INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

GAP-analyse

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
GAP-analyse

Versienummer
2.0

Versiedatum
April 2019

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1	Augustus 2013	
1.0.1	Augustus 2016	Taskforce BID verwijderd, GBA vervangen door BRP en contactgegevens IBD aangepast
2.0	April 2019	BIO Update

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van de GAP-analyse is dat gemeenten kunnen controleren of en in welke mate de beveiligingsmaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) zijn geïmplementeerd. Hierbij gaat het om gemeenten die het onderzoek uitvoeren of laten uitvoeren.

Doelgroep

Dit document is van belang voor de verantwoordelijke die onderzoekt of en in welke mate de BIO binnen de gemeente is ingevoerd. Dit document is ook van belang voor de CISO, het management van de gemeente en de auditor.

Relatie met overige producten

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente
- Introductie aanpak BIO
- GAP-analyse (spreadsheet)
- Factsheet beleid BIG en BIO
- Geheimhoudingsverklaringen

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

- Geen specifieke verwijzingen.

INFORMATIE
BEVEILIGINGS
DIENST

Wat is er veranderd ten opzichte van de BIG?

Het verschil ten opzichte van de BIG is dat de BIO verplichte èn niet verplichte. De verplichte beveiligingsmaatregelen moeten altijd geïmplementeerd worden en zijn ook soms van toepassing op de hele gemeente. Er kan dus een eerste gemeente brede analyse over de verplichte controls en beveiligingsmaatregelen worden uitgevoerd door de CISO en de eindverantwoordelijke van de dienstverlening (bij gemeenten: de gemeentesecretaris) voor 3 basisbeveiligingsniveaus (BBN's). Een tweede analyse kan worden uitgevoerd in aanvulling op de eerste door de proceseigenaar nadat is vastgesteld welke aanvullende beveiligingsmaatregelen noodzakelijk zijn.

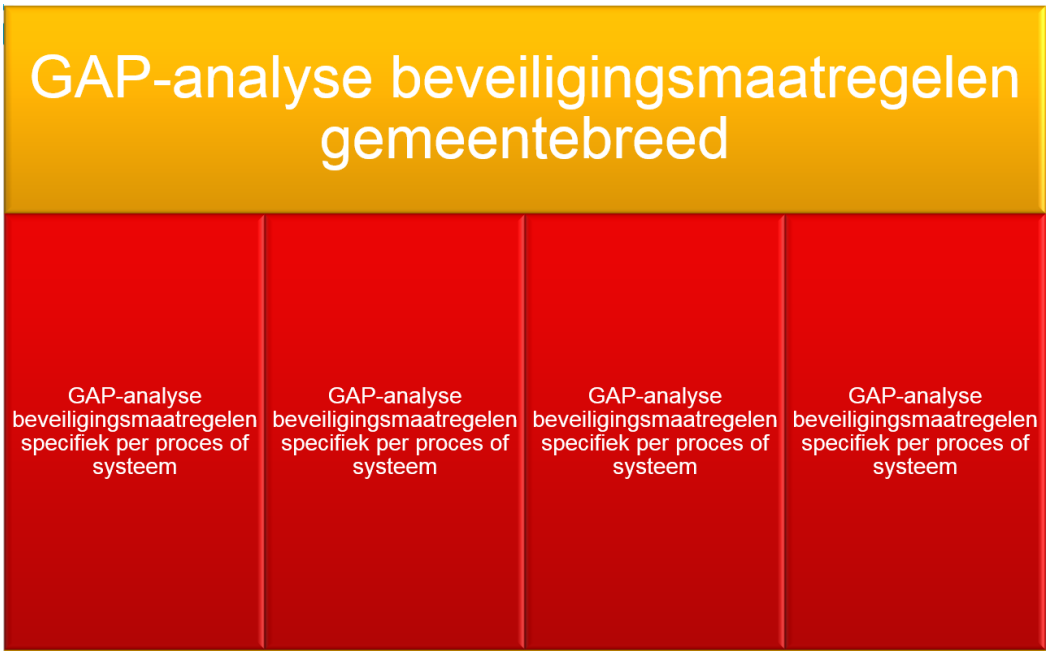
Inhoudsopgave

1. Inleiding

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van gemeenten. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.

De eerste stap in het beveiligingsproces is het maken van een risicoafweging. Daarbij wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende beveiligingsmaatregelen getroffen of wordt het (rest)risico geaccepteerd. De GAP-analyse biedt gemeenten de mogelijkheid om te controleren of en in welke mate de beveiligingsmaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) aanwezig zijn of geïmplementeerd zijn en welke nog niet. De GAP-analyse bevat alle beveiligingsmaatregelen uit de BIO met daarbij controlevragen. De GAP-analyse is een methode om een vergelijking te maken tussen een bestaande of huidige situatie en de gewenste situatie, de beveiligingsmaatregelen uit de BIO.

De GAP-analyse kan gebruikt worden als tweetrapsraket. Hiermee wordt bedoeld dat er beveiligingsmaatregelen van toepassing zijn op de hele gemeente en dat er beveiligingsmaatregelen specifiek van toepassing zijn afzonderlijke processen of informatiesystemen (zie figuur 1). Daardoor kan de eerste analyse over de controls en beveiligingsmaatregelen gemeentebreed/ centraal onderzocht worden door de Chief Information Security Officer (CISO) en de eindverantwoordelijke van de dienstverlening (bij gemeenten: de gemeentesecretaris). De andere analyses worden door de lijnverantwoordelijke[1] gedaan in aanvulling op de gemeentebrede analyse. Daarbij kan de lijnverantwoordelijke gebruik maken van wat er binnen de gemeentebrede/ centrale GAP-analyse al naar voren gekomen is.



Figuur 1 Verhouding gemeentebrede en specifieke GAP-analyse.

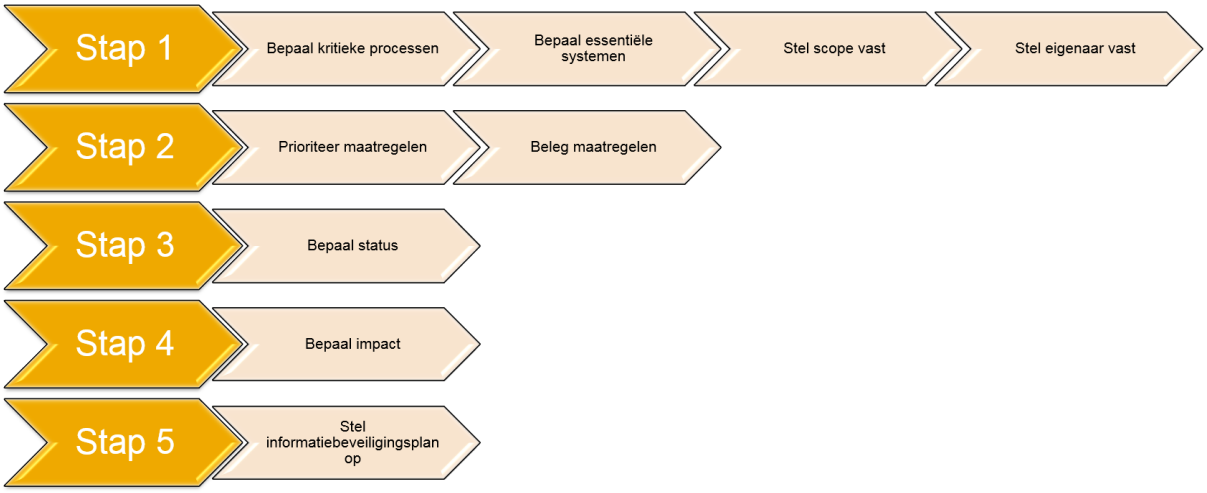
Het is verstandig om de spreadsheet GAP-analyse (bestand met extensie .xlsx) op te slaan onder een andere naam voordat men begint.

