INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

BIO voor kleine gemeenten

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

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking BIO voor kleine gemeenten

Versienummer

1.0

Versiedatum

Juli 2019

Versiebeheer

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

INFORMATIE
BEVEILIGINGS
DIENST

Met dank aan

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

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	Juli 2019	Eerste versie van het document

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 dit document is een praktische aanpak te schetsen voor implementatie van de BIO in kleine gemeenten.

Doelgroep

Dit document is van belang voor informatiebeveiligers van de gemeente, de CISO, het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO) v1.03
- Introductie aanpak BIO
- Handreiking informatiebeveiligingsbeleid BIO gemeenten met apart format informatiebeveiligingsbeleid
- Baselinetoets BIO inclusief uitleg
- GAP-analyse BIO met aparte uitleg
- Diepgaande risicoanalyse met aparte uitleg
- NEN/ISO 270001/2

Inhoudsopgave

1. Inleiding

In 2013 is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) aangenomen. De BIG wordt in 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO), waarbij 2019 het overgangsjaar is. Vanaf 2020 is de Informatiebeveiligingstoets van ENSIA gebaseerd op de BIO.

Gemeenten hebben inmiddels ervaring opgedaan met de BIG en gaan nu over naar een meer risicogestuurde aanpak. Hoe te beginnen met de BIO is voor veel gemeenten een uitdaging. Want de BIO geldt voor alle gemeentelijke processen en de verantwoordelijkheid voor informatieveiligheid ligt nu expliciet(er) bij de proceseigenaar. De handreiking "Introductie aanpak BIO" van de IBD geeft een beknopte basis voor de aanpak.

De BIG en de BIO verschillen in werkelijkheid niet veel van elkaar, want de BIO is net als de BIG gebaseerd op ISO 27002. Het grootste verschil tussen de BIO en de BIG zit in de hoeveelheid maatregelen. Maatregelen die in het kader van de BIG getroffen zijn, zullen in het algemeen ook passend zijn in het kader van de BIO. Daarnaast legt de BIO meer nadruk op risicomanagement dan de BIG. Informatiebeveiliging is een verantwoordelijkheid van de proceseigenaar. De proceseigenaar bepaalt welke kwetsbaarheden zich kunnen voordoen binnen het proces dat onder zijn/haar verantwoordelijkheid wordt uitgevoerd en hoe groot het risico is als een kwetsbaarheid zich manifesteert. Op basis van risicoanalyse wordt vervolgens bepaald welke beveiligingsmaatregelen getroffen dienen te worden om uiteindelijk op een door de proceseigenaar geaccepteerd risico uit te komen.

De Baseline Informatiebeveiliging Overheid (BIO) helpt proceseigenaren bij het nemen van hun verantwoordelijkheid ten aanzien van informatiebeveiliging. Op welke wijze dit gebeurt, wordt toegelicht in hoofdstuk 2.

1.1. Belangrijke begrippen

Basisbeveiligingsniveaus

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een uitwerking van het risicomanagement op basis van drie basisbeveiligingsniveaus (BBN).

- BBN1: op dit niveau ligt de nadruk op ‘wat mag minimaal verwacht worden?’.
- BBN2: op dit niveau ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe ‘valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?’.
- BBN3: dit (uitzonderlijke) niveau is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement.

Controls

In de BIG werd gesproken over beheersmaatregelen. In de BIO is de term beheersmaatregel vervangen door de term *control*. Controls zijn in principe techniek- en organisatie- onafhankelijk geschreven. Controls hebben een relatie met één of meer risico’s en hebben tot doel bij te dragen aan de betrouwbaarheidseisen zoals die door de organisatie zijn gesteld.

Maatregelen

Maatregelen maken de controls concreet. Een maatregel kan gevonden worden in de BIO als verplichte overheidsmaatregel, in de oude BIG, de ISOR, de ISO 27002:2017 en verder uitgewerkt in operationele kennisproducten van de IBD. Ze kunnen ook bepaald worden op basis van een risicoanalyse. Dat is de reden waarom voor alle BIO gebruikers de toegang tot NEN-connect afgekocht is zodat iedereen die met de BIO bezig gaat ook van de ISO 27001:2017 en ISO 27002:2017 gebruik kan maken voor het bedenken van passende maatregelen als een control geen maatregelen bevat.

