INFORMATIE
BEVEILIGINGS
DIENST

Webinar Pragmatische aanpak BIO

Praktische tips en oplossingen

Kees Hintzbergen en Ger Lütter

Ondersteuning Webinar: Frits Grotenhuis (IBD)
Datum: 23 januari 2020

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

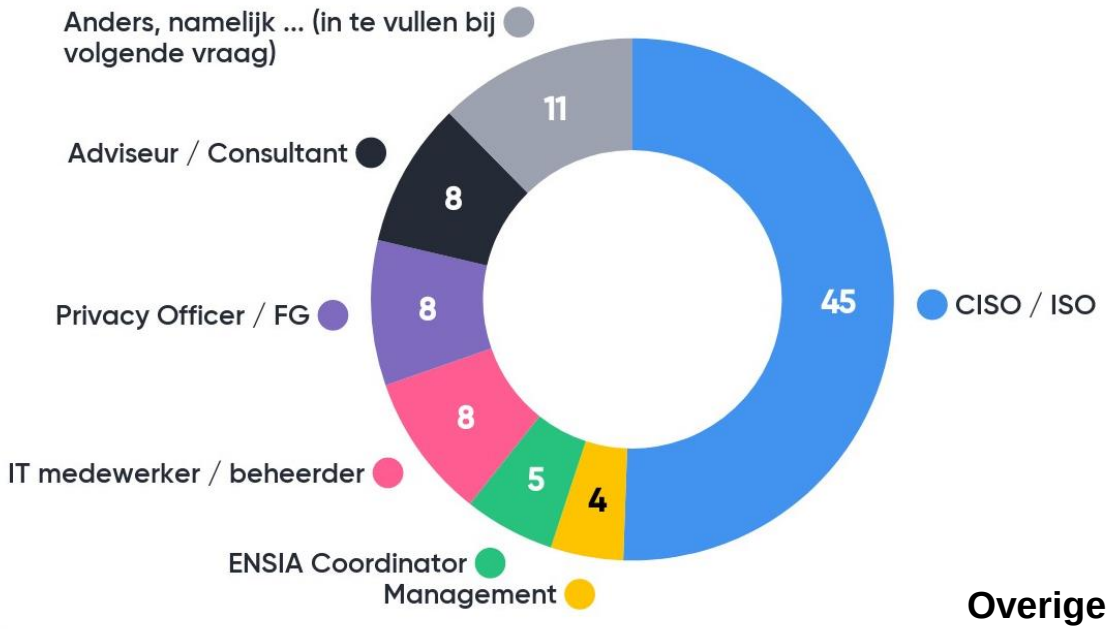
Doel van dit Webinar

Aan het eind van dit Webinar heeft u inzicht in:

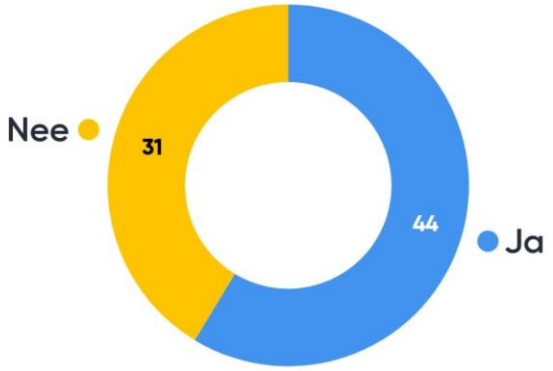
- Het stellen van de juiste prioriteiten bij de implementatie van de BIO
- Hoe op eenvoudige wijze het juiste BBN op de BIV-aspecten van elk werkproces kan worden bepaald
- Hoe het door de IBD ter beschikking gestelde hulpmiddel u hierbij kan ondersteunen
- Het belang van een risicoregister en een risicoacceptatie-overeenkomst (RAO)

INFORMATIE BEVEILIGINGS DIENST

Wat zijn de deelnemers?



3. Bent u verantwoordelijk voor het implementeren van de BIO?



Overige functies:

