Informatiebeveiligingsplan 2020-2022

ISD-BOL

Eindhoven, 1 januari 2020
Versie: 1.0
2019FR349

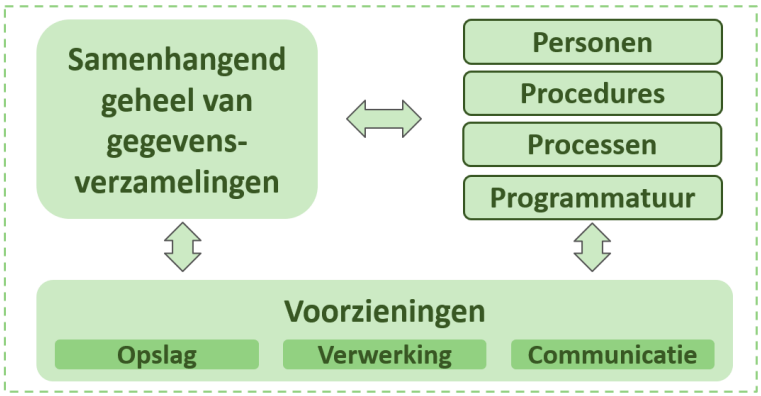
1 Informatiebeveiligingsplan ISD-BOL

ISD-BOL heeft een informatiebeveiligingsbeleid vastgesteld op basis van de Baseline Informatiebeveiliging Overheid (hierna BIO). De richtlijnen uit het beleid worden tot uitvoering gebracht op basis van dit informatiebeveiligingsplan dat de periode 2020-2022 bestrijkt.
Dit plan beschrijft de te implementeren beveiligingsmaatregelen op basis van de organisatie brede GAP-analyse die in het laatste kwartaal van 2019 is uitgevoerd. Voor deze GAP-analyse zijn de aanwezige maatregelen afgezet tegen de maatregelen die vanuit de BIO-norm voor informatiebeveiliging worden verwacht.

2 Plan en aanpak

Om een concrete invulling te geven aan informatiebeveiliging is dit plan opgesteld. Hierin worden duidelijke doelen gesteld met een specifieke tijdslijn voor de komende drie jaar.

In dit informatiebeveiligingsplan wordt de organisatie als een set van informatiesystemen benaderd. Een informatiesysteem is een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie (bron: BIO 1.03). Hieronder is de samenhang van de onderdelen in een informatiesysteem schematisch weergegeven:



Binnen ISD-BOL zijn er verschillende informatiesystemen die organisatiebreed de beveiliging afdekken. Denk hierbij aan beveiligingsmaatregelen die worden getroffen op facilitair gebied, gebouwbeheer, ICT-beheer en personeelszaken. Deze organisatiebrede informatiebeveiliging inclusief de benodigde maatregelen komen verder aan bod in hoofdstuk 3. In dit hoofdstuk wordt daarbij extra aandacht besteed aan:

1. Rollen, verantwoordelijkheden en overlegstructuren
2. Bewustwording en opleiding
3. Beveiliging van dienstverlenende partijen

De organisatiebrede maatregelen bieden een basisbeschermingslaag voor de andere informatiesystemen. In deze andere informatiesystemen moeten specifieke informatiebeveiligingsmaatregelen ingericht worden. Het bepalen van deze informatiesystemen en de wijze waarop deze maatregelen ingericht worden, komt verder aan bod in hoofdstuk 4. In dit hoofdstuk komt ook aan bod op welke wijze rapportage en sturing ingericht moet worden om

ISD-BOL in control te laten zijn op het gebied van informatiebeveiliging. Deze rapportage en sturing moet niet alleen toegepast worden op de specifieke informatiesystemen, maar ook ten aanzien van de organisatiebrede informatiesystemen.

3 Organisatiebrede maatregelen en afspraken met dienstverleners

De maatregelen die ISD-BOL dient te treffen komen voort uit het informatiebeveiligingsbeleid en de BIO. De BIO bevat een groot aantal controls en onderliggende overheidsmaatregelen die geïmplementeerd dienen te worden. De BIO stelt dat implementatie van de overheidsmaatregelen verplicht is voor gemeenten en dus ISD-BOL. Onderstaand een overzicht van drie belangrijke onderwerpen rondom organisatiebrede informatiebeveiliging.