Implementatierichtlijnen

Iedere control is in de ISO 27002 uitgewerkt in implementatierichtlijnen. Bij het uitvoeren van risicoafwegingen zijn de implementatierichtlijnen zeer nuttig. Ze helpen bij het kiezen van de benodigde beveiligingsmaatregelen. Deze richtlijnen moeten dus worden gezien als voorbeelden hoe de controls uitgewerkt *kunnen* worden in maatregelen; het volgen van deze richtlijnen is niet verplicht. Deze implementatierichtlijnen zijn niet in de BIO opgenomen, hiervoor wordt verwezen naar de ISO 27002.[1]

Overheidsmaatregelen

Een deel van de controls is uitgewerkt in verplichte maatregelen, omdat zij:

- voortvloeien uit *wet- en regelgeving*. Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;
- zo basaal zijn dat zij het *fundament* vormen van een betrouwbare c.q. professionele informatievoorziening;
- dienstbaar zijn aan de beveiliging in een procesketen of netwerk; niet-naleving door een enkele organisatie is per saldo niet *effectief* voor de gehele keten.

De BIO noemt deze verplichte maatregelen ‘overheidsmaatregelen’. In het geval een maatregel voor een specifiek geval niet van toepassing *kan* zijn, vervalt de verplichting. Dit geldt bijvoorbeeld voor een overheidsmaatregel die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft.

Addendum

De BIO is generiek geschreven en geldig voor alle doelgroepen. Sommige overheidslagen hebben specifieke wet- en regelgeving die alleen gelden binnen die overheidslaag.
Om tegemoet te komen aan de behoefte van deze overheidslagen en deze specifieke wet- en regelgeving niet verloren te laten gaan is er aan de BIO een addendum toegevoegd. In dit addendum is deze wet- en regelgeving gekoppeld aan de control of maatregel waartoe zij behoren. Het addendum is toegevoegd aan de BIO in deel 3.

Operationalisering in handreikingen

Om de praktische toepasbaarheid van de BIO te verhogen, wordt de BIO aangevuld met handreikingen. Dit zijn aanbevelingen in het kader van de bedrijfsvoering die niet een verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel. Voor gemeenten zijn deze handreikingen terug te vinden op de website van de Informatiebeveiligingsdienst.[2]

1 https://www.informatiebeveiligingsdienst.nl/nen-iso-27001-2/

2 https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

2. Wie doet wat?

2.1. Verantwoordelijkheden binnen de BIO

Binnen het informatiebeveiligingsproces zijn verschillende actoren actief. In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie (hoofd)rollen: de Secretaris/algemeen directeur, de proceseigenaar en de dienstenleverancier. Deze rollen zijn hieronder beschreven vanuit het perspectief van informatiebeveiliging. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om wie uiteindelijk verantwoordelijk is voor de beveiliging van informatiesystemen.

Secretaris/algemeen directeur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de Secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging. In de praktijk kan deze rol worden uitgevoerd door bijvoorbeeld de CIO of een directeur Inkoop.
Proceseigenaar	Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
Dienstenleverancier	Bedoeld wordt de dienstenleverancier (bijv. SSO) binnen de overheid of organisaties in de markt waaraan de Secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

De BIO gaat ervan uit dat de verantwoordelijkheid voor informatie bij de proceseigenaar ligt. Met proces bedoelen we eigenlijk: bedrijfsproces en de definitie daarvan is: “Een ordening van activiteiten om een product of dienst te leveren die toegevoegde waarde biedt aan de klant. Een keten van activiteiten, gekoppeld en gestuurd door beslissingen.”[3] De proceseigenaar bevindt zich ergens in de uitvoeringsorganisatie. Maar op welk niveau is op voorhand niet te zeggen, dat hangt af van lokale afspraken en van het besturingsmodel waarop de gemeente ingericht is. Als geen proceseigenaar gevonden kan worden voor een bepaald proces, of de proceseigenaar het eigenaarschap niet accepteert, dan is de GS de eindverantwoordelijke voor de juiste beveiliging van dat proces.