INFORMATIE BEVEILIGINGS DIENST

Basisbegrippen

5

- Hoofdstukken
- Controls
- Overheidsmaatregelen

Informatiebeveiliging

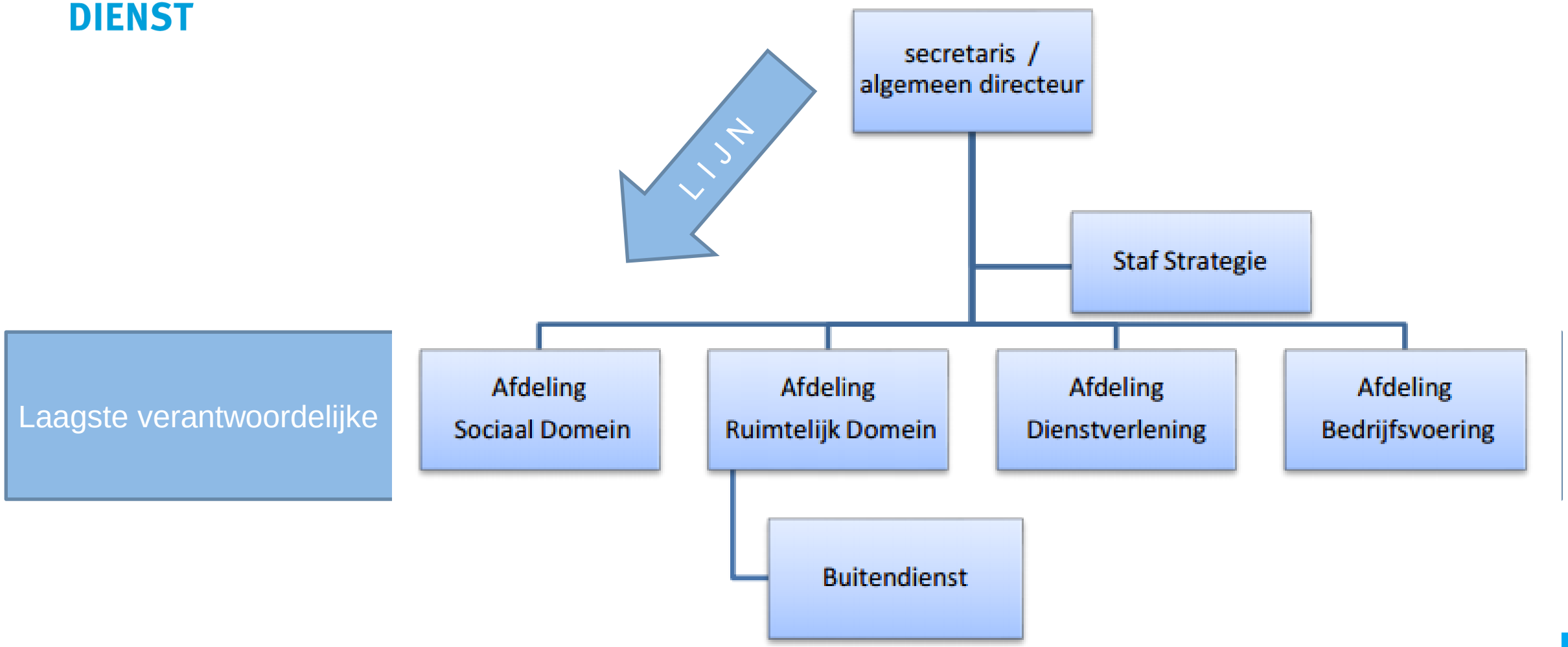
5.1 Aansturing door de directie van de informatie

Doelstelling: Het verschaffen van directieaansturing van en -steun voor overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

5.1.1	**1**	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsr te worden gedefinieerd, goedgekeurd door de directie, gepublicee gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten:

INFORMATIE BEVEILIGINGS DIENST

Lijnmanager (= procesverantwoordelijke)



INFORMATIE BEVEILIGINGS DIENST

Taken en bevoegdheden

- **Taken en bevoegdheden teammanager**

1.De teammanager wordt benoemd, geschorst en ontslagen door de gemeentesecretaris/algemeen directeur op voordracht van de directeur organisatie.

2.Teamleden worden benoemd, geschorst en ontslagen door de teammanager.

3.De teammanager is integraal resultaatverantwoordelijk leidinggevende voor zijn/haar team.

4.De teammanager heeft een adviserende taak richting de gemeentesecretaris/algemeen directeur en de directeur organisatie.

5.De teammanager is belast met en verantwoordelijk voor:

a. Het leidinggeven aan zijn/haar team

b. De inzet van de door de directie beschikbaar gestelde middelen (ten aanzien van personeel, informatie, organisatie, financiën, automatisering, communicatie en huisvesting) voor de realisatie van de doelen van het team en de organisatie.

g. Het opleiden, goed functioneren, coachen, motiveren en beoordelen van teamleden.

h. De prestaties/resultaten van het team.

j. Een adequate bedrijfsvoering binnen zijn/haar team.

k. Het goed laten verlopen van de P&C-cyclus.

