INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

*Handreiking*

# Introductie aanpak BIO

## Hoe implementeren gemeenten de BIO en hoe ziet het proces er dan uit?

INFORMATIE
BEVEILIGINGS
DIENST

# Colofon


**Naam document**

Introductie aanpak BIO

**Versienummer**

1.03

**Versiedatum**

April 2019

**Versiebeheer**

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





**Met dank aan**

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

### Wijzigingshistorie

| Versie | Datum | Wijziging / Actie |
|---|---|---|
| 0.1 | 06-11-2018 | Initiële opzet |
| 0.6 | 5-12-2018 | Start reviewronde |
| 0.9 | 15-01-2019 | Opmerkingen verwerkt, gereed voor redactie |
| 1.0 | 29-01-2019 | Publicatieversie gereed |
| 1.01 | 30-01-2019 | Enkele typos aangepast |
| 1.02 | 05-04-2019 | Opmerkingen review groep verwerkt |
| 1.03 | 05-04-2019 | Uitwerking 5.3 aangepast |

# 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 gebruik maken 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 het ondersteunen van proceseigenaar en de CISO bij het procesmatig omgaan met de BIO, want een procesmatige aanpak is de beste manier om risico's te beheersen op basis van de BIO. Voor het procesmatig uitvoeren van deze aanpak zijn een aantal stappen en activiteiten noodzakelijk die in dit document nader uitgewerkt worden.

## Doelgroep

Dit document is van belang voor de CISO.

## Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Quickscan informatiebeveiliging (QIS) (BZK)
- Handreiking Risicomanagement voor Lijnmanagers
- Diepgaande risicoanalyse (MAPGOOD)
- Data protection impact assessment (DPIA)
- Baselinetoets (spreadsheet)
- GAP-analyse
- NEN-ISO/IEC 27001:2017
- NEN-ISO/IEC 27002:2017
- Handreiking ISMS

# Inhoudsopgave

# 1. Samenvatting

In dit document is beschreven hoe met de Baseline Informatiebeveiliging Overheid (BIO) kan worden omgegaan. Dit document is geschreven voor proceseigenaren en de CISO.
De BIO is per 2020 de opvolger van de Baseline Informatiebeveiliging voor Gemeenten (BIG) waarbij het jaar 2019 als overgangsjaar is ingesteld. Het grote verschil tussen de BIG en de BIO is dat de BIO op de meest actuele versie van de ISO 27002[1] is gebaseerd en dat de BIO meer ruimte geeft voor het treffen van passende maatregelen op basis van risicomanagement. Het is de verantwoordelijkheid van elke proceseigenaar om ervoor te zorgen dat risico's binnen zijn proces passend worden beheerst op basis van de BIO. Het uitvoeren van de Baselinetoets BIO ondersteunt in de aanpak en is een activiteit dat in principe wordt uitgevoerd door de proceseigenaar.

In de inleiding van voorliggend document is het algemene belang van risicomanagement uitgelegd en de relatie met de Deming Cirkel Plan-Do-Check-Act (PDCA) van het Information Security Management Systeem (ISMS) en planning en control (P&C)-cyclus van de gemeente. Dit is noodzakelijk om iedereen die met de BIO aan de slag gaat op vlieghoogte te brengen. In hoofdstuk 3 wordt nader ingegaan op de BIO, de opbouw van de BIO en de eigenschappen in vergelijking met de BIG. Hoofdstuk 4 gaat over de procesaanpak van de baselinetoets. En hoofdstuk 5 gaat over het selecteren van controls en beheersmaatregelen met als afsluiting de vastlegging in documenten.

Voorliggend document wordt ondersteund door andere documenten uit de reeks operationele kennisproducten BIO (BIO-OP). Zo is er de Baselinetoets BIO, de diepgaande risicoanalyse met de MAPGOOD-methode, de GAP-analyse en de handreiking risicomanagement voor de lijnmanagers (zie pagina 4).