[1] Voor lijnverantwoordelijke kan ook proceseigenaar worden gelezen.

2. GAP-analyse en de impactanalyse

In dit hoofdstuk staan de randvoorwaarden en stappen beschreven om de GAP-analyse en de impactanalyse uit te voeren, tevens wordt een koppeling gemaakt met de gemeentebrede actoren die verantwoordelijk zijn voor een onderdeel van de bedrijfsvoering binnen de gemeente.

De insteek van de BIO is om op basis van een risicoafweging te gaan werken. Waar moet een gemeente beginnen? Het gaat om prioriteiten stellen: wat moet nu gedaan worden en wat kan (tot later) wachten. Hou hierbij rekening met de ontwikkelingen die op een gemeente afkomen. Betrek hierbij het management aangezien het management hierbij een belangrijke rol heeft.



Figuur 2 Stappen GAP-analyse en impactanalyse.

De stappen die gemeenten (moet kunnen) uitvoeren zijn:

1. **Bepaal kritieke processen** en **bepaal essentiële informatiesystemen** bij deze processen, stel de **scope** vast (informatiesystemen) en stel vast wie de **eigenaar** is.
2. **Prioriteer BIO-maatregelen** (focus aanbrengen), eerst op generieke beveiligingsmaatregelen, daarna de specifieke beveiligingsmaatregelen en **beleg de BIO-maatregelen** (SCOPAFIJTH[2]-actoren, proceseigenaren)
3. Bepaal de **status per beveiligingsmaatregel**
4. Bepaal de **impact per beveiligingsmaatregel**
5. Stel een **informatiebeveiligingsplan** op

Hierbij zijn de stappen 1 en 2 de randvoorwaarden om een GAP-analyse uit te kunnen voeren, stap 3 en 4 is de uitvoeren van de GAP-analyse en impactanalyse en stap 5 is het resultaat van de uitgevoerde GAP-analyse.

GAP-analyse

De GAP-analyse is het uitzoeken waar men staat ten opzichte van de BIO-maatregelen. Een soort 0-meting, wat heeft men aan beveiligingsmaatregelen al 'in huis' en wat is hiervan nog up to date. Hierbij is het van belang om alvast na te denken of beveiligingsmaatregelen gemeentebreed of informatiesysteem specifiek zijn. Deze stap geeft ook al inzicht in hoe het nu geregeld is, dus wie voert feitelijk welke informatiebeveiligingsmaatregelen uit. Probeer bij deze stap te timeboxen, ofwel niet te lang te zoeken. Kleine gemeenten kunnen deze stap het beste hoog over voor alle informatiesystemen in een keer uitvoeren.

[2] SCOPAFIJTH is een acroniem voor: Security, Communicatie, Organisatie, Personeel, Administratieve organisatie, Financiën, Informatievoorziening, Juridisch, Technologie en Huisvesting.

De impactanalyse

De impactanalyse is het tweede deel van de GAP-analyse spreadsheet. Hier wordt voor ontbrekende beveiligingsmaatregelen bepaald wie wanneer en hoe een ontbrekende of niet volledige beveiligingsmaatregel implementeert. Hier is het van belang dat de verantwoordelijken bekend zijn, maar ook inzicht in de vraag: 'Hoe willen we binnen de gemeente het onderwerp beveiliging aanpakken en wie doet wat?'. Denk bij deze stap ook na over kosten en wanneer het klaar moet zijn en hoe hierover verantwoording afgelegd moet worden. Bedenk ook dat kosten een nauwe relatie hebben met de budget/planning en control (P&C)-cyclus binnen de gemeente. Als men te laat in het jaar met kosten voor beveiligingsmaatregelen komt zou het wel eens twee kunnen duren voordat de beveiligingsmaatregel gerealiseerd is. Deze informatie kan in een informatiebeveiligingsplan (stap 5) opgenomen worden.

2.1. Stap 1: Bepaal kritieke processen en daarbij behorende essentiële informatiesystemen

Beperk bij deze stap de scope van de analyse tot de kern van wat aangepakt moet worden in de komende periode. Impliciet is dit een vorm van risicoafweging omdat de focus wordt gelegd op wat er nu toe doet. Zoek ook uit wie de eigenaar is.

Criteria voor het bepalen van kritieke processen zijn:

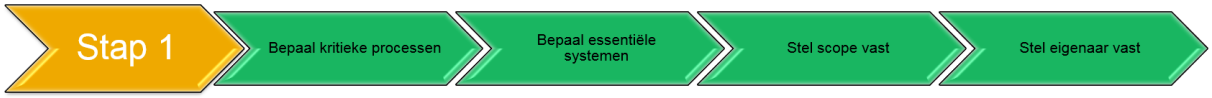
- Verstoring of uitval van het proces:
  - Heeft impact op het leven van de burger of de bedrijfsvoering van het bedrijf.
  - Zorgt voor vertraging bij het halen van onze ambities.
  - Verstoring of uitval van het proces stokt de dienstverlening van de organisatie.
  - Stokt de bedrijfsvoering van meer afdelingen of ketenpartners.
  - De eigen organisatie imagoschade op.
  - Brengt een aanzienlijke kostenpost met zich mee.
  - Levert schade op bij andere (samenwerkings-)partijen.
  - Heeft een wettelijke termijn waarbinnen het proces beschikbaar moet zijn.
- Snelle doorlooptijd van het proces is belangrijk voor burger of bedrijf.

De stelregel is dat als er meer dan 5 criteria kunnen worden aangevinkt er grote kans is dat dit een kritiek proces is. Als er erg veel kritieke processen en daarmee informatiesystemen zijn is het handig om op basis van een telling van de criteria een top 5 vast te stellen.[3]

- Resultaat: een lijst met processen en informatiesystemen en hun eigenaar waar de komende periode de prioriteit op ligt (scope), stem deze lijst af met het management, laat de lijst vaststellen.
- Als in deze lijst processen en onderliggende informatiesystemen staan die al een eigen beveiligingsbeleid en -documentatie hebben dan hoeft daar nu niks voor te gebeuren, die kunnen voorlopig worden geparkeerd. Bijvoorbeeld BRP, PUN, BAG, BGT, BRO, DigiD en GEVS Suwinet als daarvoor de laatste (ENSIA[4]) audit al goed was.[5]

[3] Zie voor een lijst met processen ook naar de handreiking dataclassificatie.
[4] ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit. De focus van ENSIA ligt op de horizontale verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid, over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).
[5] BRP: Basisregistratie Personen, PUN: Paspoortuitvoeringsregeling Nederland, BAG: Basisregistratie Adressen en Gebouwen, BGT: Basisregistratie Grootschalige Topografie, BRO: Basisregistratie Ondergrond, DigiD: Digitale Identiteit en GeVS Suwinet Gezamenlijke elektronische Voorzieningen (GeVS) SUWI (Structuur Uitvoering Werk en Inkomen).

