ISO 27001

Certificatie voor informatiebeveiliging

Certificatie voor informatiebeveiliging

U wilt graag aantoonbaar maken dat u op een verantwoorde manier met informatie omgaat. We laten u daarom graag zien hoe de weg naar certificatie voor ISO 27001 verloopt. Zo kunt u zelf bepalen welke stappen u wanneer neemt, om uw managementsysteem gereed te maken voor certificering. Vanzelfsprekend praten we ook graag persoonlijk met u over dit proces.

De weg naar certificatie

De weg naar certificatie verloopt via een vastgesteld proces. De beste manier om uw vertrekpunt te bepalen is met de PDCA (PLAN-DO-CHECK-ACT)* techniek. Bepaal met deze PDCA checklist of u klaar bent voor certificering.

Vul de checklist in!

PLAN – Het bepalen van de reikwijdte van uw systeem

- ☐ Is de scope van de certificatie bepaald?
- ☐ Is er binnen uw organisatie een informatiebeveiligingsbeleid opgesteld?
- ☐ Is er een methode voor risicomanagement gekozen en gedocumenteerd?
- ☐ Is de risicoanalyse volgens de gekozen methode uitgevoerd?
- ☐ Zijn de maatregelen die uit de risico-analyse voortkwamen gekozen en gedocumenteerd?
- ☐ Is de 'Verklaring van Toepasselijkheid' opgesteld?

DO – Implementeren van de maatregelen

- ☐ Is de "gap" tussen norm en realiteit geïdentificeerd?
- ☐ Is ter overbrugging van deze gap een implementatieplan opgesteld?
- ☐ Is de wijze van meting per maatregel of groep maatregelen gedefinieerd?
- ☐ Wordt het plan (inmiddels) uitgevoerd?

CHECK – Monitoren en intern beoordelen

- ☐ Zijn er interne audits uitgevoerd?
- ☐ Is de effectiviteit van de genomen maatregelen gemeten?
- ☐ Is er een managementreview uitgevoerd?

ACT – Onderhoud en verbeteren

- ☐ Zijn de corrigerende- en verbetermaatregelen doorgevoerd?

*W. Edwards Deming, Out of the Crisis, Massachusetts Institute of Technology Press, 1986, p. 88.

Het certificatietraject

Start certificatietraject

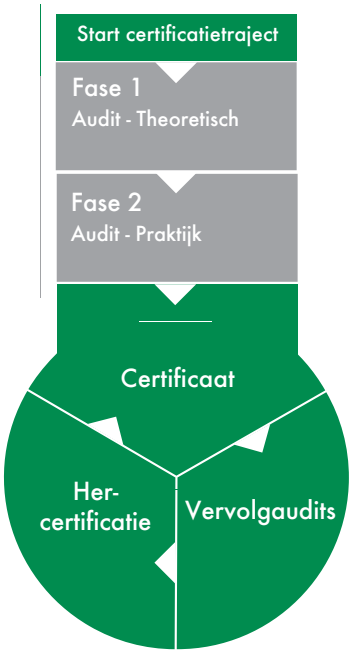
Kunt u checklist afvinken? Dan is uw informatiebeveiligingssysteem klaar voor de start van het certificatietraject. Is dat niet zo? Zet dan de openstaande acties uit te zetten binnen uw bedrijf. Afhankelijk van het vertrekpunt van uw organisatie, duurt het hele traject zes tot negen maanden.

Fase 1: risicobeoordeling

In Fase 1 beoordeelt onze auditor de risicoanalyse, de verklaring van toepasselijkheid en de beschikbare systeemdocumentatie van uw organisatie. In de periode tot Fase 2 heeft u de mogelijkheid om eventuele verbeterpunten aan te pakken.

Fase 2: toetsen in de praktijk

In Fase 2 worden op basis van het auditprogramma onderwerpen en processen geselecteerd. De implementatie, effectieve werking van het managementsysteem en de genomen maatregelen toetsen we in de praktijk. Dat doen we altijd met oog voor de mensen in uw organisatie. We noemen dit een People Based Auditing en bieden het standaard aan als toegevoegde waarde bij ISO-certificeringen.



Certificaat, vervolgaudits en hercertificatie

Als de audits succesvol zijn afgerond ontvangt u een certificaat. Dit certificaat is drie jaar geldig. Jaarlijks worden twee vervolgaudits uitgevoerd. Na deze periode volgt de hercertificatie. Hierbij kijkt onze auditor hoe het managementsysteem functioneert. Om dit te beoordelen worden interviews afgenomen met de directie, het management en medewerkers. Het eindresultaat bepaalt of u weer een certificaat ontvangt. Zo blijft het certificatietraject zich herhalen.

Contact DEKRA Audit

Meander 1051
6825 MJ Arnhem
Nederland

Telefoon: +31 88 96 83 016

SalesAudit.nl@dekra.com
dekra.nl/audit