## 1.1. Processchema op hoofdlijnen

De BIO ondersteunt verschillende niveaus van beveiligen op basis van een te beschermen belang. De systeem- of proceseigenaar bepaalt procesmatig wat het beveiligingsniveau van het desbetreffende systeem of proces is en welke maatregelen genomen moeten worden om dat belang adequaat te beschermen. Het is daarnaast goed te beseffen 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 de wel aanbeveling om de resultaten van die baselinetoets op te vragen en na te lopen op bijzonderheden. De gemeente die het proces goed doorlopen heeft zal dan ook al de extra controls en maatregelen hebben uitgewerkt zodat meteen kan worden begonnen met de GAP-analyse. Met de GAP-analyse wordt dan inzichtelijke gemaakt in hoeverre de gemeente de controls en maatregelen al heeft geïmplementeerd.

In het kort zien de stappen er als volgt uit:

1. Voer de GAP-analyse uit voor alle gemeenschappelijke en centraal genomen controls en maatregelen, maak daarbij gebruik van de GAP-analyse aanpak van de IBD.
2. Inventariseer de bedrijfsprocessen volgens het interne model van procesbeschrijvingen en maak een keuze over welke eerst aan te pakken (op basis van belangrijkheid).
3. Zoek de verantwoordelijke voor het bedrijfsproces en vertel hem het belang van de baselinetoets en zijn rol in het geheel van de BIO.
4. Deze verantwoordelijke moet (eventueel onder begeleiding van de CISO) in workshop verband de baselinetoets voor zijn bedrijfsproces uitvoeren.[2]
5. Voer indien nodig een diepgaande risicoanalyse uit bij afwijkende betrouwbaarheidseisen van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid (BIV)).
6. Voer een data protection impact assessment (DPIA) uit als dat verplicht is en deze nog niet eerder uitgevoerd was.

[1] Op moment van schrijven betreft dit versie 27002:2017.
[2] De IBD heeft een baselinetoets gemaakt in de vorm van een spreadsheet met een uitleg.

7. Zoek in de BIO de controls en verplichte maatregelen bij het geselecteerde BBN om de gevonden risico's adequaat te beheersen.
8. Selecteer (bijvoorbeeld op basis van de ISO 27002) of bedenk passende maatregelen bij de controls uit de BIO waar geen verplichte maatregelen bij staan en leg dit vast.
9. Noteer de controls die niet van toepassing zijn, onderbouw waarom deze niet van toepassing zijn en bewaar het verslag van de analyse, dit is de ingevulde baselinetoets en de eventueel uitgevoerde diepgaande risicoanalyse en eventueel de uitgevoerde DPIA.
10. Cluster de controls en te treffen maatregelen naar soort en verdeel ze indien nodig onder andere uitvoerders binnen de gemeente of samenwerking (PIOFAH).
11. 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.
12. Voer over de eigen controls en maatregelen een GAP-analyse (verschillenanalyse) uit om vast te stellen wat nog gedaan moet worden en neem de GAP op in een ISMS en/of in het (integraal) informatiebeveiligingsplan zodat ze gepland worden voor implementatie.
13. Bewaak de voortgang van de implementatie (risicomanagement).

# 2. Inleiding

In dit hoofdstuk worden aan aantal begrippen uitgewerkt die nodig zijn bij het implementeren van de BIO en leggen de basis voor de verdere uitwerking van de stappen in voorliggend document.

## 2.1. Belang van Risicomanagement

Risicomanagement is de manier om de risico's te beheersen die ervoor kunnen zorgen dat de dienstverlening hinder ondervindt als deze manifest worden. Risico's in het kader van informatiebeveiliging zien toe op de betrouwbaarheidseisen: beschikbaarheid (B), integriteit (I) en vertrouwelijkheid (V) van informatie (BIV). Informatie is essentieel voor een goede dienstverlening en als deze niet of niet op tijd beschikbaar is, of niet juist of eerder of breder openbaar wordt dan gewenst, dan heeft dat gevolgen voor de gemeente én de inwoners, ondernemers, klanten en anderen. Het risico bestaat uit de kans maal de impact van deze gevolgen. Risicomanagement identificeert, beoordeelt en behandelt risico's, die mogelijk een negatieve impact hebben op de gemeentedoelen, door het waarborgen van de betrouwbaarheid van de informatie(voorziening) en de continuïteit van de dienstverlening.

