Implementatie van de BIO met IC Control en IC Content

De implementatie van de BIO kost veel tijd. Bovendien: waar begin je? Met de tools van SafeHarbour IC Content en IC Control kun je direct aan de slag met de implementatie van de BIO. De IBD heeft een stappenplan opgesteld om de BIO te implementeren. Op basis van dit stappenplan met 13 stappen lichten wij in dit document toe hoe je met gebruik van de tools van SafeHarbour de stappen eenvoudig kunt doorlopen. De functionaliteit en content van de tools schelen je veel tijd in het implementeren. Gelukkig begin je niet van nul af aan. Je hebt immers al de maatregelen uit de BIG geïmplementeerd die voor een deel terugkomen in de BIO.

Iedere stap heeft SafeHarbour voor jou nader toegelicht met wat er van jouw organisatie wordt gevraagd én hoe onze tools concreet hierbij helpen.

SafeHarbour

Stap 1

Voer de GAP-analyse uit voor alle gemeenschappelijke en centraal genomen controls en maatregelen, maak daarbij gebruik van de GAP-analyse aanpak van de IBD.

IC Control van SafeHarbour bevat alle normen, controls en maatregelen van de BIO. Wanneer je op maatregel niveau aangeeft of er voldaan wordt aan de maatregel werkt dat door op de controls en de normen. Daardoor heb je via het dashboard direct inzicht in welke thema's aandacht nodig hebben. Zie stap 9 voor de uitleg over labels.

Binnen IC Content is ook de BIO als normenkader opgenomen. Per norm is aangegeven wat er gedaan moet worden. Bovendien vind je diverse links naar documenten die je kunt gebruiken bij de implementatie.

Stap 2

Inventariseer de bedrijfsprocessen volgens het interne model van procesbeschrijvingen en maak een keuze over welke eerst aan te pakken (op basis van belangrijkheid). (vraag 4) Deze verantwoordelijke moet (eventueel onder begeleiding van de CISO) in workshop verband de baselinetoets voor zijn bedrijfsproces uitvoeren.

In IC Control kun je een proces en verwerkingsregister opnemen. Bij praktisch alle processen komen we uit op het niveau BBN2. Deze vorm van classificeren zegt dus nog weinig over wat we eventueel extra moeten doen om de bedreigingen weg te nemen. Het zegt wel iets over het basisniveau (overheid verplichte maatregelen) wat geïmplementeerd te worden.

Binnen IC Control is er nog wel de mogelijkheid geboden om de BIV-classificatie aan te brengen. Op grond van deze classificatie kun je inschatten of een diepgaande risicoanalyse noodzakelijk is. Op grond van de aard van het proces of specifieke proceseigenschappen kun je aangeven wat de risicoprocessen zijn. Dit zijn uiteraard de processen die jouw eerste aandacht vragen. Vanzelfsprekend kun je zo gedetailleerd gaan als je wilt. Echter is ons advies, begin klein en breidt daarna uit.

Vanuit SafeHarbour adviseren we jou om deze vraag te combineren met vraag 4. Een baseline toets is namelijk per definitie gericht op het classificeren van jouw processen.

Binnen IC Content hebben we ondersteunende artikelen die je als naslag kunt gebruiken en die je helpen om een BIV-classificatie uit te voeren.

Stap 3

Zoek de verantwoordelijke voor het bedrijfsproces en vertel hem het belang van de baselinetoets en zijn rol in het geheel van de BIO.

Als CISO en FG is het belangrijk om vooral een coördinerende rol te hebben. Geef daarom aan wie van een norm en proces de eigenaar is. Zodoende kun je binnen IC Content aangeven wie een beleidsstuk / procedure of bijlage actueel moet houden. Daarnaast kun je taken uitzetten en de voortgang bewaken. Deze functionaliteit tref je zowel in IC Content aan, als in IC Control.

De artikelen binnen IC Content geven extra informatie aan de proces eigenaren en de vakspecialisten. Daardoor lopen ze niet tegen het probleem aan dat ze niet weten wat er wordt bedoeld met een bepaalde norm. Zo voorkom je dat de voortgang stagneert.

Stap 4

Voer indien nodig een diepgaande risicoanalyse uit bij afwijkende betrouwbaarheidseisen van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid (BIV)).