#	Onderwerp	Verantwoordelijke
1	Benoemen rollen, verantwoordelijkheden en overlegstructuren.	Management
2	Bewustwording en opleidingen.	CISO
3	Evalueren en eventueel herzien contracten dienstverlenende partijen.	CISO/ Management

Planning

	2020				2021				2022			
	1	2	3	4	1	2	3	4	1	2	3	4
Benoeming rollen, verantwoordelijkheden en overlegstructuren												
Bewustwording en opleiding												
Evalueren en enventueel herzien contracten dienstverlenende partijen.												

3.1 Benoemen rollen, verantwoordelijkheden en overlegstructuren

In het informatiebeveiligingsbeleid zijn de verschillende rollen beschreven. Deze rollen dient het management formeel vast te stellen en vervolgens te beleggen binnen de organisatie.
De CISO zal de werkgroep Privacy en Informatieveiligheid (PIV) op zetten en zorgt dat deze minstens zes keer per jaar overleg pleegt over in het informatiebeveiligingsbeleid geformuleerde takenpakket. Verder krijgt elk proces een proceseigenaar waardoor duidelijk is wie rapporteert en verantwoordelijk is. De rapportage en sturing komt verder aan bod in het informatiebeveiligingsbeleid en in hoofdstuk 4 van dit plan.

#	Actie	Verwachte tijdsbesteding	Verantwoordelijke
1	Rol en taken van CISO beschrijven en formaliseren	8 – 10 uur	CISO/P&O
2	Rol en taken van Privacy Officer beschrijven en formaliseren	8 – 10 uur	CISO/PO/P&O
3	Koppel processen aan proceseigenaren	24 – 30 uur	CISO/proceseigenaren/ lijnmanagement
4	Opstellen werkgroep PIV, planning maken en meetings voorbereiden	8 – 10 uur	CISO

Planning

	2020											
	jan	feb	mrt	apr	mei	jun	jul	aug	sept	okt	nov	dec
Verankeren profiel CISO en PO in functieprofiel												
Beleg proceseigenaren												
Zet werkgroep PIV op (Privacy en informatieveiligheid)												

3.2 Bewustwording en opleidingen

Menselijk handelen is een van de grootste bedreigingen voor informatieveiligheid. Hoewel het feit is dat waar mensen werken fouten worden gemaakt, kunnen met de juiste training, opleiding en organisatiecultuur de risico's aanzienlijk verkleind worden. Momenteel is er een themapagina informatiebeveiliging op intranet aanwezig, worden beveiligingsincidenten en datalekken achteraf besproken in vergaderingen en er is een introductie e-learning over veilig gebruik van Suwinet. Maar om privacy en informatieveiligheid voldoende te verankeren in de organisatiecultuur is een bewustwordingstraject noodzakelijk. Een bewustwordingstraject op het gebied van informatiebeveiliging biedt houvast om medewerkers bewuster te maken van informatiebeveiliging. Ook de risico's die gemoeid zijn met bepaalde handelingen binnen hun dagelijkse werkzaamheden komen hierdoor aan bod. Door middel van herhaling van dit thema kan een meer permanent effect behaald worden.

Een goed moment voor een start van bewustwording van medewerkers is het indiensttredingsproces. Daarom dient ISD-BOL een korte interne training aan te bieden ten aanzien van informatiebeveiliging en privacy tijdens het indiensttredingsproces zodat medewerkers vanaf het begin weten hoe zij veilig om gaan met informatie.

Om een bewustwordingstraject helemaal goed te borgen in de organisatie moet permanent en cyclisch leren worden geïmplementeerd, waardoor periodiek aandacht wordt gevraagd aan alle aspecten van leren over deze onderwerpen op een natuurlijke en blijvende manier. Dit omvat allereerst een 0-meting om te zien waar de organisatie staat en welke onderwerpen extra aandacht verdienen. Vervolgens geeft de CISO een workshop aan alle collega's. Hierna kan het de verandering in niveau getest worden door vragenlijsten of bijvoorbeeld een phishingtest.

Afhankelijk van de uitslagen kan weer een vervolg worden gegeven aan de bewustwordingscampagne.