Het proces van risicomanagement bestaat in veel modellen uit zes stappen[3]:

1. Bepaal doelstelling: wat wil de gemeente bereiken.
2. Identificeer risico's: een dreiging is een onzekere gebeurtenis met mogelijke gevolgen voor de doelstelling.
3. Identificeer mogelijke impact: Een risico is een dreiging waaraan een kans en gevolg toegevoegd zijn.
4. Beoordeel de risico's: Een gemeente moet van tevoren bepalen hoeveel risico gelopen mag worden, door het maken van een risicoprofiel en de risicobereidheid uit te werken en de belangrijkste risico's te prioriteren.
5. Beheers risico's: Dit kan op vier manieren:
    - Vermijden: alle mogelijke beheersmaatregelen treffen om het risico's te vermijden
    - Verminderen: beheersmaatregelen selecteren die de kans en/of impact verkleind, maar waarbij een restrisico overblijft
    - Overdragen/verzekeren: het risico wordt overdragen aan een andere partij (denk aan een brandverzekering)
    - Accepteren: het (rest)risico wordt geaccepteerd en er worden hiervoor geen beheersmaatregelen getroffen
6. Monitoring: Gedurende het hele proces volgen van risico's (meten, controleren en rapporteren) en de werking van maatregelen door deze maatregelen ook te koppelen aan het incidentmanagement proces.

Informatiebeveiliging is risicomanagement. De stap monitoring draagt bij aan het verbeteren van de kwaliteit van de informatiebeveiliging en de meest gebruikte term daarbij is PDCA. Met de Plan-Do-Check-Act (PDCA) wordt vaak bedoeld dat risicomanagement een cyclisch kwaliteitsproces is dat bestaat uit het doorlopen van een aantal processtappen, namelijk plan, do, check en act. Een andere naam voor PDCA is ook wel de kwaliteitscirkel van Deming. Door middel van het doorlopen van PDCA-cyclus wordt gemonitord of de genomen beheersmaatregelen nog effectief zijn en zich nieuwe of andere risico's voordoen die nog niet beheerst worden. Het zorgt er dus voor dat een passend beveiligingsniveau wordt gehandhaafd en het waarborgt een lerende gemeente.

## 2.2. P&C

Planning en Control (P&C) is de begroting- en verantwoordingscyclus van een typische gemeente en beweegt zich langs de financiële verantwoording vanaf de planfase tot en met de jaarrekening. De P&C-cyclus is een bestaand proces binnen gemeenten, waar informatiebeveiliging in haar communicatie op kan aansluiten. Via de P&C-cyclus kan gerapporteerd worden aan verschillende stakeholders over de doelen van informatiebeveiliging en de voortgang op deze doelen (verantwoording). Informatiebeveiligingsdoelstellingen moeten gerelateerd zijn aan het gemeentejaarplan en moeten de gemeente ondersteunen in het behalen van de gemeente doelstellingen.

[3] https://www.coso.org/Documents/COSO-2015-3LOD.pdf

## 2.3. GAP-analyse

De GAP-analyse is bedoeld om vast te stellen welke maatregelen al in de organisatie aanwezig zijn of geïmplementeerd 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 corporate niveau door de CISO en de eindverantwoordelijke van de dienstverlening (bij gemeenten: de gemeentesecretaris) voor 3 BBN's, want de verplichte maatregelen moeten namelijk altijd geïmplementeerd worden, dus kunnen deze centraal onderzocht worden. De tweede analyse wordt gedaan in aanvulling op de eerste door de proceseigenaar nadat deze alle stappen uit dit document doorlopen heeft. Daarbij kan hij gebruik maken van wat er binnen de centrale GAP-analyse al naar voren gekomen is.

