Aantoonbaar voldoen aan de BIO?

Alle overheden en organisaties verbonden aan de overheid moeten in 2020 voldoen aan de BIO eisen.

De BIO heeft aanvullende eisen op de ISO27001 – bijlage A maatregelen vastgesteld. Veelal wordt dit ook uitgelegd dat de BIO aanvullende is op de ISO27002. dit is niet helemaal juist omdat de ISO27002 implementatie richtlijnen geeft voor de in Bijlage A vermelde beheersmaatregelen.

Feitelijk geeft de BIO aanvullende eisen op de bijlage A beheersmaatregelen uit de ISO27001.

De organisatie moet, bij wet voldoen aan de BIO. bij het niet voldoen is er feitelijk een wetsovertreding. Belangrijk dus dat de organisatie kan aantonen aan relevante stakeholders dat er ook daadwerkelijk wordt voldaan aan de aanvullende BIO eisen. Binnen de BIO bestaan er 3 Basis Beveiliging Niveau's (BBN).

BBN 1

Bij BBN1 gaat het om wat er minimaal verwacht mag worden van de overheid voor de bescherming van informatie. We hebben hier te maken met een laag betrouwbaarheidsniveau en daarom blijven complexe eisen hier achterwege. Het gaat puur om een minimale basis eis op de beheersmaatregelen.

BBN 2

De meeste informatie binnen de overheid zal op dit niveau worden ingeschaald. Het gaat hier om goed huisvaderschap voor informatie. BBN2 is het minimale niveau waarop met persoonsgegevens gewerkt wordt. BBN2 ligt qua zwaarte op hetzelfde niveau als de oude baselines. Bij BBN2 ligt voor statelijke actoren en vergelijkbare dreigers de nadruk op 'detectie'.

BBN 3

Bij BBN3 gaat het om informatie waar weerstand tegen statelijke of criminele actoren (of gelijksoortige dreigers) nodig is. De vertrouwelijkheid heeft hier een hogere score, de andere eisen kunnen nog altijd op midden zitten. Binnen de BIO zijn er nog geen eisen vastgesteld op BBN3 niveau voor specifieke beheersmaatregelen.

Hoe kies ik de juiste BBN's?

Om het juiste niveau te kiezen is er een baselinetoets beschikbaar. Op basis van een aantal vragen, wordt hiermee duidelijk welk BBN niveau van toepassing is. De proceseigenaar bepaalt op basis van de toets welk BBN gevolgd dient te worden.

BIO audits en kosten

In de praktijk worden BIO audits vaak gecombineerd met een ISO27001 certificering. De aanvullende BIO maatregelen worden dan meegenomen tijdens de certificering audit. Om te komen tot een offerte voor certificeren moeten we een goed beeld hebben van uw organisatie. U ontvangt daarvoor van ons een eenvoudig intake formulier. In dit formulier kunt u uw gegevens invullen en wat de context is van uw organisatie. Wat doet u precies, welke processen heeft u, hoeveel FTE werken er in uw organisatie.

Dit is het begin van het formele Audit proces, wij willen goed weten wie u bent en wat u doet. Immers uw organisatie is leidend, niet de norm.

Met de ontvangen informatie gaan we een berekening maken. Het begin van de calculatie begint altijd met het aantal FTE, dit is zo door de norm, waaraan wij moeten voldoen zo bepaald. Met alle ontvangen informatie zullen wij een offerte uitbrengen.

Tip; kijk altijd scherp naar het aantal FTE en inventariseer de functiegroepen en functies. Dit kan zomaar veel tijd en certificering kosten besparen.

De certificeringaudit zal bestaan uit fase 1 en fase 2. Tijdens fase 1 kijken we goed naar uw documentatie en willen we een beeld vormen of het managementsysteem ook echt aanwezig is. Werkt het en bent u dus klaar voor fase 2. Bij fase 2 kijken we goed naar de implementatie van al uw procedures en de aantoonbaarheid daarvan.

Na iedere fase krijgt u direct na de audit een auditrapport. Bij een positieve afronding van fase 2 ontvangt u het officiële certificaat.

BIO compliance verklaring of combineren met een ISO27001 certificering?