ISO-normen voor informatiebeveiliging, kwaliteits- en risicomanagement

Wat houden deze internationale standaarden in en wat zijn de voordelen?

Globalisering heeft voor veel bedrijven als nadeel dat het voldoen aan de verschillende eisen en richtlijnen per land kostenverhogend en tijdrovend is. Om uniformiteit te creëren, zijn er internationale normen ontwikkeld voor systemen, werkmethodieken, materialen, producten en begrippen. Na het lezen van deze whitepaper weet u wat de normen ISO 9001 (kwaliteitsmanagement), ISO 27001 (informatiebeveiliging) en ISO 31000 (risicomanagement) inhouden en of deze wellicht interessant zijn voor uw organisatie.

CONSIGNIUM
we create impact

Inhoud

Pag. 1. Samenvatting
Pag. 2. Wat is ISO?
Pag. 3. ISO 9001
Pag. 4. ISO 27001
Pag. 5. ISO 31000
Pag. 6. Conclusie

Samenvatting

Door implementatie van ISO 9001, ISO 27001 en/of ISO 31000 bespaart een organisatie tijd en kosten die nodig zijn voor het borgen van respectievelijk kwaliteit, informatiebeveiliging en/of risico's.

De kwaliteitsnorm bereidt de organisatie voor op het produceren van hoogwaardige producten en services. De aanpak is klantgericht en legt de nadruk op continue verbetering en een organisatiebreed framework van processen om kwaliteit blijvend te waarborgen.

ISO 27001 heeft betrekking op informatietechnologie, met als doel de beveiliging te verbeteren en de bedrijfsmiddelen te beschermen.

Het is erg belangrijk dat een organisatie op elk gebied in staat is om risico's effectief te beheren. ISO 31000 helpt hierbij en stelt een organisatie in staat om bedreigingen beter te identificeren voordat ze zich voordoen en te anticiperen op deze risico's.

De organisatie die al aan een of meerdere van de drie hierboven genoemde internationale standaarden voldoet, heeft het bijkomende voordeel dat er overlappingen zijn met de Algemene Verordening Gegevensbescherming wat helpt bij het compliant worden hieraan.

Wat is ISO?

ISO is een afkorting voor International Organisation for Standardization. De kern van de ISO is “Zeg wat je doet en doe wat je zegt”. De organisatie zorgt voor standaarden om veiligheid, efficiëntie en kwaliteit te waarborgen. Dit doet zij voor vrijwel alle branches wereldwijd. Op dit moment zijn er meer dan 22.000 verschillende documenten gepubliceerd door ISO. Een ISO-norm geeft kaders en structuur aan een organisatie om de producten of diensten beter te produceren of uit te voeren.

Vier pijlers voor normontwikkeling

- Behoefte in de markt: een ISO-norm wordt ontwikkeld als reactie op een verzoek van belanghebbenden zoals de industrie of consumentengroepen.
- Deskundigheid: ISO-normen zijn gebaseerd op de mening van deskundigen van over de hele wereld.
- Meerdere belanghebbenden: meerdere partijen met verschillende belangen zijn betrokken bij de ontwikkeling van een ISO-norm.
- Consensus: de aanpak is erop gebaseerd dat er overeenstemming moet zijn tussen alle belanghebbenden.

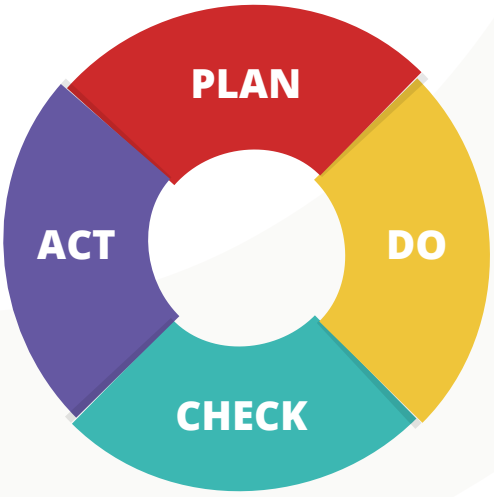
ISO 9001

De meest bekende ISO-norm geeft een organisatie grip op kwaliteit en borgt deze. Dit wordt in ISO-termen het kwaliteitsmanagementsysteem genoemd. De norm geeft aan wat er moet gebeuren en aan welke eisen voldaan moet worden. Ook geeft de norm handvatten voor de organisatie om de beoogde kwaliteit vast te houden. Hierbij is het aan de organisatie om een framework op te stellen dat de kwaliteit moet waarborgen.