# 3. Eigenschappen BIO

In dit hoofdstuk worden de belangrijkste eigenschappen van de BIO nader toegelicht, zodat een basis gelegd wordt om efficiënt met de BIO en risicomanagement te kunnen omgaan.

## 3.1. Verschil met de BIG

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)( die van 2013 tot en met 2019 geldt) en de BIO (die per 2020 geldt en waarbij 2019 het overgangsjaar is) verschillen in werkelijkheid niet veel van elkaar als het gaat om de controls (zie paragraaf 3.2 Indeling BIO). Waar het wezenlijke verschil ligt is in de aanpak en de keuzevrijheid als het gaat om de selectie van maatregelen om controls te laten werken. Een ander verschil is dat de BIG gebaseerd was op de ISO27002:2007 en de BIO op de ISO27002:2017. Waar de BIG 300+ maatregelen kent en één niveau van beveiliging kan de proceseigenaar nu kiezen 3 niveaus van beveiligen op basis van het onderkende te beschermen belang. Hierbij worden verplichte maatregelen genomen en optionele maatregelen geselecteerd die moeten bijdragen aan het behalen van de doelstelling. De nieuwe BIO kent drie basisbeveiligingniveaus, 133 controls (zie paragraaf 0) terwijl de BIG 136 controls kent. Het grootste verschil tussen de BIO en de BIG zit in de hoeveelheid maatregelen.

## 3.2. Indeling BIO

De indeling van de BIG, BIO en de ISO 27002 reeks is hetzelfde:

- Hoofdstukken (clausules):
  Dit zijn aandachtsgebieden voor beveiliging. Zo is er bijvoorbeeld een hoofdstuk 5: Beleid en een hoofdstuk 6: Rollen en verantwoordelijkheden.
- Hoofd beveiligingscategorieën (beheersdoelstellingen):
  Dit zijn in de BIO de tweede niveau paragrafen zoals bijvoorbeeld 6.1 Interne Organisatie
- Beheersmaatregelen (dit noemen wij in de BIO: Controls (ook wel maatregel doelstellingen)):
  Dit is het derde niveau van paragrafen. Controls zijn beheersmaatregelen, maar zij kennen geen specifieke implementatiemaatregelen. Tot op control niveau is er feitelijk geen verschil tussen de ISO 27002:2017 en de BIO. De teksten zijn exact gelijk. Pas vanaf BBN3 kunnen in de toekomst controls worden toegevoegd aan de BIO om mogelijke extra maatregelen een plaats te geven binnen de BIO. Control voorbeeld: 6.1.1. Interne Organisatie.
- Implementatierichtlijnen en overige informatie (maatregelen):
  De ISO 27002 kent op dit niveau losse tekst die helpt bij het inrichten van de control, allemaal aandachtspunten waar aan gedacht kan worden bij het implementeren van de controls. Het verschil tussen de ISO en de BIO ligt hierin dat de BIO bij controls soms wel en soms geen concrete maatregelen kent. Maatregelen in de BIO zijn altijd verplicht, tenzij ze niet van toepassing kunnen zijn. Bijvoorbeeld een maatregel gaat over beleid (5.1.1.1) maar deze is centraal ingevuld en dus hoeft de proceseigenaar dit niet nog eens te doen.

Als in de BIO bij een control geen maatregelen staan moeten deze tijdens risicoanalyse zelf bepaald worden of moet gebruik gemaakt worden van bestaande maatregelen, u kunt hier o.a. de ondersteuningsproducten van de IBD[4], de ISO 27002:2017, de oude BIG of de ISOR[5] voor gebruiken. U mag natuurlijk ook nog steeds zelf maatregelen verzinnen op basis van gezond verstand.

[4] https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
[5] https://www.noraonline.nl/wiki/ISOR_(Information_Security_Object_Repository) & https://www.cip-overheid.nl/category/producten/isor

## 3.3. Controls

Control is de Engelse term voor beheersmaatregel (ISO term) en er is afgesproken dat de BIO de Engelse term gebruikt in plaats van de Nederlandse ISO term. De Control is het niveau waarop een auditor beoordeelt (en de Eenduidige Normatiek Single Information Audit (ENSIA) ook). 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.