In de BIO staat aangegeven welke controls voor welke rol toepasselijk zijn. De BIO verplicht om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding. In het algemeen is de organisatie van de informatiebeveiliging (ook wel de governance genoemd, wie doet wat) terug te vinden in het informatiebeveiligingsbeleid van de gemeente.

2.2. PIOFAH-actoren en maatregelen

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

- **P**ersoneel
- **I**nkoop (soms informatievoorziening)
- **O**rganisatie
- **F**inanciën

[3] https://nl.wikipedia.org/wiki/Bedrijfsproces

- **A**utomatisering/Administratie
- **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 PIOFAH belangrijk binnen de informatiebeveiliging?
De verschillende ondersteunende processen die binnen de gemeente worden uitgevoerd hebben verantwoordelijkheid voor bepaalde beveiligingstaken, bijvoorbeeld:

Personeel
Alle personele maatregelen, zoals:

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

Inkoop (ook contractbewaking)
De IBD heeft een handreiking geschreven over inkoop, beveiliging maar ook over contractbeheer, beveiligingseisen en -contracten, de verwerkersovereenkomst, SLA et cetera.

- 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 I&A-afdeling die daarvan losstaat. Vraag en aanbod zou niet onder één afdeling moeten vallen om belangenverstrengeling te voorkomen. De informatievoorzieningskant staat voor vertaling van business vraagstukken naar informatie oplossingen en dient daarbij rekening te houden met beveiligingseisen. Denk hier aan maatregelen betreffende systeemeisen ten aanzien van ontwikkeling, beheer en informatiehuishouding binnen de gemeente over relevante systemen & documentenstromen en de website.

Organisatie

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

Financiën

- Maatregelen die samenhangen met de financiële functie/verantwoording.

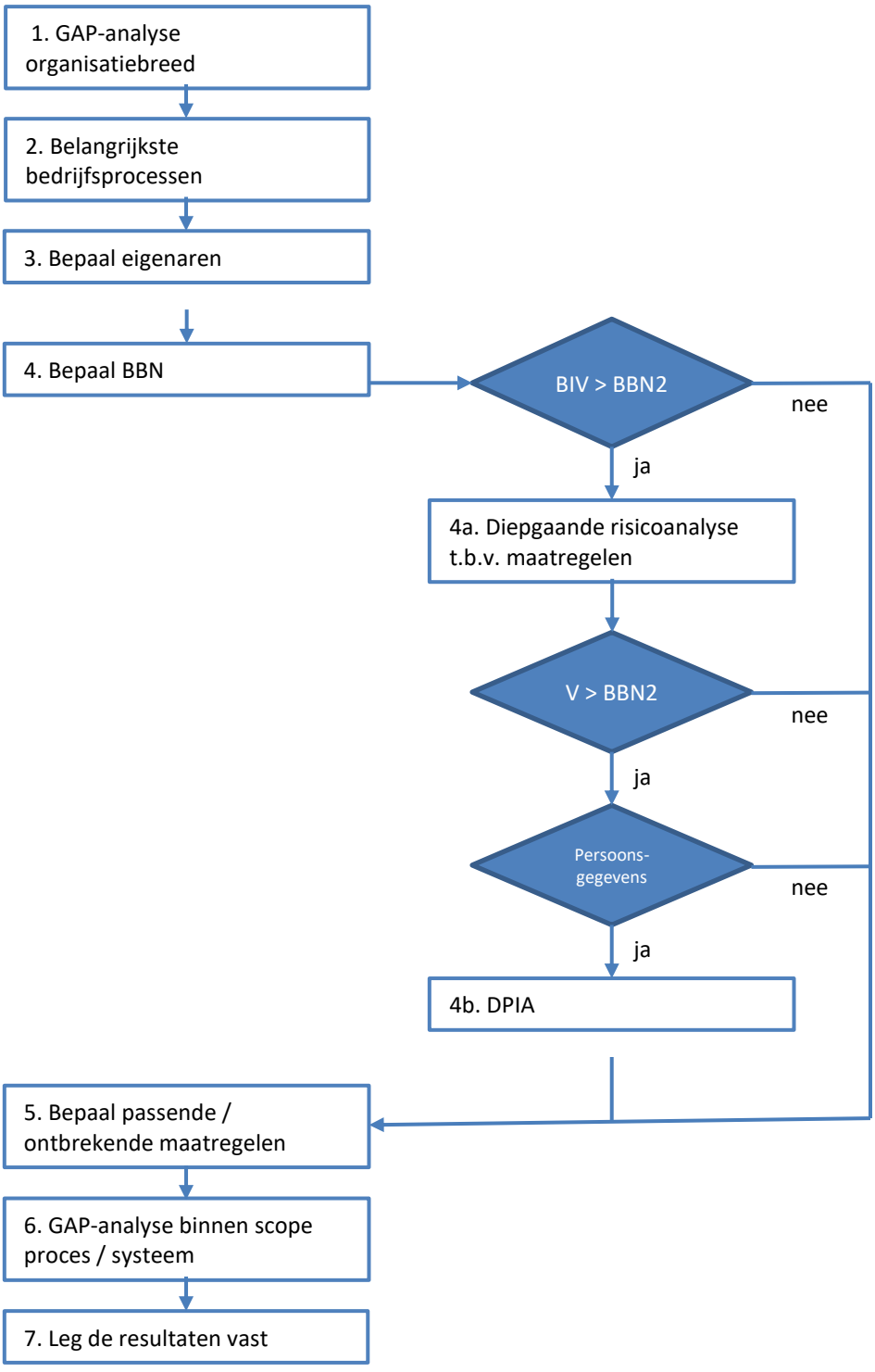
Automatisering
Bijna alle technische informatiebeveiligingsmaatregelen worden uitgevoerd door de afdeling ICT of zijn uitbesteed aan een dienstenleverancier.