Een classificatie is niet hetzelfde is als een risicoanalyse. De classificatie helpt wel bij het bepalen van een prioriteit van het oppakken van bedreiging.

Binnen IC Control zijn vragenlijsten opgenomen. Deze vragenlijsten zijn gekoppeld aan bedreigingen die op basis van kans van optreden en potentiële schade van toepassing kunnen zijn op de organisatie. Doordat de vragenlijsten laagdrempelig zijn opgesteld kunnen proceseigenaren en vakspecialisten de vragen zelf beantwoorden. De vragen zijn op de achtergrond gekoppeld aan bedreigingen en de bedreigingen op hun beurt weer aan maatregelen. Er is daarom geen specialistische kennis nodig bij het bepalen van de extra noodzakelijke maatregelen om een bedreiging terug te brengen op acceptabel niveau.

Omdat de BIO een sub-set is van de ISO27002, is de ISO27002 ook gekoppeld. Zo beschik je over een ruime keus aan mogelijke maatregelen en kun je voldoen aan de eis uit de BIO om extra maatregelen te identificeren en te implementeren.

IC Control helpt je daarmee bij het identificeren van bedreigingen en bewaakt de tijdige afhandeling daarvan met gebruik van het takenbeheer in IC Control.

Stap 5

Voer een data protection impact assessment (DPIA) uit als dat verplicht is en deze nog niet eerder uitgevoerd was.

Een DPIA is niet meer en niet minder dan een risicoanalyse die is gericht op de privacy van de betrokkene. In diverse vragenlijsten van de risicoanalyse is ook privacy opgenomen.

Stap 6

Zoek in de BIO de controls en verplichte maatregelen bij het geselecteerde BBN om de gevonden risico's adequaat te beheersen.

Deze extra stap is niet meer van toepassing, omdat deze door SafeHarbour is geïntegreerd in de stappen 4 en 5.

Stap 7

Selecteer (bijvoorbeeld op basis van de ISO 27002) of bedenk passende maatregelen bij de controls uit de BIO waar geen verplichte maatregelen bij staan en leg dit vast.

Ook deze extra stap is niet meer van toepassing, omdat deze door SafeHarbour is geïntegreerd in de stappen 4 en 5. Nog efficiënter!

Stap 8

Noteer de controls die niet van toepassing zijn, onderbouw waarom deze niet van toepassing zijn en bewaar het verslag van de analyse, dit is de ingevulde baselinetoets en de eventueel uitgevoerde diepgaande risicoanalyse en eventueel de uitgevoerde DPIA.

Binnen de ISO27001 noemen we dit de verklaring van toepasselijkheid (vvt). Binnen de ISO27001 methodiek dien je per norm aan te geven waarom een norm wel of niet van toepassing is. Omdat de BIO in principe verplicht is hoef je binnen IC Control alleen bij het niet van toepassing verklaren een motivatie toe te voegen.

Stap 9

Cluster de controls en te treffen maatregelen naar soort en verdeel ze indien nodig onder andere uitvoerders binnen de gemeente of samenwerking (PIOFAH).

In IC Control is het mogelijk 'labels' aan te maken. Door labels aan de maatregelen te koppelen is in het overzicht 'maatregelen' eenvoudig te clusteren per label.

De labels vertegenwoordigen de thema's van de GAPS en koppel je aan maatregelen, zodat in het maatregelenoverzicht een duidelijk overzicht ontstaat binnen welke thema's GAPS ontstaan.

Ook binnen IC Content kunnen labels worden aangebracht Daar wordt het een TAG genoemd. Via het management dashboard krijg je inzicht in de actualiteit van de richtlijnen en de procedures op TAG niveau.

Stap 10

Zoek aansluiting bij het organisatorische ISMS en neem daar de maatregelen en uitvoerders op ter monitoring, gebruik zo mogelijk een Governance, Risk en Compliance (GRC)-tool.

Wanneer we kijken naar de kwaliteitsbeheersing van een organisatie dan zijn informatiebeveiliging en privacy maar twee aspecten die hierbinnen een rol spelen. Ook op het gebied van financiën en compliance dient er een PDCA cyclus te worden ingericht. Wij adviseren om daar waar mogelijk de zaken te integreren waardoor de onderwerpen elkaar versterken.