## 3.4. Maatregelen

Een maatregel kan gevonden worden in de BIO (verplicht), kennisproducten van de IBD, in de oude BIG, de ISOR, de ISO 27002:2017 en ze kunnen ook bepaald worden op basis van een risicoanalyse. Een maatregel maakt de control concreet. Maatregelen kunnen bepaald worden op basis van de implementatierichtlijn uit de ISO 27002:2017. 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. Deel 2 van de BIO heeft dezelfde hoofdstukindeling en nummering als de ISO 27002:2017.

## 3.5. Implementatierichtlijn

De Implementatierichtlijn is onderdeel van de ISO 27002:27002 en bevat aanwijzingen, aandachtspunten en overige informatie om bij een control passende maatregelen te bedenken. Implementatierichtlijnen geven richting en maken een control concreet.

Zie ook Figuur 3.5: Voorbeeld Control met implementatierichtlijn.

**6.1.4 Contact met speciale belangengroepen**

Beheersmaatregel

Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele gemeenten te worden onderhouden.

Implementatierichtlijn

Lidmaatschap van speciale belangengroepen of fora behoort te worden overwogen als middel om:

a) kennis te verbeteren over 'best practices' en op de hoogte te blijven van relevante beveiligingsinformatie;

b) ervoor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is;

c) vroegtijdige waarschuwingen te ontvangen inzake alarm, adviezen en patches die verband houden met aanvallen en kwetsbaarheden;

d) toegang te krijgen tot gespecialiseerd advies over informatiebeveiliging;

*Figuur 3.5: Voorbeeld Control met implementatierichtlijn*

De ISO 27001 en 27002 kunnen worden gedownload bij de NEN door overheidspartijen op basis van het gebruikte mailadres waarmee geregistreerd wordt op NEN-connect:

**NEN/ISO vrij beschikbaar voor overheid**

De overheid heeft in overleg met NEN de volgende twee informatiebeveiligingsnormen vrij beschikbaar gesteld voor gemeenten, waterschappen en provincies in NEN Connect. Deze normen zijn nodig bij een goede implementatie van de BIO (Baseline Informatiebeveiliging Overheid).

- NEN-NL-ISO/IEC 27001:2017
- NEN-NL-ISO/IEC 27002:2017

**Samenwerkingsverbanden**

Ook samenwerkingsverbanden kunnen gebruik maken van NEN connect, maar de NEN zal naar alle waarschijnlijkheid moeite hebben met het beoordelen van de organisatienaam, want de NEN doet op basis van een ingevuld aanvraagformulier bepalen of er recht op toegang bestaat. Bij twijfel neemt de NEN vwb samenwerkingsverbanden contact op met de IBD

**Gratis toegang via NEN Connect**

Vul het online aanvraagformulier [1] in om toegang te krijgen tot NEN Connect. Ook indien u al een NEN Connect licentie heeft, dient u het formulier in te vullen. Let er wel op dat u de juiste organisatienaam gebruikt! Meer info zie [2].

[1] http://nen.m5.mailplus.nl/genericservice/code/servlet/React?wpEncId=8fZMVJAawV&wpMessageId=21577&userId=80151&command=viewPage&activityId=test&encId=1

[2] https://www.nen.nl/nenconnectbio

# 4. Procesaanpak

Het is van belang dat de beoordeling van de te beschermen belangen altijd op dezelfde manier gebeurt, de BIO kent daarvoor de term basisbeveiligingsniveau (BBN). Deze BBN's bestaan uit 3 niveaus van beveiligen. Op basis van een uitgevoerde Baselinetoets wordt gestructureerd beoordeeld op welk niveau het proces beveiligd moet worden.
De Baselinetoets BIO (een Excel bestand) behoort tot de reeks operationele kennisproducten BIO (BIO-OP).

