



## Certificering ISO/IEC 27001

### **Informatiebeveiliging is gezichtsbepalend voor veel organisaties**

Snelle en efficiënte dienstverlening, op maat en in samenhang aangeboden, is sterk afhankelijk van een adequaat ingericht stelsel informatiebeveiligingsmaatregelen.

### **Zekerheid op het gebied van informatie en ICT**

Een goede beheersing van de informatisering en de automatisering wordt steeds belangrijker. Informatie speelt vandaag de dag een steeds belangrijkere rol in het succes en voortbestaan van organisaties.

Steeds vaker komen bedrijven (negatief) in het nieuws vanwege het verlies van vertrouwelijke of bedrijfsgevoelige informatie. Naast de imagoschade wilt u er natuurlijk niet aan denken dat bedrijfsgevoelige of klantinformatie, bewust of onbewust, bij concurrenten terechtkomt met alle gevolgen van dien.

Het gebruik van een wereldwijde geaccepteerde norm biedt organisaties een procesgerichte aanpak voor het opzetten, implementeren, beheren, monitoren, evalueren, onderhouden en verbeteren van processen binnen een specifiek gebied.

De ISO/IEC 27001 is de norm voor informatiebeveiliging die organisaties handvatten geeft voor het beheren en beveiligen van waardevolle informatie en middelen. Door de invoering van ISO/IEC 27001 laat u betrokken partijen, zoals klanten, toezichthouders en medewerkers, zien dat u aandacht heeft voor het belang van:

- het vertrouwelijk omgaan met gevoelige informatie,
- het beschikbaar hebben van informatie wanneer dat gewenst is en,
- informatie die accuraat en volledig is.

### **Waarom Duijnborgh Certification?**

Wij zijn een certificerende instantie, gespecialiseerd in certificeringen op het gebied van ICT.

Wij zijn op grond van de Wet aanwijzing nationale accreditatie-instanties door de Raad voor Accreditatie (RvA) onder registratienummer C590 geaccrediteerd voor certificering tegen de ISO-IEC 27001 norm (beter bekend onder de naam Code voor informatiebeveiliging). Ook voor andere ICT gerelateerde normen zoals de NEN 7510, de ISO 20000 en de ISO 22399 kunt u bij ons terecht.

Wij zijn geen 'certificeringsfabriek', noch krijgt u bij ons het certificaat 'kado'. Als u -samen met ons- de overtuiging heeft dat certificatie geen doel op zichzelf is, maar een middel om te komen tot betere bedrijfsprestaties, dan bent u bij ons aan het goede adres.

## De norm ISO/IEC 27001 (Code voor informatiebeveiliging)

Het invoeren van een informatiebeveiligingsbeheerssysteem is geen doel op zichzelf. Redenen voor invoer kunnen extern gestuurd zijn zoals een eis van een toezichhoudend orgaan of van een organisatie die diensten uitbesteedt, of intern gestuurd vanuit een wens om bijvoorbeeld de bedrijfscontinuïteit te borgen.

Door de opzet van de 27001 norm is deze geschikt voor elke organisatie, groot of klein, in welke sector of welk deel van de wereld dan ook. De norm is zeker van belang voor sectoren waar de beveiliging van informatie cruciaal is, zoals in de financiële sector, de gezondheidssector, de publieke sector en de ICT-sector.



### De aanpak van Duijnborgh Certification B.V.

Als geen ander weet Duijnborgh Certification dat het opzetten van een systeem volgens generieke eisen niet zo maar past bij uw unieke organisatie. Samen met u zoeken wij naar de meerwaarde van het beheerssysteem om relevante activiteiten te beheersen en te verbeteren. Eerst worden de wensen van uw organisatie in kaart gebracht. Op basis van het resultaat zal een offerte worden uitgebracht.

Vanuit een (facultatieve) proefbeoordeling kan de organisatie een indruk krijgen over de status van haar informatiebeveiliging en beslissen om wel of niet een certificatie traject in te gaan of een geschikt tijdsplan te bepalen voor certificering.

### Gefaseerde aanpak

Het certificeringstraject zelf wordt uitgevoerd in 2 fasen waarbij per fase een rapportage wordt opgeleverd met daarin de conclusie, tekortkomingen, verbeter-suggesties en aandachtspunten voor het management.

**Fase 1** - tijdens fase 1 van het certificeringstraject wordt het gedocumenteerde beheerssysteem van de organisatie beoordeeld. Het gaat hierbij om de methode van risicoanalyse, de Verklaring van Toepasselijkheid en de aanwezigheid en werking van de

kernelementen van het beheerssysteem. Eventuele tekortkomingen dienen voor fase 2 te zijn opgepakt.

**Fase 2** - Tijdens fase 2 van het certificeringstraject wordt beoordeeld of het gedocumenteerde systeem van de organisatie in voldoende mate is ingevoerd en het beheerssysteem ondersteunt. Het beheerssysteem dient in overeenstemming met de eisen uit ISO/IEC 27001, zoals eigen beleid, vigerende wet- en regelgeving en eisen van belanghebbenden te functioneren en in staat te zijn om continue te verbeteren en onderkende risico's te minimaliseren.

Op basis van de resultaten uit fasen 1 en 2 zal worden besloten of er overgegaan wordt tot certificering en het verstrekken van het certificaat. Indien er (nog)onvoldoende aan de eisen vanuit de norm wordt voldaan dient de organisatie maatregelen te treffen. Na het corrigeren van de tekortkomingen, kan het resultaat worden geëvalueerd en alsnog worden overgegaan tot certificering.

Een certificaat is drie jaar geldig, waarbij het beheerssysteem minimaal jaarlijks wordt geëvalueerd.

Duijnborgh Certification BV  
WTC Papendorp  
Papendorpseweg 100  
3528 BJ Utrecht  
T 31(0)88 160 1750  
F 31(0)88 160 1799  
E [info@dbcert.nl](mailto:info@dbcert.nl)

  
**DUIJNBORGH**  
**CERTIFICATION®**