Huisvesting

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

3. Aan de slag met de BIO

De BIO geeft ruimte om op basis van een risicoafweging te gaan werken en dat is ook de insteek waarmee kleine gemeenten moeten beginnen. Het gaat om prioriteiten te stellen in wat nu gedaan moet worden en wat tot later kan wachten. Houd daarbij in het achterhoofd dat de gemeente niet opnieuw begint, maar aansluit bij het beveiligingsniveau dat met de invoering van de BIG is gerealiseerd. Hieronder is het proces om de BIO in te voeren in een schema weergegeven.[4]



4 Zie voor de ondersteunende producten: https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

Hieronder worden de stappen uit het voorgaande schema verder toegelicht.

3.1. GAP-analyse organisatiebreed

De GAP-analyse is bedoeld om vast te stellen welke maatregelen al in de organisatie aanwezig zijn en welke nog niet. In het geval van de BIO valt de GAP-analyse eigenlijk uiteen in twee analyses. Dat komt doordat de BIO verplichte maatregelen kent en ook niet verplichte maatregelen. De verplichte maatregelen moeten altijd geïmplementeerd worden en zijn ook soms van toepassing op de hele gemeente. Daardoor kan de eerste analyse over de verplichte controls en maatregelen uitgevoerd worden op organisatiebreed niveau door de CISO en de eindverantwoordelijke voor de dienstverlening (bij gemeenten: de gemeentesecretaris). De verplichte maatregelen moeten altijd geïmplementeerd worden, dus kunnen deze centraal onderzocht worden. Cluster de controls en te treffen maatregelen naar soort en verdeel ze indien nodig onder andere uitvoerders binnen de gemeente of samenwerking (PIOFAH). Binnen ENSIA en ook in de GAP-analyse is uitgewerkt welke BIO controls en maatregelen voor de proceseigenaar zijn en welke centraal of aan PIOFAH actoren gegeven moeten worden. Binnen de GAP-analyse staat een kolom met specifiek en generiek. Alle specifieke maatregelen zijn in ieder geval voor de proceseigenaar. Mocht een PIOFAH actor een control/maatregel niet accepteren, dan is de GS de eerstvolgende die vanuit zijn eindverantwoordelijkheid voor de bedrijfsvoering verantwoordelijk wordt voor het borgen van de implementatie van de maatregelen om in control te komen. De basis regel was en blijft: informatie kan niet zonder eigenaar zijn, en de bijbehorende risico's (en dus maatregelen) kunnen ook niet zonder eigenaar zijn. De tweede analyse wordt in stap 6 door de proceseigenaar gedaan in aanvulling op deze eerste analyse.