Na afloop van deze stap is er inzicht in de kritieke processen, de essentiële informatiesystemen en de bijbehorende verantwoordelijken (zie figuur 3).



Figuur 3 Stap 1 GAP-analyse en impactanalyse.

2.2. Stap 2: Prioriteer en beleg beveiligingsmaatregelen

In de BIO staan 133 Controls met daaronder 137 beveiligingsmaatregelen[6], hier kan een focus per periode in worden aangebracht, dit omdat ook de implementatie van (ontbrekende) beveiligingsmaatregelen capaciteit en geld kan kosten en de hoeveelheid middelen per definitie beperkt is. Het is niet zo dat daarmee beveiligingsmaatregelen die niet geselecteerd zijn niet uitgevoerd hoeven te worden, deze blijven over om de periodes hierna mee te nemen in de planning. Leg dit vast in de GAP-analyse vragenlijst, hiervoor kan de kolom 'Scope' worden gebruikt (zie figuur 4). In deze kolom kan voor de betreffende beveiligingsmaatregelen een datum of jaartal worden ingevuld wanneer de beveiligingsmaatregel geïmplementeerd moet zijn en dus wanneer men deze beveiligingsmaatregel getoetst wil hebben.

Control / Maatregel	Vraag	Generiek/ Specifiek	SCOPAFIJTH	Scope	Aanwezig
Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.	Is er een door de organisatie vastgesteld en gepubliceerd informatiebeveiligingsbeleid op basis van de BIO en zijn daarin verantwoordelijkheden op basis van de baseline benoemd? Zijn de beschreven aspecten hierin opgenomen?	Generiek	IBF		Onbekend
Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	Is het informatiebeveiligingsbeleid in de afgelopen 3 jaar aangepast? Zo nee, was daar een goede reden voor?	Generiek	IBF		Onbekend

Figuur 4 Aanbrengen focus (scope) in beveiligingsmaatregelen.

Stel vast welke gemeentebrede beveiligingsmaatregelen geregeld moeten zijn. Bijvoorbeeld, het hebben van een informatiebeveiligingsbeleid, personele beveiligingsmaatregelen of een (fysieke) toegangsregeling. Gebruik de GAP-analyse met de vragenlijst en bepaal waar de focus op moet liggen voor de komende periode. Deze informatie kan in het informatiebeveiligingsplan (IB)-plan worden gebruikt. Deze gemeentebrede beveiligingsmaatregelen hebben vaak een SCOPAFIJTH-eigenaar/verantwoordelijke (zie bijlage A voor een uitgebreide beschrijving), leg dit vast in de GAP-analyse vragenlijst. Als er geen eigenaar bepaald kan worden dan moet dit alsnog gebeuren door het toewijzen van de beveiligingsmaatregel aan een andere functionaris.

Bepaal welke informatiesysteemspecifieke beveiligingsmaatregelen echt belangrijk zijn. Breng in beeld welke getoetst moeten worden bij essentiële informatiesystemen. Denk hier bijvoorbeeld aan gebruikers- en rechtenbeheer, afscherming van informatie, logging (alle vormen), beheerafspraken, back-up, uitwijk et cetera.

Impliciet is deze focus aanbrengen een vorm van risicoafweging. Hier biedt de BIO ook ruimte toe. Let wel op, er kunnen beveiligingsmaatregelen zijn die wettelijk verplicht zijn om te nemen. Leg dit vast in de GAP-analyse vragenlijst.

[6] Dit aantal is zonder de aanvullende beveiligingsmaatregelen onder de lege controls, die door de IBD zijn voorgesteld.

Na afloop van deze stap is er inzicht in de prioriteit (scope) van de beveiligingsmaatregelen en welke beveiligingsmaatregelen generiek (gemeentebreed) en welke specifiek (per proces/ informatiesysteem) zijn en aan wie de beveiligingsmaatregel is toegewezen/ de verantwoordelijke (zie figuur 5).

Figuur 5 Stap 2 GAP-analyse en impactanalyse.

2.3. Stap 3: Bepaal de status van maatregelen

Generieke beveiligingsmaatregelen

De term 'Baseline Informatiebeveiliging Overheid' suggereert één basisbeveiligingsniveau aan beveiligingsmaatregelen voor informatiebeveiliging voor de gehele overheid inclusief alle gemeenten. Dus beveiligingsmaatregelen die je altijd verwacht aan te treffen.

Het is mogelijk om 'hoog over' gemeentebreed te toetsen wat van de BIO is geïmplementeerd. Het advies is om hierbij uit te gaan van BBN 2[7]. Met name de generieke beveiligingsmaatregelen die gemeentebreed gelden worden zo bekeken. Bij deze generieke beveiligingsmaatregelen kan worden gedacht aan:

- Het gemeentelijk informatiebeveiligingsbeleid, dit is eenmalig voor de gehele gemeente.
- Het toewijzen van de Chief Information Security Officer (CISO)-rol.
- Verantwoordelijkheden van de lijnmanagers (te verankeren in het beleid).
- (ITIL) beheerprocessen en aandacht voor beveiliging.
- Personele beveiligingsmaatregelen.
- Fysieke toegangsbeveiligingsmaatregelen.
- Beveiligingsmaatregelen voor apparatuur en software.
- Malware scanning als generieke dienst (dus niet ten behoeve van één informatiesysteem).
- Omgang met (mobiele) gegevensdragers.
- Het hebben van een Information Security Management Systeem (ISMS).

Controleer de status van die vastgestelde gemeentebrede beveiligingsmaatregelen bij de betreffende eigenaren door middel van een kort interview. Of de vragenlijst als leidraad gebruikt wordt of dat er een (vrij) gesprek plaatsvindt is aan de persoon die het doet, voorwaarde is wel dat achteraf de GAP-analyse lijst moet worden bijgewerkt met de bevindingen. Blijf niet te lang hangen bij een onderwerp, als iets niet direct duidelijk is probeer er dan een tweede gesprek aan te weiden of vraag iets uit te zoeken en terug te koppelen (Bewaak dit wel).

Beveiligingsmaatregel	Generiek	Specifiek	GAP-analyse beveiligingsmaatregelen gemeentebreed	GAP-analyse beveiligingsmaatregelen specifiek per proces of systeem	GAP-analyse beveiligingsmaatregelen specifiek per proces of systeem
Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	X		Ja	Nee	Nee
De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	X	X	Ja	Ja	Ja
De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.		X	Nee	Ja	Ja

Figuur 6 Uitvoering GAP-analyse voor gemeentebrede en specifieke beveiligingsmaatregelen.

