediteerde certificeringsinstantie. De audit beoordeelt het ISMS van de organisatie aan de hand van de vereisten van de ISO 27001 norm.

De reikwijdte van de ISO 27001 certificeringsaudit omvat het ISMS van de organisatie, met inbegrip van het beleid, de procedures en de controles die zijn geïmplementeerd om de risico's voor informatiebeveiliging te beheren. Het omvat ook de context van de organisatie, de betrokken partijen en de reikwijdte van het ISMS.

ISO 27001 schrijft geen specifieke controles voor, maar biedt organisaties een raamwerk voor het identificeren en implementeren van de controles die nodig zijn om hun specifieke risico's aan te pakken. De norm legt de nadruk op een risico gebaseerde aanpak, waarbij organisaties hun informatiebeveiligingsrisico's moeten identificeren, analyseren en evalueren en geschikte controles moeten selecteren om deze risico's te beperken. Een succesvolle audit resulteert in de afgifte van een ISO 27001-certificaat dat geldig is voor een bepaalde periode, meestal drie jaar, en waarop periodieke surveillance audit worden uitgevoerd.

Informatiebeveiligingsmanagement

Informatiebeveiligingsbeheer is het proces waarbij de informatiemiddelen van een organisatie worden beschermd tegen ongeoorloofde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging. Het omvat een systematische aanpak voor het identificeren, beoordelen en beheren van risico's voor informatiebeveiliging.
Het doel is om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te garanderen.

Om ISO 27001 certificering te behalen, moeten serviceorganisaties hun ISMS-scope definiëren, inclusief de relevante processen, een risicobeoordelingsmethode en een verklaring van toepasselijkheid (Statement of Applicability) waarin de geïmplementeerde controles worden gedetailleerd. Deze documentatie moet de controles beschrijven en hoe ze de geïdentificeerde risico's aanpakken.

Na certificering moeten serviceorganisaties hun ISMS onderhouden. Dit betekent dat alle gedocumenteerde procedures en controles actief moeten worden uitgevoerd. Consequente toepassing van deze procedures, zorgvuldig beheer van informatiebeveiligingsprocessen en een cultuur van beveiligingsbewustzijn binnen de organisatie zijn cruciaal voor de voortdurende naleving van de ISO 27001 norm en de blijvende geldigheid van de certificering. Deze voortdurende naleving wordt meestal geverifieerd door regelmatige surveillance audit door de certificeringsinstantie.

Branches

Organisaties die diensten leveren aan andere organisaties, bijvoorbeeld Asset/Property Managers, aanbieders van pensioendiensten, Software as a Service (SaaS)-aanbieders, Infrastructure as a Service (IaaS)-aanbieders, Platform as a Service (PaaS)-aanbieders en aanbieders van Datacenterdiensten zijn over het algemeen verplicht om zich te certificeren volgens de ISO 27001 norm.

Fase 1. Definiëren van Reikwijdte

Hoe definieert u de reikwijdte van uw ISO 27001 certificering?

Het definiëren van de reikwijdte van uw ISO 27001 certificering is een cruciale eerste stap in het opzetten van uw Information Security Management System (ISMS). Het stelt de grenzen vast voor wat er in uw ISMS wordt opgenomen en dus voor wat er voor certificering zal worden gecontroleerd.

De Reikwijdte Voorbereiden

Het opstellen van de ISO 27001 scope is een fundamentele eerste stap, waarbij de grenzen van het Information Security Management System (ISMS) worden vastgesteld en de gebieden worden gedefinieerd die aan een audit worden onderworpen.

Dit proces begint met een grondig begrip van de ISO 27001 norm. De informatiemiddelen van de organisatie, waaronder gegevensclassificaties, bedrijfsprocessen, ondersteunende IT-systemen en hun respectieve locaties, moeten worden geïdentificeerd.

Vervolgens is een precieze definitie van het ISMS nodig, waarbij expliciet wordt aangegeven welke onderdelen zijn opgenomen en welke niet. Deze definitie wordt geformaliseerd in een beknopte scopeverklaring, aangevuld met ondersteunende documentatie zoals organigrammen, netwerkdiagrammen en proceskaarten.