3.2. Bepaal de belangrijkste processen

Inventariseer de bedrijfsprocessen en maak een keuze over welke eerst aan te pakken (op basis van belangrijkheid): de kritieke bedrijfsprocessen en de daarbij behorende essentiële systemen. Criteria voor het bepalen van kritieke bedrijfsprocessen 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.
  - Levert 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 bedrijfsproces is. Het resultaat van deze stap is een lijst met bedrijfsprocessen waar de komende periode de prioriteit op ligt (scope), stem deze lijst af met het management, laat de lijst vaststellen.

NB: 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 als daarvoor de laatste zelfevaluatie al goed was.

3.3. Bepaal de eigenaar van het proces/systeem

Zoek uit wie de proceseigenaren zijn van de kritische bedrijfsprocessen en vertel ze wat hun rol is in het geheel van de BIO. De proceseigenaar maakt op basis van een risicoafweging een keuze voor passende maatregelen. Als geen proceseigenaar kan worden benoemd, dan is de GS eindverantwoordelijk. Informatie en de bijbehorende risico's mogen nooit zonder eigenaar zijn, anders loopt de organisatie het gevaar dat de risico's

manifest worden en dat de informatie, in termen van beschikbaarheid, integriteit en vertrouwelijkheid, de bedrijfsprocessen waarbinnen deze informatie gebruikt wordt, niet meer kan ondersteunen.

3.4. Bepaal BBN

De proceseigenaren moeten (eventueel onder begeleiding van de CISO) in workshopverband de baselinetoets[5] voor hun bedrijfsproces uitvoeren. Bedenk wel dat processen binnen vergelijkbare gemeenten vaak hetzelfde zijn. Als een andere vergelijkbare gemeente al een baselinetoets uitgevoerd heeft op hetzelfde proces, dan hoeft de baselinetoets in principe niet nog eens uitgevoerd te worden. Het verdient wel aanbeveling om de resultaten van die baselinetoets op te vragen en na te lopen op bijzonderheden. Het uitvoeren van de baselinetoets is alleen noodzakelijk wanneer het vermoeden bestaat dat een proces of systeem voor wat betreft de betrouwbaarheidseisen boven het niveau van BBN2 uitkomt.
Ook is het zo dat risico's binnen één afdeling vaak van toepassing zijn op meerdere processen. Dus dat niet voor alle processen opnieuw alle stappen doorlopen moet worden, maar dat de risico's op afdelingsniveau kunnen worden bepaald. Ons advies is: cluster vergelijkbare processen en houdt de aanpak pragmatisch.

3.5. Bepaal passende/ontbrekende maatregelen

Zoek in de BIO de controls en verplichte overheidsmaatregelen bij het geselecteerde BBN om de gevonden risico's adequaat te beheersen. Naast de verplichte overheidsmaatregelen die zijn opgenomen in de BIO, dienen de proceseigenaren op basis van de risicoanalyse zelf maatregelen toe te voegen om het risico terug te brengen tot een door hen geaccepteerd niveau.

Gemeenten hebben al bestaande beveiligingsmaatregelen in het kader van de BIG, ENSIA en bijvoorbeeld de BRP en SUWI. Deze maatregelen worden ook grotendeels door de BIO afgedekt. Al geïmplementeerde beveiligingsmaatregelen kunnen dus worden meegenomen in de bepaling van controles en maatregelen op basis van de BIO. In het algemeen zullen deze maatregelen al passend zijn.