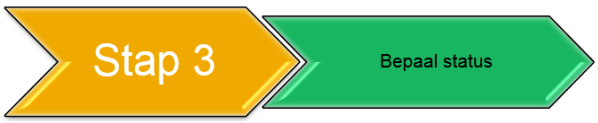
[7] Het niveau van de BIG is BBN2.

Als er goed is geïnventariseerd, wat de status is van deze gemeentebrede beveiligingsmaatregelen, hoeft dit niet voor alle informatiesystemen opnieuw onderzocht te worden. In figuur 6 zijn een aantal beveiligingsmaatregelen uit de GAP-analyse spreadsheet weergegeven en per beveiligingsmaatregelmaatregel is aangegeven of de beveiligingsmaatregel gemeentebreed (generiek) of specifiek per proces of informatiesysteem is. Daarnaast is per beveiligingsmaatregelmaatregel aangegeven of een beveiligingsmaatregel gemeentebreed/centraal onderzocht kan worden door de CISO en de eindverantwoordelijke van de dienstverlening. De aanvullende analyses worden door de lijnverantwoordelijke gedaan in aanvulling op de gemeentebrede analyses. Daarbij kan de lijnverantwoordelijke gebruik maken van wat er binnen de centrale GAP-analyse al naar voren gekomen is. Men kan bijvoorbeeld het template voor de GAP-analyse en impactanalyse van tevoren invullen zodat dit niet voor ieder informatiesysteem opnieuw onderzocht hoeft te worden.

Systeemspecifieke beveiligingsmaatregelen

Naast de generieke beveiligingsmaatregelen, die gemeentebreed gelden, zijn er ook specifieke beveiligingsmaatregelen die per proces (kunnen) verschillen. Het kan zelfs zijn dat deze beveiligingsmaatregelen binnen é én gemeente per informatiesysteem verschillen. Hiervoor kunnen de eerder vastgestelde proceseigenaren worden geïnterviewd. De GAP-analyse spreadsheet is daarbij een goede leidraad die ook op basis van dat interview achteraf kan worden bijgewerkt.

Na deze stap is er inzicht in de status van belangrijke gemeentebrede beveiligingsmaatregelen en systeemspecifieke beveiligingsmaatregelen waar voor de komende periode de focus op ligt. Er is na deze stap dus overzicht over de gemeentebrede beveiligingsmaatregelen die de CISO onderzocht heeft en overzichten per proces/ informatiesysteem die door de lijnmanager gecontroleerd zijn als aanvulling op de gemeentebrede lijst (zie figuur 7).



Figuur 7 Stap 3 GAP-analyse en impactanalyse

Met het inzicht over wat er wel en niet is kan alvast een eerste stap gezet worden met het invoeren van quick wins, meestal zijn dit beveiligingsmaatregelen die:

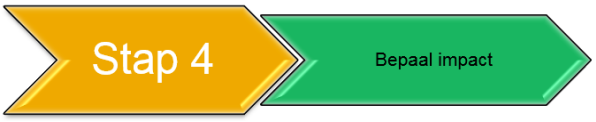
- gemeentebreed gelden;
- weinig kosten;
- betrekkelijk eenvoudig te implementeren zijn.

Bijvoorbeeld: het ophangen van posters over het onderwerp (verhogen van de bewustwording onder medewerkers), het opstellen en vaststellen van een gemeentelijk beveiligingsbeleid en aanvullend beveiligingsbeleid voor onderwerpen uit het gemeentelijk beveiligingsbeleid.

2.4. Stap 4: Bepaal de impact

Een belangrijke stap is nu om vast te stellen wie welke beveiligingsmaatregel gaat invoeren en wat deze beveiligingsmaatregel (geschat) kost. Dit wordt in dezelfde spreadsheet als de GAP-analyse bijgehouden (deel 2). Deze lijst moet bij het management getoetst worden omdat de eigenaar van een informatiesysteem die kosten moet dragen (de eigenaar kan ook besluiten iets niet te doen als risico afweging, maak dat expliciet en leg dat vast).

Na deze stap is er inzicht in de status van belangrijke gemeentebrede beveiligingsmaatregelen en systeemspecifieke beveiligingsmaatregelen waar voor de komende periode de focus op ligt (zie figuur 8).



Figuur 8 Stap 4 GAP-analyse en impactanalyse

De lijst met ontbrekende beveiligingsmaatregelen, actiehouders en geschatte kosten moet door het management worden goedgekeurd. Het management moet de afweging maken tussen kosten en risico en kan ook besluiten een beveiligingsmaatregel niet uit te voeren of deze later uit te voeren. Deze goedkeuring kan gemeentebreed gelden (als je de BIO hoog over gemeentebreed toepast) maar ook per proces/ informatiesysteem. In dat geval is de systeemeigenaar hiervoor verantwoordelijk. De systeemeigenaar gaat vaak niet over gemeentebrede beveiligingsmaatregelen. Let wel op, bewuste keuzes om bepaalde beveiligingsmaatregelen niet te implementeren dienen door de verantwoordelijk manager expliciet te worden gemaakt en te worden vermeld bij de betreffende beveiligingsmaatregel op de impactanalyse zodat dit later ook kan worden verantwoord.

2.5. Stap 5: Stel het informatiebeveiligingsplan op

Als het management de implementatie van de ontbrekende beveiligingsmaatregelen heeft goedgekeurd, dient de implementatie van de beveiligingsmaatregelen in een informatiebeveiligingsplan voor de komende periode te worden opgenomen. Dit informatiebeveiligingsplan is het projectplan voor de gemeente waarin ook de verantwoordelijkheden, actiehouders en de rapportage over de implementatie is vastgelegd. De ingevulde impactanalyse is de input voor het informatiebeveiligingsplan (zie figuur 9).

DEEL 2 (ImpactAnalyse)			
Status	Actiehouder	Wanneer gereed?	Geaccepteerd risico?
Nog niet onderzocht			
Nog niet onderzocht			
Nog niet onderzocht			
Nog niet onderzocht			
Nog niet onderzocht			

Figuur 9 Impact bepalen van de BIO-maatregelen.

In het informatiebeveiligingsplan zijn de verschillende activiteiten en soms deelprojecten om beveiligingsmaatregelen ingevoerd te krijgen, opgenomen. Dit moet leiden tot een geïmplementeerde BIO. Dit informatiebeveiligingsplan wordt periodiek, bij voorkeur jaarlijks gemaakt. Dit informatiebeveiligingsplan dient er ook voor om de benodigde budgetten te verkrijgen binnen de P&C-cyclus van de gemeente. De bewaking van het plan ligt bij de CISO. De rapportage over de voortgang van het plan wordt van alle actiehouders gebundeld en periodiek aan de gemeentesecretaris gezonden. Het informatiebeveiligingsplan heeft ook de functie om de aandachtspunten uit het gemeentelijk informatiebeveiligingsbeleid (het wat) te vertalen naar uitvoering (hoe, waarmee, door wie).