Behalve de BBN-bepaling is daarin ook een blad opgenomen met vragen over de 13 verwerkingsgronden en de vragen waarvoor een data protection impact assessment (DPIA) verplicht is uit de Algemene verordening gegevensbescherming (AVG) om te bepalen of een DPIA moet worden uitgevoerd. Feitelijk is dit een PRE-PIA om vast te stellen of een DPIA moet worden uitgevoerd.

## 4.1. Baselinetoets aanpak

De Baselinetoets BIO kent de volgende stappen:

Stap 1: Beantwoord algemene vragen, bepaal scope, het proces, de keten, de externe eisen, wet- en regelgeving en de eigenaar
Stap 2: Vul vragen in over beschikbaarheid
Stap 3: Vul vragen in over integriteit
Stap 4: Vul vragen in over vertrouwelijkheid
Stap 5: Vul vragen in over privacy
Stap 6: De spreadsheet geeft in het tabblad resultaat de score weer en hieruit kan worden afgeleid wat de vervolgstappen zijn.
Stap 7: Stel resultaten vast

## 4.2. Vervolg baselinetoets

In het geval dat de betrouwbaarheidseisen (BIV) allen op hetzelfde BBN-niveau uitkomen na het uitvoeren van de baselinetoets, hoeft er geen diepgaande risicoanalyse meer te worden uitgevoerd, het proces valt dan binnen de baseline voor dat niveau. Wat dan nog wel moet gebeuren is dat de controls die binnen de geselecteerde BBN vallen en die geen maatregelen kennen, voorzien van passende maatregelen op basis van een risicoafweging. In principe bepaalt de BBN score voor vertrouwelijkheid het overall eindresultaat.

Valt één (of meerdere) betrouwbaarheidseis(en) van beschikbaarheid en/of integriteit buiten de geselecteerde BBN voor vertrouwelijkheid (in positieve zin, dus zwaarder), dan moet voor die betrouwbaarheidseis of die betrouwbaarheidseisen een diepgaande risicoanalyse uitgevoerd worden om daarmee de extra controls en maatregelen te selecteren voor die betrouwbaarheidseisen. Als vastgesteld wordt dat privacy mogelijk van belang is dan moet mogelijk daarnaast nog een DPIA worden uitgevoerd. Beide analyses zijn geen onderdeel van deze aanpak beschrijving en zijn separaat uitgewerkt in onze handleiding DPIA[6] en de diepgaande risicoanalyse[7] met MAPGOOD.

[6] https://www.informatiebeveiligingsdienst.nl/?s=pia
[7] https://www.informatiebeveiligingsdienst.nl/?s=risicoanalyse

# 5. Maatregelselectie

## 5.1. Goede doelstellingen en maatregelen

Het uitvoeren van een baselinetoets is stap één (zie paragraaf 1.1 voor een beschrijving van het processchema) maar het vinden van passende maatregelen bij geselecteerde controls vereist risicodenken. Er moet worden vastgesteld wanneer een maatregel passend is en hoeveel deze maatregel dan bijdraagt aan de control. Voor maatregelen geldt:

1. De maatregel is passend en draagt voldoende bij aan het behalen van de doelstelling van de control;
2. De maatregel is niet passend:
    a. Maatregel is te duur > zoek alternatieven of andere maatregelen of;
    b. Maatregel past niet (geheel) > zoek naar alternatieven die beter aansluiten bij de doelstelling of;
    c. Kies uit andere mitigatie strategieën:
        i. Preventie: het voorkomen dat iets gebeurt of het verminderen/verkleinen van de kans dat het gebeurt;
        ii. Detectie: het detecteren van de (potentiële) schade wanneer een bedreiging optreedt;
        iii. Repressie: het beperken van de schade wanneer een bedreiging optreedt;
        iv. Correctie: het instellen van maatregelen die worden geactiveerd zodra iets is gebeurd om het effect hiervan (deels) terug te draaien;
        v. Acceptatie: geen (additionele) maatregelen, men accepteert de kans en het mogelijke gevolg van een bedreiging;
        vi. Overdragen: financieel d.m.v. verzekeren of operationeel d.m.v. outsourcen.