Niet elke control uit de BIO bevat concrete maatregelen. De proceseigenaar moet in dat geval bepalen welke aanvullende beveiligingsmaatregelen moeten worden getroffen om aan de control te voldoen. Ontbrekende maatregelen kunnen met behulp van de implementatierichtlijnen uit de ISO27002[6] standaard worden gekozen. Daarnaast kunnen de ondersteuningsproducten van de IBD[7] of de oude BIG worden gebruikt. En uiteraard speelt ook het gezond verstand een belangrijke rol bij de selectie van maatregelen.

3.6. GAP- en impactanalyse binnen de scope van een proces/systeem

De proceseigenaren voeren over de controls en maatregelen die van toepassing zijn op het door hen te beheren proces of systeem een GAP-analyse (verschillenanalyse) uit om vast te stellen wat nog gedaan moet worden. De overgebleven gevonden tekortkomingen en nog uit te voeren maatregen dienen in een informatiebeveiligingsplan voor de komende periode te worden opgenomen. 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.

De impactanalyse is het tweede deel van de GAP-analyse spreadsheet. Hier wordt voor ontbrekende maatregelen bepaald wie wanneer en hoe een ontbrekende of niet volledige maatregel implementeert. Dit deel geeft antwoord op de vraag: 'Hoe willen we binnen de gemeente het onderwerp beveiliging aanpakken en wie doet wat?'.
Binnen de BIO is dit vrij gelaten. Dit is een lokale keuze. Er is echter wel een 'best practice' te geven. Zie het vorige hoofdstuk over PIOFAH-actoren en maatregelen. Denk in deze stap ook na over kosten en wanneer het

[5] https://www.informatiebeveiligingsdienst.nl/product/baselinetoets-bbn-bio/
[6] https://www.informatiebeveiligingsdienst.nl/nen-iso-27001-2/
[7] https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

klaar moet zijn en hoe hierover verantwoording afgelegd moet worden. Bedenk ook dat kosten een nauwe relatie hebben met de budget/P&C-cyclus binnen de gemeente. Als men te laat in het jaar met kosten voor maatregelen komt zou het wel eens twee jaar kunnen duren voordat de maatregel gerealiseerd is.

3.7. Leg de resultaten vast

Bij het selecteren van passende controls en maatregelen is het van belang dat alles goed vastgelegd wordt. Dit omdat bij een audit, maar ook achteraf als iets onverhoopt toch misgaat (informatiebeveiliging en/of privacy gerelateerd) aangetoond kan worden dat het proces om te komen tot een BBN, controls en maatregelen juist uitgevoerd is. De proceseigenaar kan daarmee aantonen dat hij voldoende activiteiten ontplooid heeft om de informatie die onder hem berust, passend te beveiligen.

In ieder geval moet bij de proceseigenaar het volgende aanwezig zijn:

- Het verslag van de geselecteerde BBN, de controls en uitgewerkte maatregelen.
- Opname van controls, maatregelen en actiehouders in het ISMS.
- Ontbrekende controls en maatregelen in een (systeem)informatiebeveiligingsplan.

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 maatregel niet uit te voeren (als dit geen verplichte overheidsmaatregel is) of deze later uit te voeren. Dit past binnen het ‘pas toe en leg uit’ principe van de BIO. Deze goedkeuring kan gemeentebreed gelden (als je de BIO hoog over gemeentebreed toepast) maar ook per proces of per afdeling: let wel op, bewuste keuzes om bepaalde maatregelen niet te implementeren dienen door de verantwoordelijke proceseigenaar expliciet te worden gemaakt en te worden vermeld bij de betreffende maatregel zodat dit later ook kan worden verantwoord. De resultaten van deze stap worden vastgelegd in een informatiebeveiligingsplan.