De input voor het informatiebeveiligingsplan komt uit het gemeentelijk beveiligingsbeleid en de impactanalyse. In de impactanalyse is al een globale volgorde bepaald die door het management bekrachtigd moet worden. Daarbij kan het voorkomen dat informatiebeveiligingsmaatregelen over langere tijd gepland worden om deze in te voeren. Dit kan verschillende redenen hebben, bijvoorbeeld:

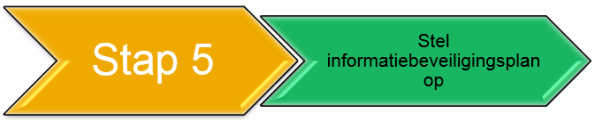
- De grootte van de organisatie, ofwel de slagkracht of de mogelijkheid om het werk door meerdere mensen te laten uitvoeren en ook te specialiseren. Grotere gemeenten zijn hier in het voordeel.
- Beschikbaar budget.
- Beschikbare menskracht.
- Veranderbereidheid van de organisatie.
- Risicobereidheid (is de organisatie risicomijdend, risiconeutraal of risicodragend).

In het informatiebeveiligingsplan moeten in ieder geval de quick wins staan die eerder zijn vastgesteld. Quick wins zijn belangrijk. Er is niks erger dan eerst management commitment te krijgen en vervolgens de eerste resultaten na een jaar pas op te leveren.

Betrek vroegtijdig de actiehouders of voortrekkers bij het opstellen van het informatiebeveiligingsplan. Zo wordt het draagvlak voor de in te voeren beveiligingsmaatregelen en afspraken beter ondersteund op de diverse onderdelen van de gemeente. Door betrokkenheid neemt de veranderbereidheid toe en lijkt het niet alsof er iets opgelegd wordt.
Wat moet er minimaal in een informatiebeveiligingsplan staan:

- Het doel van het plan.
- De eigenaar van het plan.
- De reikwijdte van het plan (gemeente, proces of informatiesysteem), dus ook de verantwoording en het resultaat van de gekozen aanpak om de BIO te implementeren.
- Het resultaat van de impactanalyse BIO dan wel het resultaat van een risicoanalyse, en dan alleen de ontbrekende beveiligingsmaatregelen noemen, met het BIO-nummer.
- - De vertaling van uitspraken van het informatiebeveiligingsbeleid naar het hoe, waarmee en door wie.
- De beveiligingsmaatregelen en de prioriteit van invoeren (hoog, midden, laag) met BIO-nummer.
- De beveiligingsmaatregel planning met: BIO-nummer, -maatregel, -doorlooptijd, -capaciteitsbeslag, eventuele kosten en wie er verantwoordelijk is.
- Welke beveiligingsmaatregelen worden doorgeschoven naar een volgende periode erop op basis van een risico inschatting of de prioriteitsstelling.
- Startdatum.
- Rapportage en verantwoording.

Na deze stap is informatiebeveiligingsplan opgesteld of bijgewerkt (zie figuur 10).



Figuur 10 Stap 6 GAP-analyse en impactanalyse

3. Opbouw van de spreadsheet GAP-analyse

De spreadsheet geeft de GAP-analyse weer, die bestaat uit 3 tabbladen, te weten:

1. **Vragenlijst**: de inhoud van de BIO met vragen.
2. **Resultaat**: een sheet met grafieken als resultaat van de vragenlijst.
3. **Aantekeningen**: ruimte voor eigen aantekeningen

3.1. Gebruiksaanwijzing spreadsheet GAP-analyse

De persoon die gaat onderzoeken of en in welke mate aan de BIO wordt voldaan, gaat met de spreadsheet binnen de eigen organisatie vaststellen of een beveiligingsmaatregel bestaat of niet. Hiervoor worden de kolommen gebruikt onder het kopje deel 1 (GAP-analyse) van het tabblad vragenlijst.
De GAP-analyse tegen de BIO aanhouden is een brede onderzoeksvraag en gaat binnen de gemeente over alle processen en applicaties heen.

Bijvoorbeeld beveiligingsmaatregel 5.1.1.1.:
Als er een informatiebeveiligingsplan gevonden wordt binnen de BRP informatiebeveiliging documentatieset of in de set die gemaakt is voor DigiD, dan is daarmee deels voldaan aan de vraag of er een informatiebeveiligingsplan is. Pas als in het plan de scope is opgenomen “alle bedrijfsvoeringsprocessen van de gemeente” en de BIO, dan pas kan van een informatiebeveiligingsplan gesproken worden in de zin van de BIO.

3.2. De vragenlijst

Opbouw GAP-analyse kolommen (tabblad vragenlijst):

- **BIO-nummer** – Het nummer van het BIO-hoofdstuk/paragraaf;
- **Controls en/ of Beveiligingsmaatregelen** – Is het een control of beveiligingsmaatregel;
- **Hoofdgroep** – Hoofdstuk aanduiding, kan gebruikt worden voor selecteren;[8]
- **Control/ Beveiligingsmaatregel** – De control of beveiligingsmaatregeltekst;[9]
- **Vraag** – De beveiligingsmaatregelvraag.
- **BIG-nummer** - Het corresponderen nummer uit de BIG-hoofdstuk/paragraaf;
- **BBN (1, 2 en/of 3) -** De aanduiding van het basisbeveiligingsniveau (BBN).
- **Aspect (B, I, V of G**) – De aanduiding waarop de control of beveiligingsmaatregel op van toepassing is.[10]
- **Verantwoordelijke (Gemeentesecretaris, Proceseigenaar of Dienstenleverancier)** – De rol die verantwoordelijk is voor de uitvoering van de control/beveiligingsmaatregel.
- **Generiek/ Specifiek** - Is een beveiligingsmaatregel generiek (gemeentebreed) of specifiek (proces/ informatiesysteem).
- **SCOPAFIJTH** – De functie/rol die betrokken is bij de implementatie van de beveiligingsmaatregel.
- **Scope** - Wanneer deze beveiligingsmaatregel getoetst dient te zijn.

Onderdeel van de vragenlijst zijn de GAP-analyse en de Impactanalyse. De GAP-analyse is deel 1 en hier wordt vastgesteld of de betreffende beveiligingsmaatregel aanwezig is binnen de gemeente. Deel 2 bestaat uit de Impactanalyse en in dit deel wordt vastgesteld wat de status is van de beveiligingsmaatregelen en wie hiervoor verantwoordelijk is.

[8] Deze kolom is initieel verborgen.
[9] De controltekst is standaard verborgen.
[10] B= Beschikbaarheid, I = Integriteit, V= Vertrouwelijkheid en G = Generiek. Generiek betekent hier dat een beveiligingsmaatregel niet specifiek de beschikbaarheid, integriteit en/of vertrouwelijkheid beschermd. De organisatorische inrichting van informatiebeveiliging is een voorbeeld van een generieke beveiligingsmaatregel. Beveiligingsmaatregelen, zoals een noodstroomvoorziening of een brandmeldinstallatie, richten zich op één specifieke bedreiging.

