



Certificering ISO 27017:2015

ISO/IEC 27017:2015 'Code of practice voor Clouddiensten'

Deze Internationale standaard biedt richtlijnen ter ondersteuning van de implementatie van informatiebeveiligingsmaatregelen voor cloudserviceklanten en cloudserviceproviders.

Zekerheid op het gebied van Clouddiensten

Clouddiensten worden in verschillende vormen aangeboden. Hierbij valt te denken aan SaaS (Software as a Service), IaaS (Infrastructure as a Service), PaaS (platform as a Service), DRaaS (Disaster Recovery as a Service), BaaS (Business as a Service), et cetera, et cetera. Het einde is nog (lang) niet in zicht: volgens onderzoeksbureau Gartner zullen toekomstige ontwikkelingen, in combinatie met de inmiddels brede acceptatie van clouddiensten, tot een aanzienlijke groei binnen dit marktsegment leiden.

De beheersmaatregelen in de ISO 27017:2015 zijn een aanvulling op de ISO 27002:2013. Het gaat om 7 nieuwe beheersmaatregelen en 35 bestaande beheersmaatregelen die specifiek zijn gemaakt. Sommige richtlijnen zijn voor cloud serviceklanten en anderen zijn voor cloud serviceproviders. De selectie van geschikte controls zal afhangen van een risicobeoordeling en van alle wettelijke, contractuele, regulerende of andere specifieke informatiebeveiligingseisen. Hiervoor wordt het ISMS van ISO 27001:2013 gebruikt. Certificatie vindt dan ook doorgaans plaats in samenhang met de ISO 27001:2013.

Door de invoering van de ISO 27017:2015 laat u als leverancier van clouddiensten betrokken partijen, zoals klanten, toezichthouders en medewerkers, zien dat u aanvullende controles heeft geïmplementeerd om cloudspecifieke informatiebeveiligingsbedreigingen en -risico's aan te pakken.

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) geaccrediteerd voor certificering tegen de ISO-IEC 27001 norm (ook bekend onder de naam Code voor informatiebeveiliging). Ook voor andere ICT gerelateerde normen zoals de NEN 7510, de ISO 27017, ISO 27018, 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 ISO 27001 en ISO 27017 in samenhang

De ISO 27017 is primair van belang voor sectoren waar gebruik gemaakt wordt van clouddiensten. Zoals hiervoor opgemerkt, is deze norm zowel voor de leverancier van clouddiensten als voor de afnemer hiervan van toepassing en wordt een certificatie-traject doorgaans in samenhang met de ISO 27001 uitgevoerd. De ISO 27017 steunt op het managementsysteem van de ISO 27001.

Indien uw organisatie niet gecertificeerd is tegen de norm ISO 27001, en dit ook niet gewenst is, kunnen we samen met u bekijken welke elementen uit de ISO 27001 in uw organisatie moeten worden geïmplementeerd om een afzonderlijke certificatie tegen ISO 27017 mogelijk te maken.



Certificering tegen ISO 27017 in 5 stappen.

Het volgende stappenplan kan gehanteerd worden bij het voldoen aan ISO 27017 en het laten uitvoeren van een certificatie audit:

Stap 1: Risicoprofiel en beheersingsdoelstellingen vaststellen

Met behulp van de bestaande risico behandelmethodiek brengt u de risico's in beeld die gerelateerd zijn aan cloud computing. Tevens wordt in kaart gebracht welke wettelijke, contractuele, regulerende of andere specifieke informatiebeveiligingseisen van toepassing zijn. De focus is hierbij gericht op de manier waarop IT-middelen technisch zijn ontworpen, worden beheerst en beheerd. In beginsel gebruikt u hiervoor het bestaande managementsysteem (ISMS) van ISO 27001. De geïdentificeerde risico's worden vertaald in beheersingsdoelstellingen en op basis van deze doelstellingen worden de beheersmaatregelen geselecteerd.

Stap 2: Pre-audit en terugkoppeling

De beheersmaatregelen worden in opzet en bestaan in een korte tijd gecontroleerd om een eerste indruk te verkrijgen. De bevindingen worden aan u teruggekoppeld. Op basis van de uitkomsten van de pre-audit wordt tevens vastgesteld wanneer het certificatie-onderzoek kan starten.

Stap 3: Iteratief verbeterproces

Op basis van de uitkomsten van de pre-audit brengt uw organisatie gewenste verbeteringen aan. Duijnborgh Certification is gedurende deze periode –en waar dat binnen haar auditrol past- beschikbaar voor het tussentijds beoordelen van de verbeteracties. Hierdoor worden verrassingen achteraf voorkomen en wordt de kans van slagen bij de eindbeoordeling aanzienlijk vergroot.

Stap 4: Audit opzet en bestaan beheersmaatregelen

Op het moment dat uw organisatie aangeeft klaar te zijn voor het certificatie-onderzoek zullen wij een audit uitvoeren ter beoordeling van de opzet en het bestaan van de op cloud computing gericht beheersmaatregelen.

Stap 5: Certificatie

Op basis van de resultaten uit de voorgaande stappen 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 jaarlijks een controle-audit wordt uitgevoerd gericht op de effectieve werking van de beheersmaatregelen.