4. Het informatiebeveiligingsplan

4.1. Waarom een informatiebeveiligingsplan?

Als het management de implementatie van de ontbrekende maatregelen heeft goedgekeurd, dient de implementatie van de maatregelen in een informatiebeveiligingsplan te worden opgenomen. Dit informatiebeveiligingsplan is het projectplan voor de gemeente waarin ook de verantwoordelijkheden, actiehouders en de wijze van verantwoording over de implementatie zijn vastgelegd. In het informatiebeveiligingsplan zijn de verschillende activiteiten en soms deelprojecten om beveiligingsmaatregelen ingevoerd te krijgen, opgenomen. Dit moet leiden tot een geïmplementeerde BIO. Dit plan wordt periodiek, bij voorkeur jaarlijks gemaakt. Dit plan 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. Dit kan gecombineerd worden met de jaarlijkse verantwoording in het kader van ENSIA. 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, de impactanalyse en de ENSIA-verantwoording over het voorgaande jaar. 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).

Betrek vroegtijdig de actiehouders of voortrekkers bij het opstellen van het informatiebeveiligingsplan. Zo wordt het draagvlak voor de in te voeren maatregelen 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 systeem), 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 maatregelen noemen, met het BIO-nummer.
- De vertaling van uitspraken van het informatiebeveiligingsbeleid naar het hoe, waarmee en door wie.
- De maatregelen en de prioriteit van invoeren (hoog, midden, laag) met BIO-nummer.
- De maatregel planning met: BIO-nummer, -maatregel, -doorlooptijd, -capaciteitsbeslag, eventuele kosten en wie er verantwoordelijk is.
- Welke maatregelen worden doorgeschoven naar een volgende periode op basis van een risico inschatting of de prioriteitsstelling.
- Startdatum.
- Rapportage en verantwoording.

Vastlegging van bovenstaande punten vindt veelal plaats in een ISMS.

4.2. Rapportage over de maatregelen

Gedurende de hele levenscyclus van maatregelen, vanaf het plannen tot en met uitfaseren, dient periodiek gerapporteerd te worden. Dit rapporteren gebeurt als volgt:

- De clusters aan generieke maatregelen, daarover wordt gerapporteerd door de functionaris die hier voor verantwoordelijk is, en:
- Over de specifieke maatregelen wordt gerapporteerd door de proceseigenaar of de dienstenleverancier. Dit hangt er vanaf waar de verantwoordelijkheid voor beveiligingsmaatregelen voor ICT-systemen binnen de gemeente belegd is.

Tijdens de implementatie en beheer van de maatregelen dienen de actiehouders, verantwoordelijken die benoemd zijn om maatregelen in te voeren, periodiek over de voortgang te rapporteren. Bijvoorbeeld in managementrapportages zodat op de voortgang gestuurd kan worden.

4.3. Horizontale en verticale verantwoording

De informatievoorziening en -veiligheid raakt de legitimatie van het werk van de gemeentelijke bestuurders. Gemeenten dienen hierbij invulling te geven aan hun lokaal informatieveiligheidsbeleid en dit zowel bestuurlijk als ambtelijk in de organisatie te borgen. Gemeenten dienen hierin transparant te zijn. Dit kunnen gemeenten verwezenlijken door hierover zowel horizontaal als verticaal verantwoording af te leggen.

Horizontale verantwoording is de interne verantwoording vanuit het College van B&W aan de gemeenteraad: het eigen toezichthoudend orgaan. Verticale verantwoording is de verantwoording aan de tweedelijnstoezichthouders. Op dit moment betreft dit de volgende stelsels:

Afkorting	Stelsel	Verantwoordelijk Ministerie
BRP	Basisregistratie Personen	BZK (RvIG)
PNIK	Paspoorten en Nederlandse IdentiteitsKaarten	BZK (RvIG)
BAG	Basisregistratie Adressen en Gebouwen	BZK (DGBRW)
BGT	Basisregistratie Grootschalige Topografie	BZK (DGBRW)
BRO	Basisregistratie Ondergrond	BZK (DGBRW)
DigiD	Digitale Identiteit	BZK (Logius)
GeVS (Suwinet)	Gezamenlijke elektronische Voorzieningen (GeVS) SUWI (Structuur Uitvoering Werk en Inkomen)	SZW

Voor gemeenten vindt zowel de horizontale als de verticale verantwoording plaats via ENSIA (Eenduidige Normatiek Single Information Audit).

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

VNG Realisatie