Deel 1 - GAP-analyse

- **Aanwezig** – Is de beveiligingsmaatregel aanwezig binnen de gemeente. Deze kolom bevat keuzes: gedeeltelijk, Ja, Nee, Niet van toepassing en Onbekend;
- **Vindplaats/ Opmerking**;
  1. Vindplaats - waar is de beschrijving, beveiligingsmaatregel gevonden;
  2. Opmerking – [eigen tekst];
- **Eigenaar** – Naam van eigenaar.

Deel 2 - Impactanalyse

- **Status** – wat is de status van de beveiligingsmaatregel;
- **Actiehouder** – wie is aanspreekbaar voor de beveiligingsmaatregel, verantwoordelijk voor implementatie;
- **Wanneer gereed** – planning;
- **Geaccepteerd risico** – management besluit.

4. Invullen spreadsheet GAP-analyse

In dit hoofdstuk wordt een korte invulinstructie geven voor zowel deel 1 (GAP-analyse) en deel 2 (Impactanalyse)

4.1. Deel 1 (GAP-analyse)

Het uitvoeren van de GAP-analyse hoeft niet lang te duren, het gaat om een Quick scan. De keuzes die gemaakt kunnen worden in de kolom 'Aanwezig' (zie figuur 11[11]):

- **Ja**: De beveiligingsmaatregel is aanwezig. Vul ook de vindplaats in, wie de beveiligingsmaatregel uitvoert, waar de beveiligingsmaatregel is vastgelegd en overige bijzonderheden.
- **Nee**: Er is niks gevonden.
- **Gedeeltelijk**: De beveiligingsmaatregel is gedeeltelijk geïmplementeerd.
- **Niet van toepassing**: De beveiligingsmaatregel is niet van toepassing. Vul daarbij in kolom 'Vindplaats / opmerking' ook een reden in!
- **Onbekend**: Onduidelijk of er iets is dat voldoet. Er moet te lang naar gezocht worden of er liggen nog een aantal onopgeloste vraagstukken.

	DEEL 1 (GAP-Analyse)		
Vraag	Aanwezig	Vindplaats / opmerking	Eigenaar
Is het informatiebeveiligingsbeleid in de afgelopen 3 jaar aangepast? Zo nee, was daar een goede reden voor?	Onbekend		
Heeft de leiding van de organisatie vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging? Zo ja welke zijn dit? Is in functiebeschrijvingen aandacht voor informatiebeveiliging?	Ja		
Zijn de verantwoordelijkheden en rollen (bijvoorbeeld CISO en lijnmanagement) ten aanzien van informatiebeveiliging gebaseerd op relevante voorschriften en wetten? Zo ja, welke zijn dit?	Gedeeltelijk Ja Nee Niet van toepassing Onbekend		
Is de rol en verantwoordelijkheden van de CISO in een CISO-functieprofiel vastgelegd?			
Is er een CISO aangesteld conform een vastgesteld CISO-functieprofiel?	Onbekend		
Zijn er maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen?	Onbekend		

Figuur 11 Schermvoorbeeld deel 1 (GAP-analyse) met keuzemogelijkheden.

Als de vragenlijst is afgewerkt, weet de gemeente waar men staat ten opzichte van de BIO. Dit kunt u bekijken door in het tabblad 'resultaat' naar de bovenste figuur 'Status GAP-analyse gemeente' te kijken. Binnen dit tabblad kan men cel B8 tot en met B22 selecteren en door middel van de toetsaanslag ALT-F5 een verversing van de resultaten bewerkstelligen. Het figuur geeft een procentuele score aan ten opzichte van het optimale resultaat.

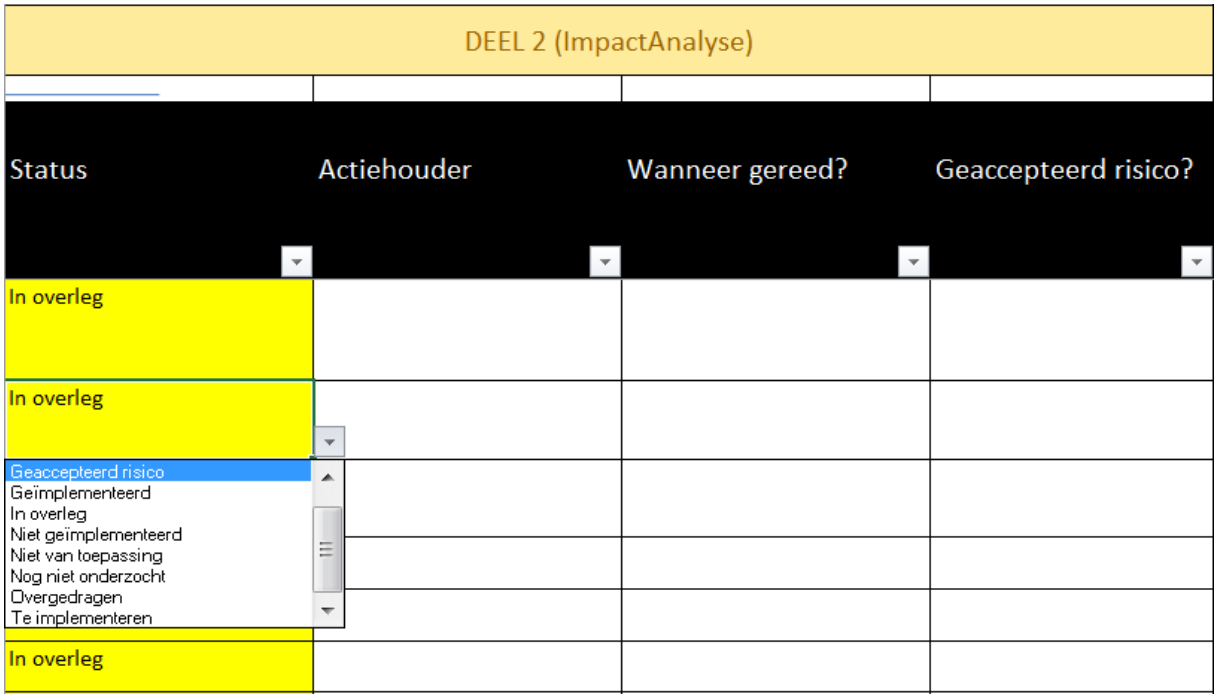
Na het invullen van deel 1 is de GAP-analyse uitgevoerd.

4.2. Deel 2 (Impactanalyse)

In de kolommen van deel 2 van het tabblad Vragenlijst kan men de ontbrekende of onbekende beveiligingsmaatregelen verder onderzoeken en een managementrapportage maken. Deel 2 van de lijst wordt gebruikt bij de Impactanalyse. De Impactanalyse is een stap in de toewijzing van beveiligingsmaatregelen en het gaat erom dat er een reële planning gemaakt wordt. Hier worden de nog niet gevonden beveiligingsmaatregelen of de onbekende beveiligingsmaatregelen verder verdeeld in de volgende statussen (zie figuur 12[12]):

[11] Deze keuzes kunnen klein uitvallen als de sheet ver wordt uitgezoomd.
[12] Deze keuzes kunnen klein uitvallen als de sheet ver wordt uitgezoomd.

