In negen stappen naar ISO 27001 certificering

STAP 1
DOE KENNIS OP OVER DE ISO 27001-STANDAARD TIJDENS ONZE TRAININGEN
Het is belangrijk dat u goed begrijpt wat de vereisten zijn van ISO 27001 en welke eisen gesteld worden aan uw organisatie. Leer hier alles over tijdens onze ISO 27001 normtraining.

STAP 2
START DE IMPLEMENTATIE VAN HET INFORMATIEBEVEILIGINGSMANAGEMENTSYSTEEM
ISO 27002 is de praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging. Deze standaard biedt bruikbare handvatten voor de implementatie van het ISO 27001 managementsysteem.

STAP 3
BEPAAL IN DE CERTIFICATIESCOPE OP WELKE ORGANISATIEONDERDELEN INFORMATIEBEVEILIGING VAN TOEPASSING IS
Ter voorbereiding op de certificatieaanvraag beslist u welke organisatieonderdelen u opneemt in de scope.

STAP 4
INVENTARISEER DE HUIDIGE STAND VAN INFORMATIEBEVEILIGING MET EEN RISICOBEOORDELING
Om een duidelijk beeld te krijgen van mogelijke bedreigingen en gevolgen voert u een risicobeoordeling uit. Vervolgens kunt u per risico de prioriteiten vaststellen.

STAP 5
STEL EEN RISICOBEHEERSPLAN OP
De input van de risicobeoordeling geeft u een goede basis om een risicobeheersplan op te stellen. Hierin bepaalt u per risico het belang en documenteert u welke preventieve maatregelen genomen moeten worden.

STAP 6
ZORG VOOR BEDRIJFSCONTINUÏTEIT
Herstelbeheersing is een belangrijk onderdeel van informatiebeveiliging geworden. Als organisatie moet u in het geval van ontwrichting zorgen dat de bedrijfsactiviteiten blijven doorgaan. Met bedrijfscontinuïteit probeert u uw bedrijf zo goed mogelijk voor te bereiden op verstorende incidenten. De ISO 22301-standaard kan uw organisatie daarbij ondersteunen. Leer er meer over tijdens onze ISO 22301 normtraining.

STAP 7
CONTROLEER OF UW ORGANISATIE KLAAR IS VOOR CERTIFICERING AAN DE HAND VAN EEN ISO 27001 PRE-AUDIT
Om zeker te stellen dat uw organisatie klaar is voor ISO 27001 certificering kunt u voorafgaand aan de certificatieaudit een ISO 27001 assessment uit laten voeren. Hierbij krijgt u een goed beeld van eventuele tekortkoming op uw informatiebeveiliging managementsysteem.

STAP 8
MAAK UW INSPANNING AANTOONBAAR MET ISO 27001 CERTIFICERING
Tijdens de certificatieaudit controleert de SGS auditor de effectiviteit van uw informatiebeveiligingssysteem. Na een positieve afronding van de certificatieaudit ontvangt uw organisatie een ISO 27001 certificaat. Hiermee heeft u aantoonbaar bewijs dat uw organisatie op een verantwoorde manier omgaat met informatie.
Jaarlijks volgen controlebezoeken en na 3 jaar volgt er een hercertificeringsaudit.

STAP 9
Na het behalen van ISO 27001 certificaat is het van belang dat u het managementsysteem goed onderhoudt. Uw auditteam is daarbij van cruciaal belang. Plan geregeld een intervisiemoment met het auditteam, dit zorgt ervoor dat iedereen op dezelfde lijn blijft denken. Daarnaast is het goed om op de hoogte te blijven van veranderingen in de wet- en regelgeving.

WHEN YOU NEED TO BE SURE