Kwaliteit is de mate waarin iets voldoet aan de gestelde eisen. De eisen die worden gesteld, zijn afkomstig van stakeholders (waaronder klanten, aandeelhouders, overheid en medewerkers). De wensen van de klanten moeten zodanig worden doorgevoerd in de organisatie dat de klanten krijgen wat ze willen.

Het nut van ISO 9001

Het werken met ISO 9001 zorgt voor klantgerichtheid binnen de organisatie. Het is duidelijk wat de klant wil en ze krijgt de mogelijkheid om haar oordeel te geven over de geleverde dienst of product. De klant staat bij de ISO 9001 centraal. Daarnaast zorgt het voor leiderschap en betrokkenheid. Er wordt een stip op de horizon afgedwongen, waar naartoe gewerkt gaat worden. Dit geeft zowel de directie als medewerkers structuur en houvast. Het zorgt voor beheersing van processen en de risico's ervan. Belangrijk is dat de organisatie haar processen zo heeft ingericht dat het in staat is om continue verbeteringen door te voeren. Alles wordt samengevat in een PDCA-cyclus.



Aan de slag met ISO 9001

Het is belangrijk dat de organisatie doelen heeft opgesteld die in lijn liggen met de strategie van de onderneming. Dit moeten voor de ISO 9001 'kwaliteitsdoelen' zijn. Deze kunnen zijn opgesteld in KPI's of een andere vorm, zolang ze meetbaar zijn. De organisatie mag deze kwaliteitsdoelen zelf bepalen, mits zij rekening houdt met de eisen van de stakeholders (klantgerichtheid). De processen van de organisatie moeten zijn omschreven en er moet helderheid zijn over wie verantwoordelijk is voor welke taken. Gedurende het jaar moeten metingen worden gedaan om te zien of de onderneming haar (kwaliteits)doelstellingen behaald heeft, waarop eventueel kan worden bijgestuurd. Dit zorgt voor een constante verbetercyclus (PDCA). Als alles is geïmplementeerd kan certificering en een audit worden aangevraagd bij een externe partij.

Plan: context van de organisatie, leiderschap en planning
Do: zorg voor ondersteuning en uitvoering
Check: meten en evalueren van prestaties
Act: verbeteren

ISO 27001

ISO 27001 staat voor de mate van informatiebeveiliging en de borging hiervan. De informatiebeveiliging is het geheel van maatregelen die zijn genomen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen. De Algemene Verordening Gegevensbescherming zorgt voor meer aandacht voor informatiebeveiliging (ISO 27001). In de norm worden eisen gesteld aan het omgaan met informatie, zoals documenten, klantgegevens, gebruikte apparatuur en applicaties. Hiermee kun je aantonen dat je goed omgaat met (privacygevoelige) gegevens.

Het nut van ISO 27001

Het is belangrijk dat de informatiebeveiliging goed op orde is. De ISO-standaarden zorgen voor duidelijkheid over hoe de organisatie omgaat met de diverse datastromen. De organisatie zorgt voor een overzicht van haar meest kritieke systemen en informatie. De organisatie zal middels ISO inzichten krijgen in de risico's die ze loopt. Hierbij wordt gekeken naar beschikbaarheid, integriteit en veiligheid van informatie. De organisatie stelt voor zichzelf doelstellingen op, dit schept een kader. Het iteratief proces zorgt ervoor dat er een constant proces is van verbeteren.

Aan de slag met ISO 27001

Bij ISO 27001 is het van belang dat er één basisdocument is dat omschrijft op welke wijze de organisatie de informatiebeveiliging waarborgt. Het belangrijkste is dat de organisatie een risicoanalyse uitvoert. Hierin wordt omschreven waar de grootste risico's zich voor kunnen doen. Op basis van deze gegevens moet bekeken worden welke beheersmaatregelen moeten worden geïmplementeerd. Dit moet te vinden zijn in ontwikkelde beleidsstukken. Er moeten volgens de norm ook doelstellingen worden opgesteld en procedures worden ontwikkeld (bijvoorbeeld voor het geval een datalek plaatsvindt). Alle beleidsstukken moeten samen één geheel vormen en bewijzen dat ISO 27001 goed is ingericht. Als alles is geïmplementeerd kan er een certificering worden aangevraagd.