Het is van belang dat deze stap goed wordt uitgevoerd omdat de discussie achteraf bij een audit juist over het selectie proces zal gaan en over de mate waarin de maatregel bijdraagt aan het behalen van de control. Uiteraard gaat het niet om de discussie alleen, maar altijd om het juist mitigeren van risico's met passende maatregelen.

## 5.2. Waar kan ik maatregelen nog meer vinden?

Voor het kiezen en vaststellen van passende maatregelen kan gebruik worden gemaakt van:

- De BIG, in de BIG waren al maatregelen vastgesteld (het niveau van de BIG is BBN2).
- De ISO 27002, hierbij kunnen op basis van de implementatierichtlijn bij een doelstelling (control) passende maatregelen worden gekozen en vastgesteld wanneer concrete maatregelen bij de control ontbreken.
- De ondersteuningsproducten van de IBD. U vindt maatregelen in het BIO-OP document met passende maatregelen bij BIO controls waarbij geen maatregel genoemd wordt.[8]
- De Information Security Object Repository (ISOR), in deze database is per thema uitgewerkt wat passende controls en maatregelen kunnen zijn, en biedt de mogelijkheid om op control basis te zoeken naar maatregelen en/binnen thema's.[9]

## 5.3. Wanneer wel of niet van toepassing verklaren?

Controls binnen een BBN kennen een aantal toestanden:

1. De control bevat al maatregelen, deze control is binnen de BBN altijd verplicht en er kan niet voor gekozen worden de control te laten vervallen (of beter het bijbehorende risico te accepteren) tenzij de control niet van toepassing is. De maatregelen zijn passend om in control te komen.
2. De control bevat nog geen maatregelen, deze control kan:
    a. Niet van toepassing zijn (er hoeven dan geen maatregelen bepaald te worden);
    b. Wel van toepassing zijn, en er moeten nog passende maatregelen bepaald worden.

[8] Dit BIO-OP document is op het moment van schrijven nog niet beschikbaar. [wellicht kun je beter aangeven per wanneer een en ander beschikbaar komt, bijvoorbeeld vanaf begin kwartaal 2-2019 komen de eerste producten beschikbaar.
[9] Zie hiervoor de website van de NORA (https://www.noraonline.nl/wiki/ISOR_(Information_Security_Object_Repository)