Een grondige risicobeoordeling, afstemming op de bedrijfsdoelstellingen van de organisatie en rekening houdend met de beschikbare middelen moeten de reikwijdte bepalen. De reikwijdte blijft een dynamisch document dat regelmatig wordt herzien en bijgewerkt, met feedback van belanghebbenden om veranderende organisatorische omstandigheden te weerspiegelen. Actieve betrokkenheid van de belangrijkste belanghebbenden, nauwkeurige en ondubbelzinnige documentatie, een pragmatische en haalbare scope en formele goedkeuring door het topmanagement zijn essentieel voor een succesvolle voorbereiding van de scope, waardoor een stevige basis voor het ISMS wordt gelegd.
Er wordt een Statement of Applicability opgesteld, die fungeert als brug tussen de informatiebeveiligingsrisico's die uw organisatie loopt en de controles die u implementeert om deze risico's te beperken. In de Statement of Applicability worden alle informatiebeveiligingscontroles opgesomd die worden beschreven in Bijlage A van de ISO 27001 norm. Deze controles vormen een uitgebreide set best practices voor het beheren van informatiebeveiliging. Voor elke controle geeft de Statement of Applicability aan of deze van toepassing is op uw organisatie. Hier bepaalt u of de controle nodig en relevant is voor uw specifieke risico's en bedrijfscontext.

Concurrentievoordeel

Hoe een ISO 27001 Certificering u een voorsprong geeft op uw concurrenten

ISO 27001 certificering biedt een marktvoordeel door meer vertrouwen te wekken bij klanten en belanghebbenden, doordat naleving van strenge controles op informatiebeveiliging wordt aangetoond. Certificering onderscheidt een organisatie van anderen, met name in gegevensgevoelige sectoren, en maakt het de voorkeurskwalificatie of een vereiste voor grote bedrijfs- en overheidscontracten. Afgezien van de positionering op de markt, vermindert ISO 27001 de risico's en verbetert het de veerkracht door proactief risicomanagement en responsplanning bij incidenten, wat de bedrijfscontinuïteit vergemakkelijkt.

Fase 2. Implementatie

Stapsgewijze Aanpak

1. Planning

In fase 1 wordt de impact (GAP-analyse) van de implementatie bepaald. Op basis van de impact en de gedefinieerde reikwijdte van de implementatie wordt een gedetailleerd plan opgesteld waarin de verschillende mijlpalen worden geïdentificeerd en afspraken met het management worden gemaakt.

2. Ontwerp

In fase 2 worden interviews gehouden om risico's te identificeren, de impact en de bestaande werkwijze te bepalen en kennis te nemen van de aanwezige informatie binnen de organisatie. Er wordt gedocumenteerd beleid en gedetailleerd beleid ontwikkeld dat is afgestemd op de ISO 27001 norm en de bedrijfsdoelstellingen van uw bedrijf.

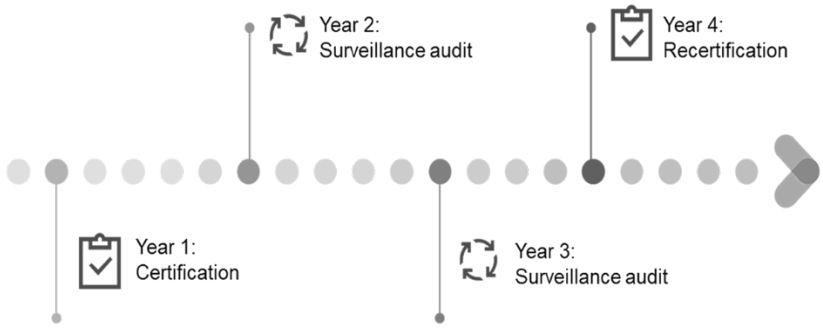
3. Monitoren, review, en verbeteren

ISO 27001 is een continu verbeteringsproces. Herzie en actualiseer uw ISMS regelmatig om ervoor te zorgen dat het effectief blijft.

Fase 3. De Audit

ISO certificeringsaudits

De ISO 27001 certificering vond plaats op basis van een driejarige cyclus.