De volgende acties dienen uitgevoerd te worden (tevens is een indicatie gegeven voor de tijd die in een dergelijk cyclisch plan verwacht moet worden voor uitvoering van de diverse elementen):

#	Actie	Verwachte tijdsbesteding	Verantwoordelijke
1	Stel een plan voor permanent en cyclisch leren op en bepaal/beschrijf: - de doelstellingen; - de relevante stappen; - de start; - de planning.	12 – 24 uur	CISO
2	Creëer het materiaal voor het traject.	36 – 40 uur	CISO
3	Creëer de 0-meting en voer deze uit.	16 – 24 uur	CISO
4	Creëer een korte interne opleiding ten aanzien van informatiebeveiliging en privacy voor tijdens het indiensttredingsproces.	16 – 20 uur	CISO/Privacy Officer
5	Voer het traject uit (posters ophangen, workshops, etc.).	16 – 24 uur	CISO
6	Meet de resultaten van het ontwikkeltraject (vragenlijsten, phishingtest, etc.).	8 – 16 uur	CISO
7	Pas het plan aan op basis van de testresultaten.	4 – 8 uur	CISO

Planning

	2020/2021/2022											
	jan	feb	mrt	apr	mei	jun	jul	aug	sept	okt	nov	dec
Stel een plan voor permanent en cyclisch leren op in de vorm van een bewustwoordingscampagne												
Creer het materiaal voor de campagne												
Creer een 0-meting en voer deze uit												
Creer een korte interne opleiding ten aanzien van PIV voor het indiensttredingsproces												
Voer de bewustswordingscampagne uit workshop, e-learning, etc												
Meet de resultaten van de bewustwordingscampagne												
Pas het plan aan op basis van de resultaten												

3.3 Evalueren en eventueel herzien contracten dienstverlenende partijen

Onderwerpen als facilitaire zaken, gebouwbeheer en ICT hebben een grote impact op informatiebeveiliging. Omdat ISD-BOL een deel van deze processen aan de gemeente Landgraaf en gemeente Brunssum uitbesteedt, dienen deze gemeenten een aantal zaken ten aanzien van informatiebeveiliging op orde te hebben. Deze duidelijke afspraken dient ISD-BOL vast te leggen in zogenaamde dienstverlenersovereenkomsten (hierna: DVO(s)) die ISD-BOL met de gemeenten of andere derde partijen heeft. Voor beide gemeenten is een DVO aanwezig. Echter zijn deze gedateerd en dient geactualiseerd te worden.

De volgende acties dienen uitgezet te worden om de relevante onderdelen, zoals hieronder in de tabel nader uitgewerkt, vast te leggen.

#	Actie	Verwachtte tijdsbesteding	Verantwoordelijke
1	Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van fysieke veiligheid	16-24 uren	Dagelijks bestuur
2	Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van bedrijfscontinuïteit	16-24 uren	Dagelijks bestuur
3	Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van gebouwbeheer.	16-24 uren	Dagelijks bestuur
4	Opstellen van eisen voor DVO gemeente Landgraaf ten aanzien van ICT.	16-24 uren	Dagelijks bestuur

Planning

	2022											
	jan	feb	mrt	apr	mei	jun	jul	aug	sept	okt	nov	dec
Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van fysieke veiligheid												
Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van bedrijfscontinuteit												
Opstellen van eisen voor DVO gemeente Brunssum ten aanzien van gebouwbeheer.												
Opstellen van eisen voor DVO gemeente Landgraaf ten aanzien van ICT.												

3.4 Controls en overheidsmaatregelen

Eind 2019 is een GAP-analyse uitgevoerd ten aanzien van de organisatiebrede informatiesystemen van ISD-BOL. Dit betreffen de onderdelen ten aanzien van facilitaire zaken, gebouwenbeheer, ICT-beheer en personeelszaken. Hierbij is de status van informatiebeveiliging in kaart gebracht. Hieronder volgt het overzicht van controls en overheidsmaatregelen voor organisatiebrede beveiliging die nog opgepakt dienen te worden. Hierbij is ook een korte omschrijving opgenomen en een vertaling naar de BIO-maatregelen. Verder is er een korte toelichting vanuit de GAP-analyse opgenomen. De volgorde van de maatregelen geeft de prioritering weer, waarbij maatregel nummer één de hoogste prioriteit heeft.

#	Maatregelen	Korte omschrijving	BIO	Toelichting
1	Informatiebeveiligings-beleid	Opstellen en vaststellen van een informatiebeveiligings-beleid met periodieke herziening.	5.1.1.1; 5.1.2.1	Vaststellen en jaarlijks herzien
2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1; 6.1.1; 6.1.1.2; 6.1.1.3; 6.1.1.4; 6.1.5	CISO en PO rol en verantwoordelijkheden definiëren, vaststellen en opnemen in functieprofiel. Verder dient Informatiebeveiliging aan de orde te komen in projectbeheer, ongeacht het soort project.
3	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	18.1.4; 18.1.4.2	Een register van verwerkingen moet samengesteld worden. Daarnaast bij relaties zullen ontbrekende verwerkingsovereenkomsten afgesloten moeten worden.
4	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	7.1.2;7.1.2.1;7.2.1	Herzien van de integriteitsverklaring t.b.v. informatiebeveiliging.
5	Naleving	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	18.2.1; 18.2.1.2; 18.2.2.1; 18.2.3.1	Er dient een information security information system (ISMS) aanwezig te zijn waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze afgedekt wordt. Daarbij is er een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.