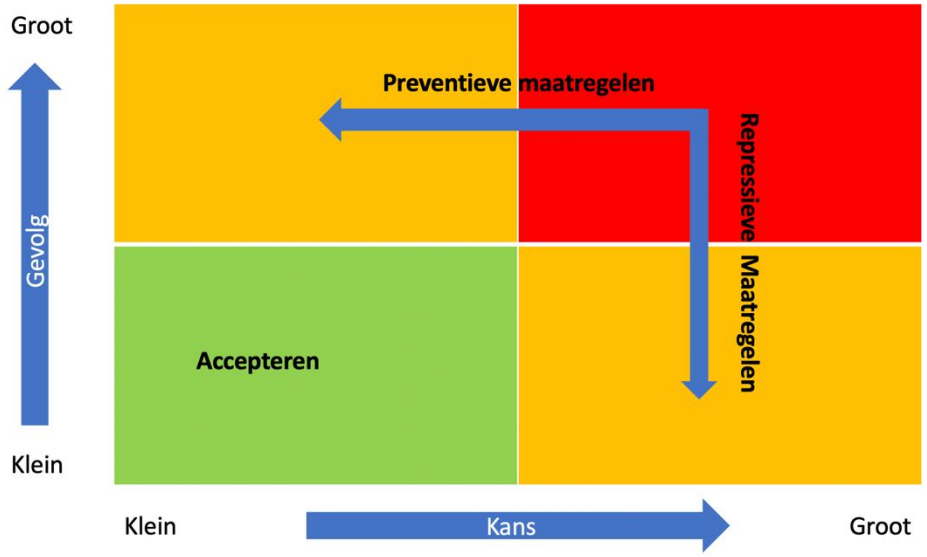
## 5.4. Implementeren van maatregelen

Controls en maatregelen moeten onderzocht worden op aanwezigheid binnen de afdeling van de proceseigenaar (middels een GAP-analyse), of binnen de gemeente. Controls en maatregelen kunnen namelijk van toepassing zijn op anderen dan de proceseigenaar zelf. Dat heeft tot gevolg dat de proceseigenaar afspraken moet maken over die controls en maatregelen. Andere afdelingen zijn bijvoorbeeld: facilitaire zaken, Personeel en Organisatie (P&O) en Informatisering & Automatisering (I&A). In de BIO is een start gemaakt met een selectie van controls en maatregelen met een toewijzing aan externe ICT-leveranciers, deze leverancier kan een (intern) ICT-samenwerkingsverband of een externe ICT-leverancier zijn.
Deze externe/interne afdelingen voeren controls en maatregelen uit voor de proceseigenaar en ondersteunen daarmee het bedrijfsproces. Afhankelijk van de afspraken in bijvoorbeeld een convenant, samenwerkingsovereenkomst of inkoopdocument zal de externe of interne behandelaar zich moeten verantwoorden over de mate waarin zij controls en maatregelen geïmplementeerd heeft.

Dit onderzoek wordt uitgevoerd met een GAP-analyse of nulmeting. Deze analyse brengt in kaart welke maatregelen al genomen zijn, wie ervoor verantwoordelijk is, welke maatregelen nog niet genomen zijn, de impact in tijd en geld. Op basis van deze analyse wordt het informatiebeveiligingsplan van de gemeente of van de afdeling gevuld met activiteiten om de ontbrekende controls en maatregelen te implementeren.[10]
Alle controls en maatregelen moeten worden opgenomen in het Information Security Management Systeem (ISMS), zodat zij kunnen worden meegenomen in de PDCA-cyclus. Voor de ontbrekende controls en maatregelen moeten actiehouders worden benoemd en afspraken worden gemaakt wanneer deze maatregelen getroffen moeten zijn.

## 5.5. Risico

Risico, wat is dat eigenlijk? Een risico is een gekwantificeerde dreiging berekend op basis van de kans en het gevolg ofwel de impact. Zoals in figuur 5-1 te zien is kunnen risico's als gevolg van een analyse in één van de vier kwadranten vallen. De blauwe pijlen in het rode kwadrant geven aan welk soort maatregelen getroffen kunnen worden. Dat betekent ook dat een combinatie van soort maatregelen nodig kan zijn om in het groene kwadrant uit te komen.




*Figuur 5-1 Risicokwadranten*

[10] Zie hiervoor ook het BIO-OP document 'GAP-analyse' van de IBD: https://www.informatiebeveiligingsdienst.nl/?s=gap

## 5.6. Restrisico

Een risico kent eigenlijk ook altijd een restrisico, want maatregelen dragen bij aan het verminderen van het risico en dan blijft er eigenlijk altijd wat risico over. Daarom dienen alleen maatregelen gekozen te worden die daadwerkelijk bijdragen aan het mitigeren van het risico tot een acceptabel niveau. Een maatregel zou ook verzekeren kunnen zijn, waarover nog een interessante discussie gevoerd is op onze community. In principe is het restrisico acceptabel als de genomen maatregelen ervoor zorgen dat de Kans en Gevolg (lees impact) beide op laag staan (risicokwadrant linksonder), maar een gemeente kan ook risico's accepteren die zich in het oranje vlak bevinden.

## 5.7. Vastlegging

Bij het uitwerken van het BBN-niveau door middel van een analyse en 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:

1. Het verslag van de uitgevoerde baselinetoets.
2. Het verslag van de geselecteerde BBN, de controls en uitgewerkte maatregelen.
3. Eventueel resultaat van een uitgevoerde diepgaande risicoanalyse.
4. Eventueel resultaat van een uitgevoerde DPIA.
5. Opname van controls, maatregelen en actiehouders in het ISMS.
6. Ontbrekende controls en maatregelen in een (systeem)informatiebeveiligingsplan.

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