Jaar 1: Initiële certificeringsaudit

De initiële certificeringsaudit voor ISO 27001 in het eerste jaar is een belangrijke mijlpaal in het behalen van de certificering. Het is een uitgebreide beoordeling van uw Information Security Management System (ISMS) om ervoor te zorgen dat het voldoet aan de ISO 27001 norm. In deze fase wordt het ISMS geauditeerd op ontwerp en implementatie. De auditor beoordeelt of alle controles van de ISO 27001 in het toepassingsgebied zijn gerealiseerd.

Jaar 2: Surveillance audit

Tijdens de eerste surveillance audit zal de auditor zich concentreren op specifieke gebieden van uw ISMS, vaak die gebieden die zijn geïdentificeerd als hoger risico of gebieden waar wijzigingen zijn aangebracht sinds de eerste certificering. Ze kunnen ook de status van eventuele corrigerende maatregelen van de eerste audit controleren. Het succesvol afronden van de surveillance-audit is essentieel voor het behouden van uw ISO 27001 certificering.

Jaar 3: Surveillance audit

De tweede surveillance audit bouwt voort op de eerste surveillance audit, om te controleren of u uw ISMS voortdurend onderhoudt en verbetert terwijl u effectief voldoet aan de vereisten van de ISO 27001-normen.

Jaar 4: Hercertificeringsaudit

De ISO 27001 certificeringsaudit is een uitgebreide beoordeling van uw Information Security Management System (ISMS) om ervoor te zorgen dat het voldoet aan de ISO 27001 norm. In deze fase wordt het ISMS geauditeerd op ontwerp en implementatie. De auditor beoordeelt of alle controles van de ISO 27001 in scope worden gehaald.

Belangrijkste Voordelen

Van ISO 27001 certificering

Ervaar de voordelen van ISO 27001 certificering

ISO 27001 certificering wordt door organisaties gebruikt als marketinginstrument. Nieuwe en bestaande klanten herkennen direct dat ze te maken hebben met een betrouwbare partij. Organisaties die niet over een dergelijke rapportage beschikken, lopen mogelijk belangrijke nieuwe kansen mis. Tijdens het verkoopproces is het gebruikelijk dat een klant zijn leverancier vraagt om een vragenlijst in te vullen om inzicht te krijgen in het huidige volwassenheidsniveau van de organisatie.

Door u te voorzien van een ISO 27001-certificaat krijgt u waarschijnlijk effectieve antwoorden op deze vragen. Het zal het proces aanzienlijk versnellen. Dit zal de klant ook het gevoel en vertrouwen geven dat de processen inderdaad op orde zijn.

Wij zijn Securance

Investeer in Efficiëntie, Waarde en Partnerschap

- **Risco's analyseren**
- **Het project plannen**
- **Systeembeschrijvingen voorbereiden**
- **Een Readiness Assessment uitvoeren**

Het implementeren van ISO 27001 vereist effectieve planning, betrokkenheid van het leiderschap, grondige analyse van processen en betrouwbare middelen en projectmanagement.

Securance komt voort uit een 'Big Four' accountantskantoor en is opgericht in 2004. Het resultaat van onze achtergrond is dat we werken volgens de hoogste professionele standaarden en ervaring hebben in het werken met strakke deadlines. We leven naar onze professionele normen en leveren altijd de hoogste kwaliteit terwijl we er voortdurend naar streven om aan de behoeften van onze klanten te voldoen.

Door onze vlakke structuur en efficiënte communicatie kunnen we snel inspelen op uw behoeften. Kiezen voor Securance betekent kiezen voor een professionele organisatie, maar ook kiezen voor een persoonlijke aanpak. Effectief projectmanagement, onze ervaring met het implementeren van risicomanagementraamwerken in uw branche en professionaliteit zijn volgens ons de basis voor uitstekende resultaten.

Als Securance geloven we dat een goed begrip, heldere communicatie en kennis van de industrie van onze klanten essentieel zijn voor het leveren van toegevoegde waarde aan u als klant. Vanuit deze benadering informeren wij u over relevante wijzigingen in wet- en regelgeving en andere belangrijke ontwikkelingen.

SECURANCE
BE SURE

Onze tevreden klanten

Referenties

SECURANCE
BE SURE

Securance Ltd.

63-66 Hatton Garden
London EC1N 8LE, UK
+44 20 351 446 56
www.securance.co.uk

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.securance.nl