6	Toegangsbeleid en autorisatiematrix	Opstellen van een toegangsbeleid en autorisatiematrix document + een procedure voor periodieke review.	6.1.2.1; 9.2.3.1; 9.2.5.2; 9.2.5.3; 9.4.1.1; 9.4.1.2	Autorisatiematrix voor alle aplicaties opstellen, en deze periodieke beoordeling
7	BCM/BCP	Vaststellen kritieke processen voor bedrijfscontinuïteit. Vaststellen bedrijfscontinuïteitplan. Afspraken maken over redundantie met gemeente Brunssum.	17.1.3.1; 17.1.3.2; 17.1.3.3	Geen calamiteitenplan en geen beheerst proces voor een calamiteit. Meenemen in evaluatie DVO gemeente Brunssum
8	Fysieke beveiliging	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast	11.1.1.1; 11.1.2.1; 11.1.3.1; 11.1.4.1; 11.1.4.2; 11.2.9.1; 11.2.9.3; 11.2.9.4	Alle aanwezigen in gebouw van gemeente Brunssum hebben toegang tot bedrijfsruimte ISD-BOL. Beveilig toegang tot bedrijfsruimte ISD-BOL (conform het informatiebeveiligings-beleid) binnen het gebouw van de gemeente Brunssum.
9	Leveranciersrelaties	Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	15.1.1; 15.1.1.1; 15.1.1.2; 15.1.1.3; 15.1.2;15.1.2.3; 15.1.2.4; 15.1.2.5; 15.1.2.6; 15.2.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, dienen eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) te worden benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging. Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leverancierstoegang tot bedrijfsinformatie vastgesteld. Bestaande contracten van leveranciers dienen op dit onderdeel herziend te worden. Jaarlijks wordt daarbij de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.

10	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	14.1.1;14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.
11	Beveiliging bedrijfsvoering	De informatie verwerkende omgeving wordt gemonitord middels detectie-voorzieningen, die worden ingezet op basis van een risico-inschatting zodat aanvallen kunnen worden gedetecteerd.	12.4.1.3	Geen SIEM en/of SOC middels detectie-voorzieningen aanwezig. Meenemen in evaluatie DVO gemeente Landgraaf.
12	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	6.2.1;6.2.1.1;6.2.1.2;6.2.2	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat de mogelijkheid om de gegevens te versleutelen en moet 'wissen op afstand' mogelijk zijn d.m.v. een MDM Mobile Device Management (MDM)-oplossing.

Planning

	2020				2021				2022			
	1	2	3	4	1	2	3	4	1	2	3	4
Informatiebeveiligingsbeleid												
Rollen en verantwoordelijkheden bij informatiebeveiliging												
Privacy en bescherming van persoonsgegevens												
Arbeidsvoorwaarden												
Toegangsbeleid en autorisatiematrix												
Leveranciersrelaties												
Acquisitie, ontwikkeling en onderhoud van informatiesystemen												
Beveiliging bedrijfsvoering												
Beleid voor mobiele apparatuur												

4 Stappenplan BIO informatiesystemen

Zoals aangegeven is een informatiesysteem is een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie (bron: BIO 1.03). Om de risico's rondom informatieveiligheid te beheersen zal hier een methodiek voor eigenaarschap, implementatie, rapportage en sturing op moeten worden toegepast. Dit geldt voor informatiesystemen die organisatiebreed voor beveiliging zorgen (zie hoofdstuk 3), maar ook voor informatiesystemen waarbij specifieke maatregelen getroffen moeten worden. In dit hoofdstuk ligt de focus op het implementeren van de BIO voor informatiesystemen met specifieke maatregelen. Het stappenplan dient echter ook toegepast te worden op de organisatiebrede informatiesystemen.

Onderstaand overzicht geven de stappen weer die gevolgd moeten worden voor het uitvoeren van een gedegen implementatie van de BIO.

1. Informatiesystemen bekend en eigenaarschap vastgelegd
2. Baselinetoets en niveau vastleggen (BBN-analyse)
3. GAP-analyse maatregelen door proceseigenaar
4. Selectie en toewijzing van controls & maatregelen aan eigenaar
5. Implementatie en borging maatregelen door proceseigenaar
6. Monitoring status via ISMS en periodieke rapportage en sturing

In de volgende alinea's zullen deze stappen concreet toegelicht worden.

4.1.1 Vaststellen informatiesystemen en eigenaarschap

Het belangrijkste informatiesysteem binnen ISD-BOL is de participatie-opdracht. Voor dit informatiesysteem dient een eigenaar vastgesteld te worden door het dagelijks bestuur. Daarnaast zal de CISO dienen te onderzoeken of er meer informatiesystemen binnen ISD-BOL afgebakend dienen te worden. Uiteindelijk bepalen de eigenaren van de informatiesystemen wat binnen de scope van die informatiesystemen valt.

4.1.2 Vaststellen basisbeveiligingsniveaus

In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per informatiesysteem bepaalt het lijnmanagement het BBN. Een BBN is het niveau dat aangeeft welke maatregelen er aanwezig moeten zijn op het gebied van informatiebeveiliging. Om te bepalen of een informatiesysteem een bepaald Basis Beveiligings Niveau (BBN) heeft of meer maatregelen nodig heeft wordt een BBN-toets uitgevoerd. De uitkomsten kunnen dan worden gebruikt om te bepalen welke maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Deze maatregelen kunnen worden verkregen uit een voorgedefinieerde lijst met maatregelen bovenop de baseline, of door een aanvullende diepgaande risicoanalyse. Voor ieder informatiesysteem binnen ISD-BOL dient het basisbeveiligingsniveau (BBN) te worden vastgesteld om inzicht te krijgen welk informatiesysteem het meest kritiek is en dus de meeste aandacht verdient rondom beveiligingsmaatregelen. Gemeenten hanteren hiervoor drie verschillende niveaus welke in onderstaande tabel zijn weergegeven.. De CISO begeleidt dit proces waarbij de eigenaar van het informatiesysteem de uiteindelijke keuze maakt welk BBN van toepassing is.

BBN	Omschrijving	Toelichting
BBN1	Basisniveau	Informatiesystemen op BBN1 zijn systemen waar BBN2 te zwaar voor is. Overheidssystemen moeten als minimum aan BBN1 voldoen. Controls en overheidsmaatregelen komen voor uit wet- en regelgeving en algemene beveiligingsprincipes.
BBN2	Niveau (bijna) alle	BBN2 vormt voor informatiesystemen binnen de overheid het uitgangspunt. BBN2 is van toepassing indien er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten leiden tot bestuurlijke commotie of de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem. Controls en maatregelen van BBN2 bevatten de controls

	gemeentelijke processen	en maatregelen van BBN1. Daarnaast komen controls en maatregelen voor BBN2 voor uit: 〉 wet- en regelgeving; 〉 aansluitvoorwaarden van gemeentelijke diensten; 〉 afhankelijkheden in ketens en netwerken; 〉 minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.
BBN3	Niveau AIVD, kritieke infrastructuur, staatsgeheimen	BBN3 is van toepassing op departementaal vertrouwelijke informatie waarbij weerstand tegen dreigingen van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3.

Bron: Baseline Informatiebeveiliging Overheid, versie 1.03.

4.1.3 GAP-analyse maatregelen door proceseigenaar

De GAP-analyse is een methode om een vergelijking te maken tussen de huidige situatie en gewenste situatie met hierin de controls en overheidsmaatregelen uit de BIO. De organisatiebrede GAP-analyse is gemaakt in het vierde kwartaal 2019. In deze stap wordt een GAP-analyse gemaakt voor individuele informatiesystemen. Dit wordt uitgevoerd door de verantwoordelijke manager, waarbij deze ondersteund en geadviseerd wordt door de CISO.

4.1.4 Selectie en toewijzing van controls & maatregelen aan eigenaar

Nadat helder is hoe de huidige situatie eruit ziet, worden controls en overheidsmaatregelen geselecteerd waarmee de 'GAP' overbrugt kan worden naar de gewenste situatie. Voor een succesvolle implementatie is het van groot belang dat voor elke control en maatregel een eigenaar wordt toewezen en er een planning aan wordt gekoppeld. De CISO begeleidt dit proces waarbij de eigenaar van het informatiesysteem de uiteindelijke keuze maakt welke controls en overheidsmaatregelen in welke volgorde toegevoegd moeten worden. De overheidsmaatregelen zijn verplicht.

4.1.5 Implementatie en borging maatregelen door proceseigenaar

Als de geselecteerde controls en maatregelen een eigenaar hebben en er een heldere planning aan ten grondslag ligt, kan aan de implementatie begonnen worden. Hierbij dient op basis van risicomanagement een afweging gemaakt te worden in prioriteit. Hoofdstuk 4 van dit plan geeft al richting aan geven wat prioriteit heeft op organisatiebreed gebied binnen ISD-BOL. Daarnaast kan er ook kritisch gekeken worden welke quick-wins te behalen zijn. De PDCA-cyclus moet zijn opgenomen in het ontwerp van de maatregel zoals beschreven in het beleid.

4.1.6 Monitoring, periodieke rapportage en sturing

Wanneer de controls en overheidsmaatregelen worden uitgevoerd dienen deze gemonitord te worden. Het ISMS speelt hierin een sleutelrol als beheersingsmethodiek. Het gaat om controle-cyclus die toegepast moet worden op afzonderlijke controls en overheidsmaatregelen. ISMS-tooling biedt hierbij een ondersteunende rol. Hierbij wordt telkens het risico tegenover de uitvoering en kwaliteit gezet. De proceseigenaar is verantwoordelijk dat de control of

overheidsmaatregel goed wordt geïmplementeerd, uitgevoerd en eventueel bijgesteld. Tussentijds moet de proceseigenaar telkens de afweging maken of tijd, middelen en budget afdoende zijn, of dat er bijgestuurd moet worden. Risico's met een kleine impact kunnen op een lager niveau in de organisatie geaccepteerd worden. Echter als het risico een significante invloed heeft op de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatie en de bedrijfsvoering van de organisatie dan beslist het dagelijks bestuur of het risico acceptabel is of dat (extra) maatregelen getroffen dienen te worden. De CISO ondersteund bij dit proces en geeft een advies.

Naast de cyclus voor specifieke controls en overheidsmaatregelen volgt er ook een periodieke rapportage. De CISO heeft hierin een coördinerende rol. Jaarlijks wordt door de CISO een rapport opgeleverd met hier een beschrijving van de huidige situatie, de gewenste situatie, de voortgang die gemaakt is, en de planning voor het komend jaar. Verder bevat dit rapport ook een advies over mogelijke bijstelling van deze planning. De CISO dient hier jaarlijks een rapportage over op te stellen en zal deze voor leggen aan het Management en het Dagelijks Bestuur. Hierdoor blijft het Management en het Dagelijks Bestuur op de hoogte van de huidige situatie, en kunnen zij indien nodig sturing geven. Naast dit jaarlijkse rapport dient er ook per kwartaal een status update afgegeven te worden waarmee op hoger niveau de voortgang in grote lijnen kan monitoren. Wanneer blijkt dat er zich nieuwe risico's aandienen of dat risico's onvoldoende zijn afgedekt zal het dagelijks bestuur besluiten om risico's te accepteren of bij te sturen. De CISO en PO kunnen het dagelijks bestuur hierbij ondersteunen en adviseren.

#	Actie	Verwachtte tijdsbesteding *	Verantwoordelijke
1	Informatiesystemen bekend en eigenaarschap vastgelegd	5 – 8 uren	CISO/ Leidinggevenden
2	Baselinetoets en niveau vastleggen (BBN-analyse)	4 uur	CISO/ proceseigenaren
3	GAP-analyse maatregelen door proceseigenaar	4 – 8 uren	CISO/ proceseigenaren
4	Selectie en toewijzing van controls & maatregelen aan eigenaar	2 – 4 uren	CISO/ proceseigenaren
5	Implementatie en borging maatregelen door proceseigenaar	Afhankelijk van de te treffen maatregelen.	CISO, proceseigenaren, procesdeskundigen en applicatiebeheerders
6	Monitoring status via ISMS en periodieke rapportage en sturing	4 uur	CISO/Dagelijks bestuur

* Tijdsindicatie is per proceseigenaar.

Planning

	2020				2021				2022			
	1	2	3	4	1	2	3	4	1	2	3	4
Informatiesystemen bekend en eigenaarschap vastgelegd												
Baselinetoets en niveau vastleggen (BBN-analyse)												
GAP-analyse maatregelen door proceseigenaar												
Selectie en toewijzing van controls & maatregelen aan eigenaar												
Implementatie en borging maatregelen door proceseigenaar												
Monitoring status via ISMS en periodieke rapportage en sturing												

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!