Stap 11

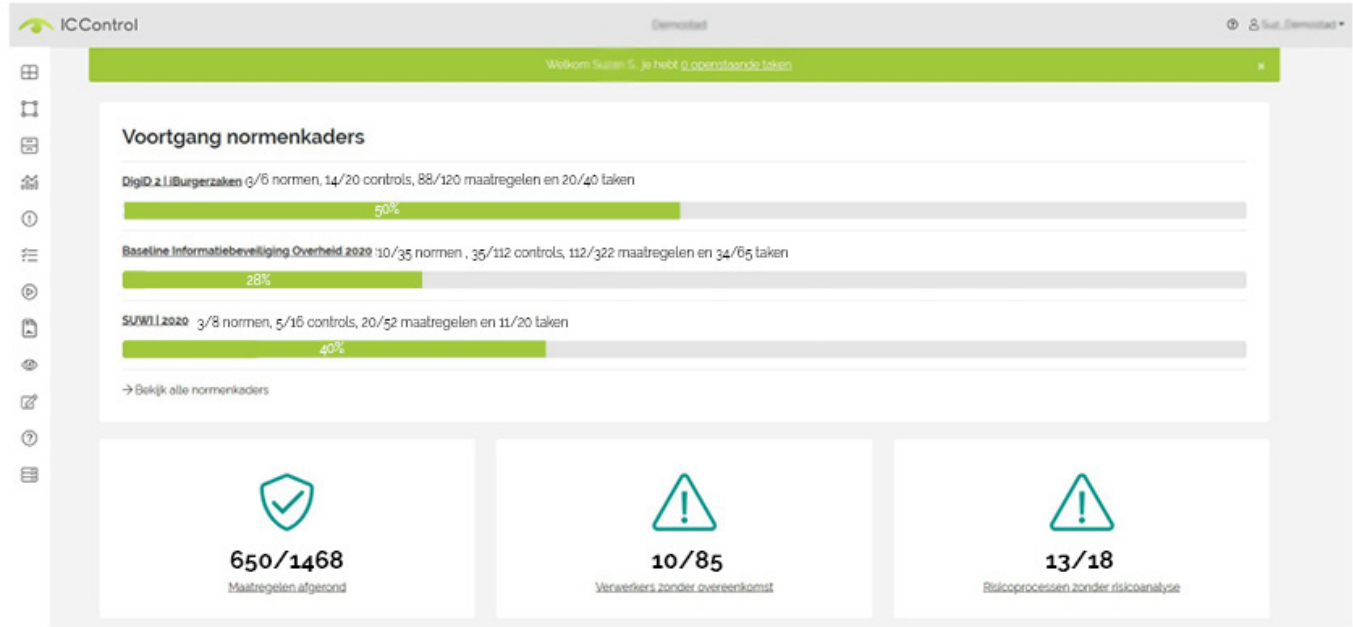
Voer over de eigen controls en maatregelen een GAP-analyse (verschillenanalyse) uit om vast te stellen wat nog gedaan moet worden en neem de GAP op in een ISMS en/of in het (integraal) informatiebeveiligingsplan zodat ze gepland worden voor implementatie.

Doordat je vanuit de ISO27002 extra maatregelen kunt koppelen in IC Control kun je ook hier controle op uitvoeren en de voortgang blijven monitoren. Wanneer je alles consistent invoert en de noodzakelijke stappen zet, is de stap naar certificeren volgens de ISO27001 niet ver meer.

Stap 12

Bewaak de voortgang van de implementatie (risicomanagement).

Het dashboard van IC Control geeft je inzicht in hoe je ervoor staat. En ja, het is nooit af. Het is een continu proces van verbeteren. Wanneer je denkt dat je er bent komt er een nieuwe wettelijke taak bij of wordt er intern gereorganiseerd. Het is dus een utopie om te denken dat je ooit volledig aan de BIO gaat voldoen. Je blijft dus aan het werk. Leuker kunnen we het niet maken, wel makkelijker.



Voortgang normenkaders dashboard IC Control

Ondersteuning en advies voor de BIO

Wil je meer weten over wat de BIO voor jouw organisatie gaat betekenen en hoe onze tools en de SafeHarbour-consultants en -auditoren kunnen ondersteunen en helpen? Neem voor een vrijblijvende demo of gesprek contact met ons op via telefoonnummer 085 – 30 30 279 of per e-mail naar info@safeharbour.nl

SafeHarbour