- **Deels geïmplementeerd**: Een beveiligingsmaatregel is deels aanwezig.
- **Geaccepteerd risico**: Een beveiligingsmaatregel wordt niet genomen, het risico dat gelopen wordt door het niet nemen wordt geaccepteerd.
- **Geïmplementeerd**: Een beveiligingsmaatregel is volledig geïmplementeerd.
- **In overleg**: Een beveiligingsmaatregel is nog in overleg.
- **Niet geïmplementeerd**: De beveiligingsmaatregel moet nog geïmplementeerd worden.
- **Niet van toepassing**: De beveiligingsmaatregel is niet van toepassing.
- **Nog niet onderzocht**: De beveiligingsmaatregel is nog niet onderzocht.
- **Overgedragen**: De beveiligingsmaatregel is overgedragen (bijvoorbeeld aan een technische beheer organisatie).
- **Te implementeren**: De beveiligingsmaatregel gaat geïmplementeerd worden binnen afzienbare tijd.



Figuur 12 Schermvoorbeeld deel 2 (Impactanalyse) met keuzemogelijkheden.

De kolommen Actiehouder'' en 'Wanneer Gereed' kunnen worden voorzien van concrete informatie over wanneer en door wie een beveiligingsmaatregel geïmplementeerd is.
Het management en beschikbare resources zoals mensen en budget bepalen in sterke mate de snelheid waarmee ontbrekende beveiligingsmaatregelen geïmplementeerd kunnen worden.

Als deel 2 ingevuld is, kan men in het tabblad 'Resultaat' bij het onderste figuur 'Status na update en management besluiten' zien welke keuzes gemaakt zijn. Binnen dit tabblad kan men cel B43 tot en met B57 selecteren en door middel van de toetsaanslag ALT-F5 een verversing van de resultaten bewerkstelligen. Het figuur geeft een procentuele score aan ten opzichte van het optimale resultaat.

5. Voortgang en rapportage

Door het rekenblad, bijvoorbeeld iedere maand met een andere naam op te slaan, kan men de voortgang eenvoudig zichtbaar maken. Als er wijzigingen zijn in statussen kunnen deze in de loop van de implementatie van de beveiligingsmaatregelen verwerkt worden. De verschillende rekenbladen kunnen samen gebruikt worden voor rapportages aan het management. Het gaat bij het rekenblad om het totale overzicht van alle processen en ondersteunende informatiesystemen binnen de gemeente waarover de toets gedaan is.

Bovenstaand beschreven proces is omslachtig en het advies is dan ook om gebruik te maken van ISMS-tooling. In paragraaf 5.1 worden de mogelijkheden en voordelen van zo'n tool beschreven.

5.1. ISMS-tooling

Gemeenten die met de BIO aan de slag gaan merken al gauw dat enkele processen en informatiesystemen en bijhouden met de GAP-analyse spreadsheet nog wel gaat. Het is dan het toevoegen van kolommen en/of bijhouden van een GAP-analyse per proces/ informatiesysteem. Echter als men voor heel veel gemeentelijke processen en informatiesystemen de GAP-analyse wil bijhouden wordt het mogelijk een behoorlijke administratieve kluif.
Daarnaast wil men binnen de gemeente de voortgang van de invoering en de status van de beveiligingsmaatregelen makkelijk kunnen bijhouden. Idealiter worden deze bijgehouden door de persoon die de beveiligingsmaatregel toepast of implementeert. Als meerdere personen dit op één plaats bijhouden is met één druk op de knop het overzicht te maken waar de gemeente staat ten opzichte van de BIO als geheel.

Voor dit probleem bestaat er 'tooling' die gemeenten helpt om een eigen normenkader bij te houden of een organisatie brede baseline te onderhouden. Mits goed ingericht, bijgehouden en gebruikt kan met één druk op de knop het overzicht verkregen worden van de status per actiehouder, informatiesysteem, proces, beveiligingsmaatregel, afdeling of voor de hele organisatie. De tooling die hiervoor wordt gebruikt heet GRC-tooling. GRC staat voor Governance, Risk and Compliance:

- Governance: beleid, procedures en beveiligingsmaatregelen om een organisatie, in dit geval de gemeente, te kunnen laten functioneren in overeenstemming met haar doelstellingen.
- Riskmanagement: procedures en beveiligingsmaatregelen gericht op het identificeren van risico's, het nemen van mitigerende beveiligingsmaatregelen en het rapporteren aan management over het functioneren van riskmanagement. Vanuit de BIO gaat het hier om de zelfevaluatie (ENSIA), de Baselinetoets BIO en, de diepgaande risicoanalyse en de data protection impact assessment (DPIA).
- Compliance: hiermee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving. Het gaat over het nakomen van normen of het zich er naar schikken. Dit is voor de BIO een belangrijk onderwerp omdat hier de verantwoording over BIO-maatregelen maar ook verantwoording over andere beveiligingsmaatregelen mee wordt bedoeld. Denk hier dan ook aan verantwoording over wetgeving zoals de Algemene Verordening Gegevensbescherming (AVG) en bijvoorbeeld Basis Registratie Personen (BRP).

De voordelen van een tool zijn:

- Als er voor meerdere processen en informatiesystemen een Baselinetoets BIO wordt uitgevoerd, neemt de hoeveelheid kolommen in de GAP-analyse toe of er worden verschillende spreadsheets bijgehouden. Dat kan veel werk kosten. De hoeveelheid regels, actiehouders, processen en informatiesystemen zijn niet meer beperkt door het gebruik van MS Excel.
- Deelname van veel verschillende personen voor het bijhouden van de status van BIO-maatregelen kan door de personen zelf worden gedaan en vereist niet het heen en weer zenden van MS Excelsheets.
- Met één druk op de knop wordt de status van de beveiligingsmaatregelen weergegeven. Dit vereenvoudigt de rapportage mogelijkheden, ook gemeentebreed. Horizontale en verticale verantwoording worden ondersteund.

Bijlage A: SCOPAFIJTH-actoren en beveiligingsmaatregelen

In de informatiebeveiliging wordt de acroniem SCOPAFIJTH gebruikt om te duiden dat bepaalde beveiligingsmaatregelen thuishoren bij een gemeentebrede actor die verantwoordelijk is voor een onderdeel van de bedrijfsvoering binnen de gemeente. SCOPAFIJTH staat voor:

- **S**ecurity
- **C**ommunicatie
- **O**rganisatie
- **P**ersoneel
- **A**utomatisering/ Administratieve organisatie
- **F**inanciën
- **I**nkoop (soms informatievoorziening)
- **J**uridisch
- **T**echnologie
- **H**uisvesting

Soms wordt de 'I' ook gebruikt voor informatievoorziening. Het kan per gemeente verschillen hoe verantwoordelijkheden binnen de bedrijfsvoering verdeeld zijn per actor. Bij een kleine gemeente kunnen meerdere verantwoordelijkheden belegd zijn bij één persoon.