Beheersmaatregelen van de ISO 27001

Een belangrijk deel van de ISO 27001 zijn de beheersmaatregelen, dit zijn er 144. Een beheersmaatregel is een middel dat wordt ingezet om een risico te beheersen. Het is de bedoeling dat aan alle 144 opgestelde beheersmaatregelen wordt voldaan, tenzij kan worden aangetoond dat één of meer maatregelen niet van toepassing zijn. Dit kan door een verklaring van toepasselijkheid te doorlopen. Er moet een relatie tussen een beheersmaatregel en een risico aanwezig zijn. Een beheersmaatregel kan inhouden dat een beleidsstuk moet worden geïmplementeerd. Voorbeelden zijn een informatiebeveiligingsbeleid, een toegangsbeveiligingsbeleid en een clean desk beleid.

ISO 31000

Risicomanagement is voor grote bedrijven een verplichting, meestal vanuit wetgeving. Echter gaan steeds meer ondernemingen zich bezighouden met risicomanagement. De term risico houdt het volgende in: een onzekerheid waar mogelijk een actie op ondernomen moet worden. Ook kleinere ondernemingen kunnen gebruik maken van ISO 31000. Het is een richtlijn voor het ontwerp, de implementatie en het onderhoud van het risicomanagement framework.

Het nut van ISO 31000

Het nut van risicomanagement voor een organisatie is dat het een kader schept, helderheid biedt en een goede link legt tussen het management van een onderneming en de risico's die op de organisatie van toepassing zijn. Ook een organisatie die regelmatig een herijking wil van zijn risicomanagement, kan steunen op het framework van de normering. Het biedt de organisatie een spiegel voor de wijze waarop zij omgaat met risico's. Maakt de organisatie gebruik van meerdere modellen of managementsystemen, dan werkt ISO 31000 als een paraplu die de onderlinge relaties zichtbaar maakt.

Aan de slag met ISO 31000

ISO 31000 bestaat uit:

- De principes van risicomanagement
- Een framework of raamwerk voor risicomanagement
- Het risicomanagementproces

De principes van risicomanagement vormen het fundament van de organisatie. Dit is het risicobewustzijn van de organisatie enerzijds en het gedrag van de medewerkers en de cultuur anderzijds. Dit geeft meteen aan dat er een goede match moet zijn tussen de mensen en de doelen van de organisatie. Als het draagvlak bij de medewerkers ontbreekt, zullen de doelen vanuit het risicomanagement nooit van de grond komen.

Het framework geeft aan waar de onderlinge relaties liggen tussen afdelingen van de organisatie (zowel horizontaal als verticaal). Dezelfde waardes worden gehanteerd, processen en procedures zijn op elkaar afgestemd en er is sprake van een continue verbetering.

Tot slot is er het proces van risicomanagement. Dit proces omvat onder meer het bepalen van de risicocontext en het identificeren, analyseren, evalueren en communiceren van risico's.

Conclusie

Normen als ISO 9001, 27001 en 31000 zorgen ervoor dat een organisatie en haar klanten erop kunnen vertrouwen dat hun producten veilig, betrouwbaar en van goede kwaliteit zijn. De internationale standaarden helpen een bedrijf, ongeacht de omvang en de sector waarin zij actief is, om kosten te verlagen en de productiviteit te verhogen. Daarnaast bieden ISO-normen een sterke basis voor de ontwikkeling van (inter)nationale regelgeving. Denk aan de Algemene Verordening Gegevensbescherming waarbij heldere processen, een goede informatiebeveiliging en inzicht in de risico's van groot belang zijn.

Over Consignium

Het realiseren van optimaal risicomanagement, verbeteren van prestaties, optimaliseren van uw organisatie en het efficiënt inrichten van wet- en regelgeving. Dat is waar de consultants van Consignium goed in zijn. Elke organisatie is anders en Consignium kan met haar verschillende producten en diensten aansluiten bij uw specifieke situatie. Wij zorgen voor impact. We create impact.

Neem vrijblijvend contact met ons op voor een kennismaking en het bespreken van de mogelijkheden voor een optimale oplossing.

Meer informatie

Consignium B.V.
Koningsweg 2-30
3762 EC Soest
035-879 56 48

Op de hoogte blijven?

www.consignium.nl
info@consignium.nl

Via de website kunt u zich inschrijven voor onze nieuwsbrief.

CONSIGNIUM
we create impact