Information Security Assessment (ISA)

Wat is een Information Security Assessment!

Het doel van het uitvoeren van een ISA is in de eerste plaats het inzichtelijk maken van de mate waarin uw organisatie beveiligingsmaatregelen heeft getroffen ter waarborging van de beschikbaarheid, integriteit en vertrouwelijkheid van uw informatie en uw informatievoorziening. De ISA doet dit door op gestructureerde wijze de aanwezige beveiligingsmaatregelen in kaart te brengen en deze te houden tegen algemeen geaccepteerde normen.

Met het uitvoeren van een ISA verkrijgt u inzicht in het gebrek aan beveiligingsmaatregelen en daarmee in de risico's voor uw bedrijfsvoering in relatie tot informatiebeveiliging.

Waarom een Information Security Assessment uitvoeren?

De afgelopen jaren hebben snelle technologische ontwikkelingen gezorgd voor een toename van de mogelijkheden om informatie op te slaan en te bewerken. Big Data, smartphones, cloud computing, biometrics, EPD's en voordeelkaarten zijn slechts enkele voorbeelden van de vele ontwikkelingen die informatiebeveiliging en privacy een steeds grotere uitdaging maken.

Het belang om zorgvuldig met informatie om te gaan wordt vrijwel elke dag in het nieuws bevestigd. Organisaties ondervinden steeds vaker negatieve gevolgen van de wijze waarop zij omgaan met informatie. Zo worden organisaties op het matje geroepen door toezichthouders en ontstaat negatieve publiciteit omdat organisaties niet voldoende in staat blijken om te voldoen aan wet- en regelgeving. Boetes en imagoschade zijn het gevolg.

Wanneer een Information Security Assessment uitvoeren?

Het beste kan een ISA worden uitgevoerd in een zeer vroeg stadium van uw beveiligingsproject om informatie beveiliging binnen uw organisatie op de kaart te zetten. De uitkomsten kunnen vervolgens worden gebruikt bij de verdere uitwerking van het stelsel van beveiligingsmaatregelen dat u voor uw organisatie van toepassing acht. Verder verdient het aanbeveling de ISA periodiek en bij grote wijzigingen te herhalen. De ISA helpt u op die manier om het belang van informatie voor uw organisatie structureel mee te nemen in veranderende omstandigheden, aangeduid als security by design.

Onze aanpak

Risk Knowledge heeft haar aanpak gebaseerd op de internationale norm op het gebied van informatiebeveiling ISO/IEC 27001:2013. Indien gewenst kan de ISA worden uitgebreid met een inspectie van de netwerkbeveiliging of het uitvoeren van pentesten waarbij gebruik wordt gemaakt van andere normen of technische standaarden.

De context, waar binnen de ISA wordt uitgevoerd, is bepalend voor de scope en reikwijdte van de voorstellen tot verbetering van het aanwezige stelsel van beheersmaatregelen. Verder zijn de branche, aard en omvang van het bedrijf en de technische en organisatorische complexiteit van de verwerking van belang voor het uitvoeren van de ISA.

De benodigde tijd en doorlooptijd voor het uitvoeren van een ISA, zal per ISA verschillen en hangt van de genoemde factoren af.

Contact

Risk Knowledge is graag bereid de mogelijkheden voor uw organisatie ten aanzien van het uitvoeren van een PIA met u te verkennen. Voor meer informatie kunt u contact met ons opnemen.