Waarom is SCOPAFIJTH belangrijk binnen de informatiebeveiliging?
De verschillende ondersteunende processen die binnen de gemeente worden uitgevoerd hebben verantwoordelijkheid voor bepaalde beveiligingstaken, bijvoorbeeld:

Security
Strikt genomen kan Security ondergebracht worden in andere aspectgebieden. Maar het belang van beveiliging is intussen zo groot geworden, dat het tegenwoordig vaak als apart aandachtspunt wordt gepositioneerd. Belangrijke trends op dit gebied zijn onder andere:

- 'Iedereen' moet anytime, anywhere kunnen werken.
- Toenemende digitale communicatie tussen de gemeente en (keten)partners.
- Cloud computing.
- Business Intelligence en big data.

Communicatie
Het gaat hierbij niet alleen om interne communicatie, maar ook om de externe communicatie met burgers en (keten)partners, leveranciers, toezichthouders en andere stakeholders. Bekijk daarom de impact voor ieder communicatiekanaal, dat wordt gebruikt. De communicatiefunctie, heeft ook raakvlakken met vrijgave van informatie (publiek) en de (externe) berichtgeving met betrekking tot beveiligingsincidenten en datalekken.

Organisatie

- Maatregelen die samenhangen met de organisatie zoals functies, functiescheiding, competenties.
- Maatregelen die samenhangen met administratieve systemen, 'harde' procedures, randvoorwaarden/ beperkingen, controle.
- Beveiligingsbeleid
- Bewustwording

Personeel

Alle personele beveiligingsmaatregelen, zoals:

- Procedures met betrekking tot indiensttreding.
- Arbeidsvoorwaarden
- Procedures met betrekking tot functiewisseling.
- Procedures met betrekking tot uitdiensttreding/ ontslag.
- Beheer van (beveiligings)functieprofielen.
- Beoordelingssystematiek waarbij ook aandacht is voor beveiligingsverantwoordelijkheid als onderwerp, het bijhouden wie een bewustwordingscursus gehad heeft.

Automatisering

Bijna alle technische informatiebeveiligingsmaatregelen worden uitgevoerd door de afdeling ICT. De technische informatiebeveiligingsmaatregelen uit de BIO zijn bijvoorbeeld:

- Back-up en restore
- Gebruikersbeheer gemeentebreed
- Inventariseren en beheren bedrijfsmiddelen (hoewel dit ook bij afdelingen zelf kan liggen)
- Beveiliging van apparatuur
- Bedienprocedures
- Systeemplanning en -acceptatie
- Beheer van netwerkbeveiliging
- Systeem logging en monitoring
- Toegangsbeheersing voor externe netwerken
- Draagbare computers en telewerken
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- ICT- en bedrijfscontinuïteitsmaatregelen

Het kan voorkomen dat bepaalde activiteiten van ICT door de afdelingen zelf worden uitgevoerd, dat hangt af van de keuze van de organisatie. Ook kan het voorkomen dat delen van de ICT-infrastructuur niet door de gemeentelijke ICT-afdeling geleverd en beheerd worden. In dat geval moeten bepaalde beveiligingsmaatregelen door derden worden uitgevoerd, denk bijvoorbeeld aan vormen van cloudcomputing bij een derde partij.

Voor wat betreft gebruikersbeheer kunnen er verschillende actoren zijn binnen de gemeente, bijvoorbeeld:

- ICT voert het gemeentebrede gebruikersbeheer uit.
- Functioneel beheer voert het gebruikers en toegangs- en rechtenbeheer binnen informatiesystemen uit, functioneel beheerders kunnen werkzaam zijn binnen de ICT-afdeling, maar ook specifiek werken voor een afdeling en niet onder ICT vallen.

Bij veel organisaties is ICT verantwoordelijk voor informatiebeveiliging in alle facetten. Dit is feitelijk onjuist. Goede beveiligingsmaatregelen zijn van procedurele, technische en organisatorische aard. De verantwoordelijkheid voor informatiebeveiliging van een informatiesysteem ligt bij de informatiesysteem- of proceseigenaar en niet bij ICT. ICT voert de technische beveiligingsmaatregelen uit die de eigenaar van een informatiesysteem noodzakelijk acht en legt daarover verantwoording af. De eigenaar van een informatiesysteem is verantwoordelijk voor de levering van een product of dienst binnen bepaalde (beveiligings)kaders, ICT is dan de uitvoerder voor de eigenaar.

Financiën

- Maatregelen die samenhangen met de financiële functie/ verantwoording.

Inkoop (ook contractbewaking)
De IBD heeft een handreiking geschreven over inkoop, beveiliging maar ook over contractbeheer: Beveiligingseisen en -contracten, de verwerkersovereenkomst, service-level agreement (SLA) et cetera.[13]

- Onderhandelen met leveranciers over inkoop- en verkoopvoorwaarden en de toegevoegde waarde en beveiligingseisen gerelateerd aan de product of dienst.
- Maatregelen die samenhangen met inkoopvoorwaarden en beveiligingseisen, (raam-) contracten, rechtspositie, verwerkersovereenkomsten.

Informatievoorziening
Dit is niet ICT, maar de vraagkant van informatievoorziening, dus de interne klant. Het hangt er vanaf waar dit belegd is. Bij sommige gemeenten is dit een ICT-taak, echter de vraagkant kan ook belegd zijn bij een aparte informatiemanagement of Informatievoorziening & Automatisering (I&A)-afdeling die daar los van staat. Vraag en aanbod zou niet onder één afdeling moeten vallen om belangenverstrengeling te voorkomen. De informatievoorzieningskant staat voor vertaling van business vraagstukken naar informatieoplossingen en dient daarbij rekening te houden met beveiligingseisen. Denk hier aan beveiligingsmaatregelen betreffende informatiesysteemeisen ten aanzien van ontwikkeling, beheer en informatiehuishouding binnen de gemeente over relevante systemen & documentenstromen en de website.

Juridisch
Uiteraard moet de organisatie voldoen aan de geldende wet- en regelgeving. De volgende punten dienen aan de orde te komen:

- Maatregelen die samenhangen met inkoopvoorwaarden en beveiligingseisen, (raam-) contracten, rechtspositie en verwerkersovereenkomsten.
- De impact vaststellen van de materie of domeinspecifieke wetgeving op de beveiliging en privacy.

Technologie
Het aspect technologie kan alle infrastructurele zaken omvatten, maar ook kan het zich toespitsen op puur de technologie, beveiligingsmaatregelen ten aanzien van automatisering, internet(web), systemen en contractpartijen. Hierbij kan gedacht worden aan onder andere:

- werkplek automatisering;
- vaste en mobiele telefonie;
- netwerk- en telecommunicatiecomponenten;
- beveiligingsapparatuur;
- stroom en no-break installaties;
- aanpassing van het continuïteitsplan;
- aangepaste logistieke infrastructuur;
- et cetra.

Huisvesting
Maatregelen betreffende fysieke beveiliging, brandbeveiliging, infrastructuur, werkplekken en faciliteiten.

[13] Zie: https://www.informatiebeveiligingsdienst.nl/product/inkoopvoorwaarden-en-informatiebeveiligingseisen/

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie