gemeente Gemert-Bakel

Informatiebeveiliging

Ruud Kerssens RE RA CISA CRISC

Secura

Onderzoek Rekenkamer Commissie

Rol en ambitie Rkc

Zinnig, zuinig en zorgvuldig?

Aanleiding

1. Data afhankelijkheid steeds belangrijker
2. Datalekken en ontoereikende beveiliging

Doel

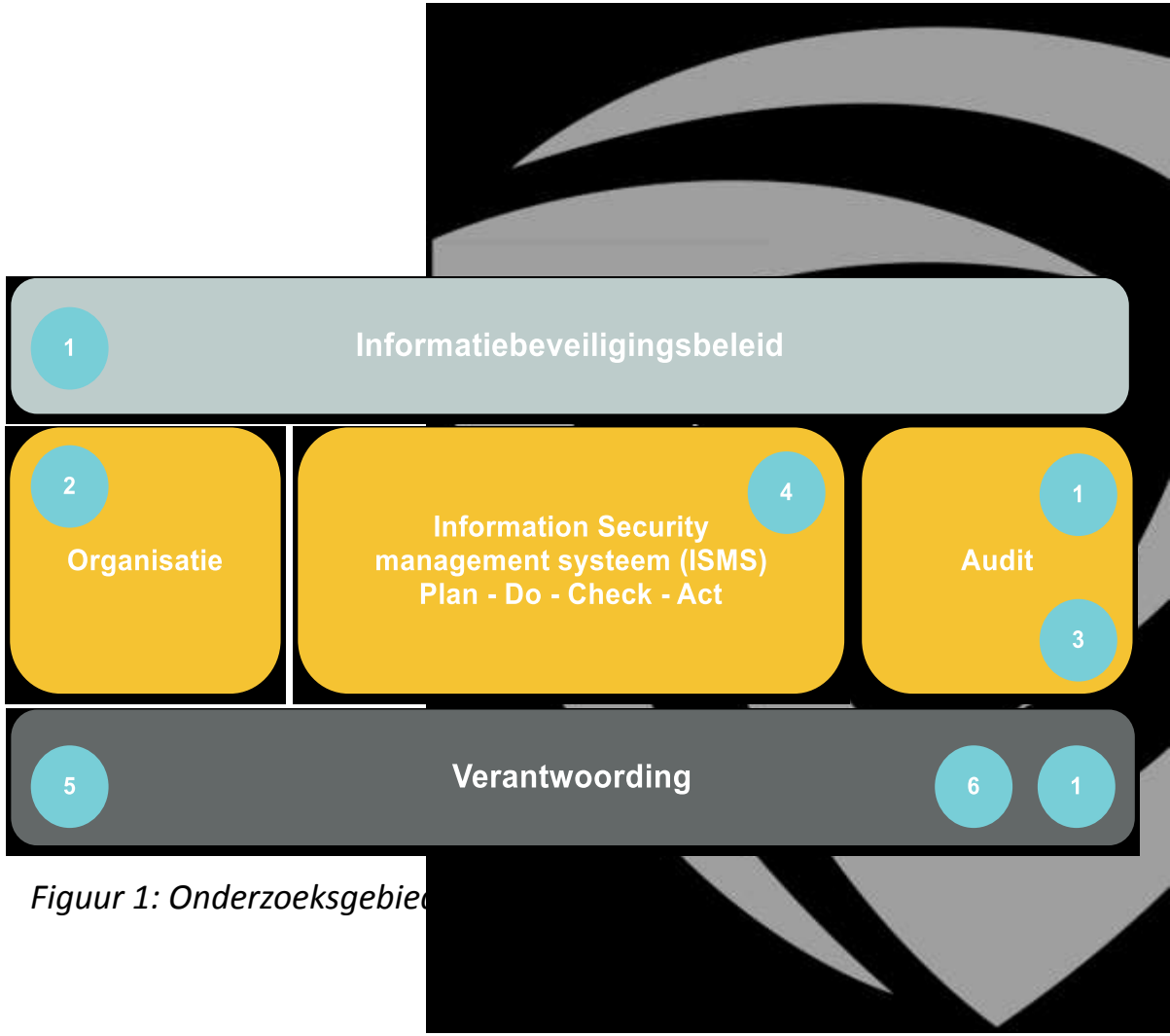
Raad in positie brengen

Secura

1. Opdracht

Hoofddoel

1. In hoeverre is de (digitale) informatiebeveiliging van de gemeenten Gemert-Bakel en Laarbeek in de praktijk op orde?
2. Zijn beide gemeenten alert en actief genoeg om de informatiebeveiliging oplossingsgericht te verbeteren en kan de raad ervan op aan dat het goed gaat?



Figuur 1: Onderzoeksgebied

<u>Vooronderzoek</u>:

1. Voldoet de gemeente Gemert-Bakel aan de ‘normen’?
2. Hoe is de organisatorische inrichting van de informatiebeveiligin
3. Welke beveiligingschecks worden zoal uitgevoerd?
4. Welke maatregelen zijn getroffen rond back-ups?
5. Hoe vindt de opvolging plaats bij gesignaleerde tekortkom n?
6. Hoe is de monitoring ingericht door de raad?

Secura

2. Dreigingen voor gemeenten

Risico's en prioriteiten

Risico's 2019–2020	**Imagoprobleem informatiebeveiliging** Laag op de politieke agenda, weinig bewustzijn en onvoldoende budget. › pag. 10	**Risico's niet integraal in beeld** De risico's die wel in beeld zijn, krijgen bovenmatig veel aandacht › pag. 11	**Basis niet op orde** Simpele routine-aanvallen zijn vaak succesvol › pag. 12	**Te weinig mensen** Te veel werk, en te weinig gekwalificeerde specialisten › pag. 12	**Complexiteit neemt toe** Gemeenten zien kansen van innovatie, maar niet de risico's › pag. 13
Prioriteiten 2019–2020	**Informatiebeveiliging op de agenda** Zorg ervoor dat informatie-beveiliging aandacht krijgt. › pag. 16	**De basis op orde** Verhoog de digitale weer-baarheid van uw gemeente. › pag. 17	**Versterk de menselijke schakel** Bewuste medewerkers zijn de beste beveiligings-maatregel. › pag. 18	**Versterk de CISO** Stel de CISO in staat om u optimaal te kunnen adviseren. › pag. 18	**Inzicht in nieuwe technologieën** Pas *security- & privacy-by-design*-principes toe. › pag. 19

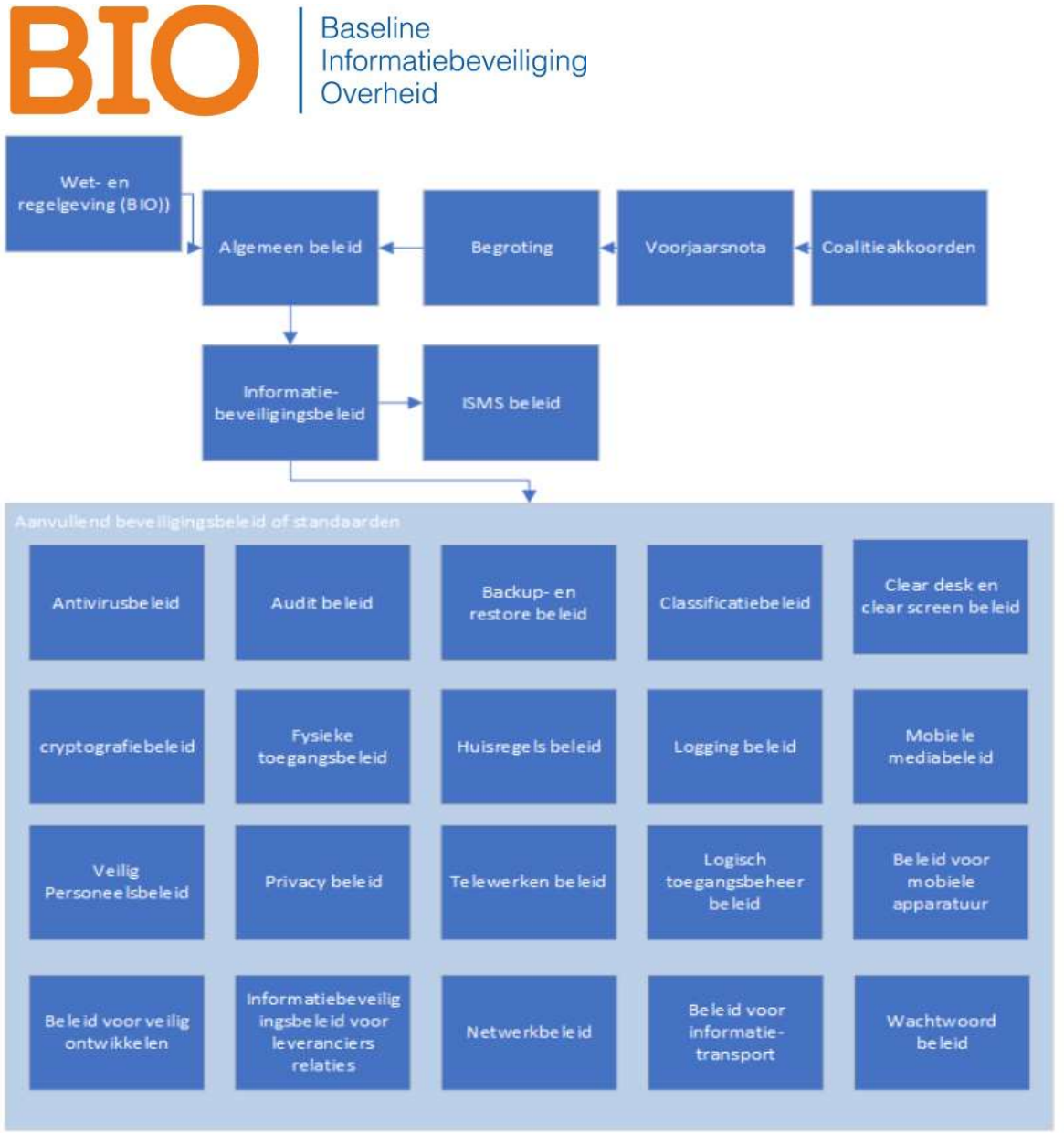
Secura

3. Belangrijk

Bron: Pawnixel.com

Dus

1. Beleid stelt de doelstellingen.
2. Informatieveiligheid is een samenspel.
   De mensfactor is zeer bepalend.
3. Informatie kun je niet 100% te beveiligen.
4. Informatiebeveiliging kan niet met onevenredige investeringen. Effectiviteit en efficiëntie spelen een rol.
5. Risicomanagement drijft op het kennen van je risico's en risicohouding.



Bron: IBD – Handreiking beleid BIO V1.0 – april 2019

Secura

4. Daarom aandachtsgebieden

Identify	Protect	Detect	Respond	Recover
Het vaststellen van wat belangrijk is voor de organisatie. Het uitvoeren van een risk assessment. Het bepalen van het informatie-beveiligings-beleid	Het nemen van preventieve maatregelen zoals toegangs-beveiliging, technische maatregelen bewustwording, gegevens-beveiliging, IT beheer, wijzigingen-beheer etc.	Het inregelen van logging van activiteiten en gebeurtenissen in het netwerk en met IT systemen. Het inrichten van monitoring.	Incidenten opvolgen, communiceren, analyseren, oplossen, maatregelen plannen, leren van incidenten en realiseren van verbeter-maatregelen	Herstelmaatregelen inrichten, verbeteren en over het gebruik ervan communiceren.

Secura

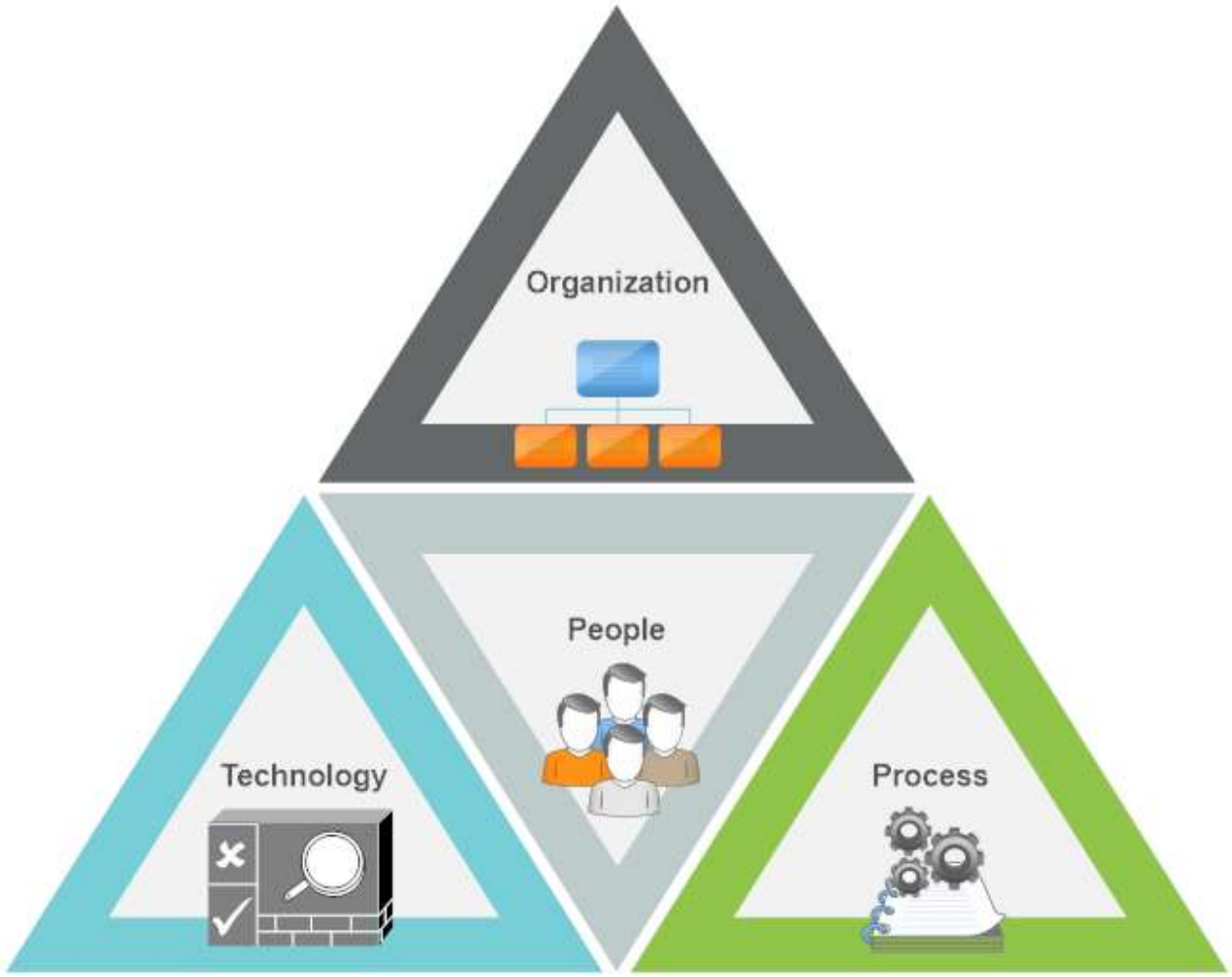
5. PPOT

People

Process

Organization

Technology



6 Risicomanagement

INFORMATIE BEVEILIGINGS DIENST

BIO | Baseline Informatiebeveiliging Overheid

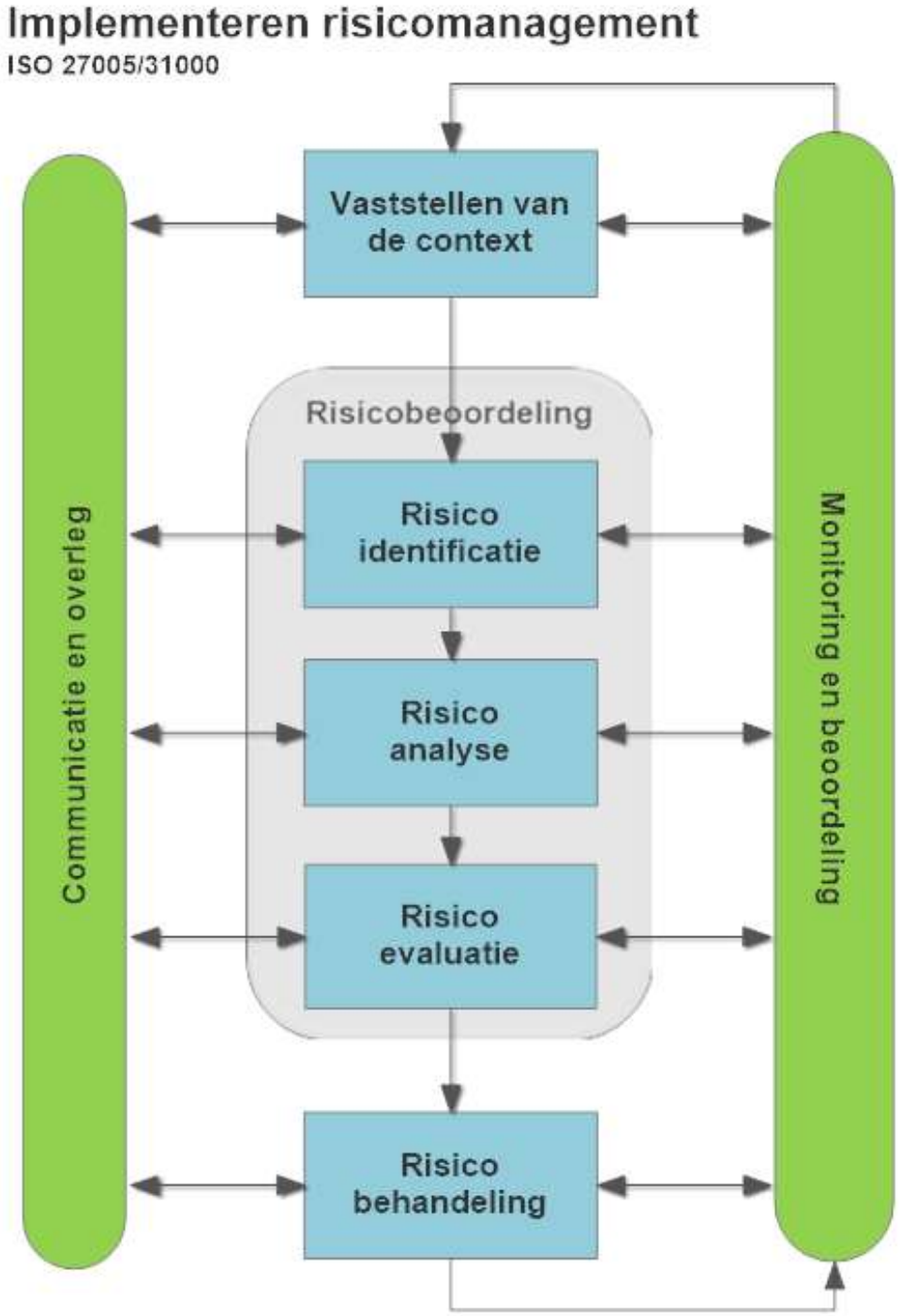
Baselinetoets BBN BIO

- BBN1: beschikbaarheid = Laag; integriteit = Laag; vertrouwelijkheid = Laag
- BBN2: beschikbaarheid = Laag; integriteit = Laag; vertrouwelijkheid = Midden
- BBN3: beschikbaarheid = Laag; integriteit = Laag; vertrouwelijkheid = Hoog

Diepgaande risicoanalyse methode gemeenten

versie 1.1, november 2016
– Wijzigingsvoorstellen en opmerkingen verwerkt, huisstijl gelijkgetrokken met de andere BIG-producten

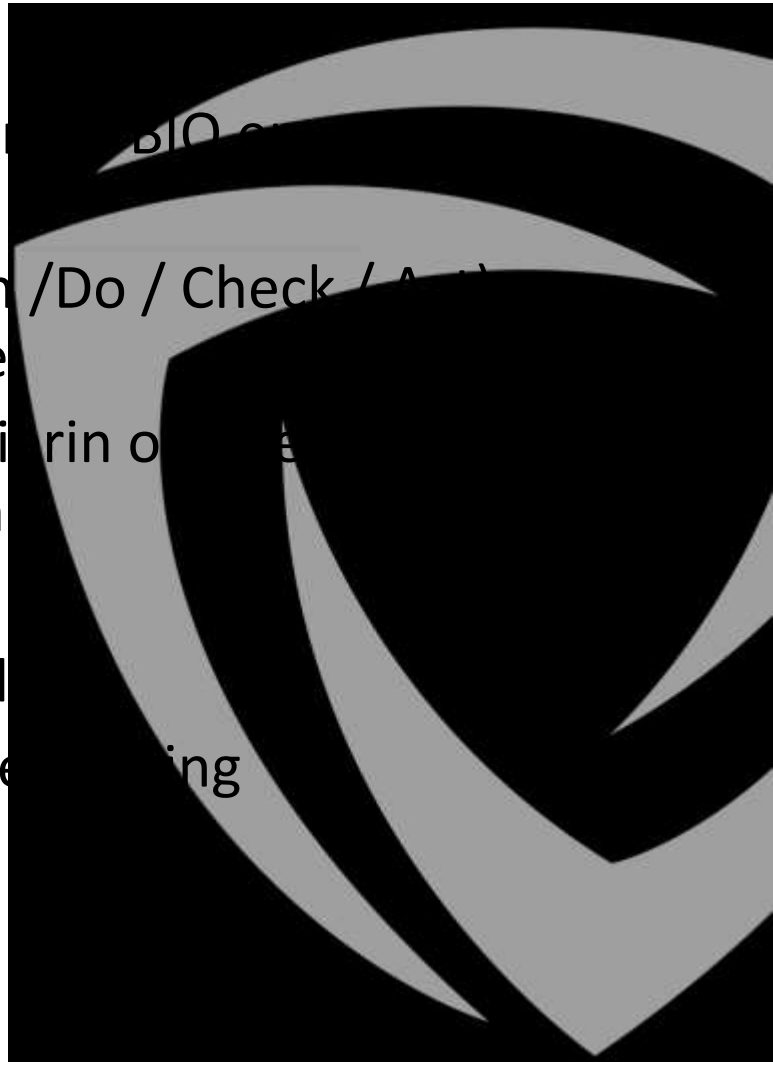
versie 2.0, april 2019
– BIO update



Secura

7. Aanbevelingen

1. **Informatiebeveiligingsbeleid** actualiseren aan de hand va[illegible] BIO e[illegible] producten IBD;
2. Inrichten **risicomanagement** proces. Betrek de PDCA (Plan /Do / Check / A[illegible] management cyclus in de P&C cyclus binnen de gemeente
3. **Afhankelijkheden- en kwetsbaarheden analyse**. Betrek hi[illegible]rin o[illegible] BIO toets om het BBN (Basisbeveilignsniveau) te bepalen
4. **Communicatieplan** (“People” aspect)
5. **Classificatie** van gegevens (waaronder privacy gerelateerd
6. **Samenwerkingsverbanden / uitbesteding** en informatiebe[illegible]ing synchroniseren;
7. **Continuïteitsplan** (en implementatie);
8. **Nulmetingen** (BIO en AVG) en bewaken opvolging.



Secura

Raad?

- Op de agenda
- Eén aanspreekpunt in College B&W
- Rapport een handvat
- Bevragen B&W op mijlpalen
- Bewaken opvolging mijlpalen
- Monitoren opvolging uitkomsten nulmetingen

FOLLOW US ON

Secura