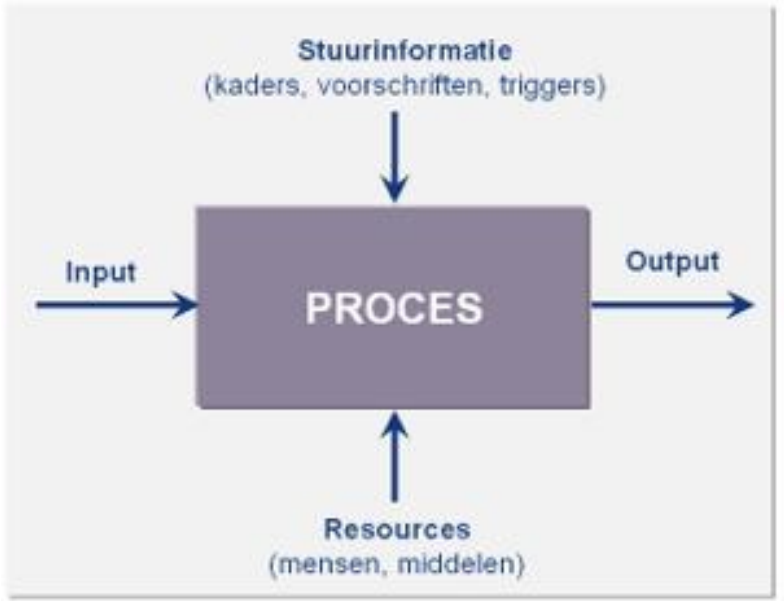
l. Het gezamenlijk behalen van de resultaten van de organisatie

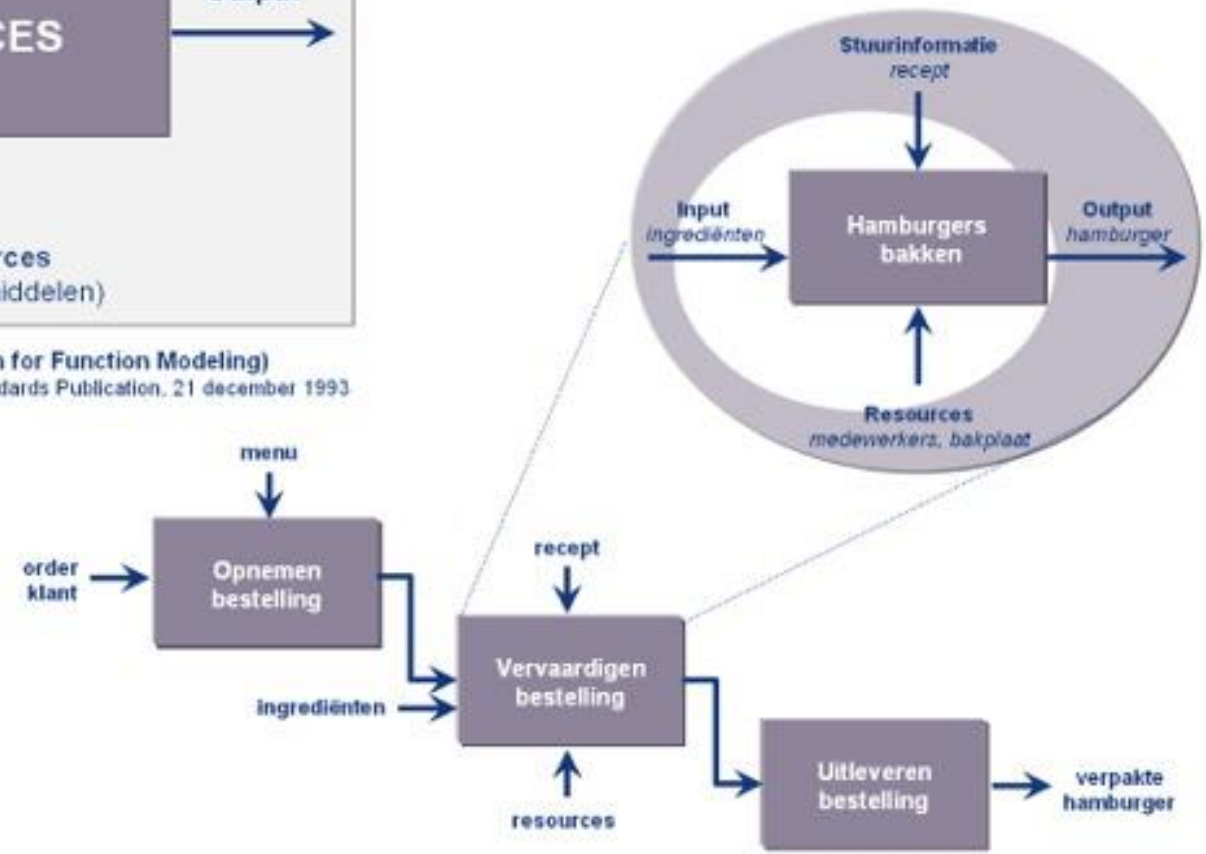
m. Het nemen van eigenaarschap en verantwoordelijkheid van teamleden.

INFORMATIE BEVEILIGINGS DIENST

Procesdefinitie

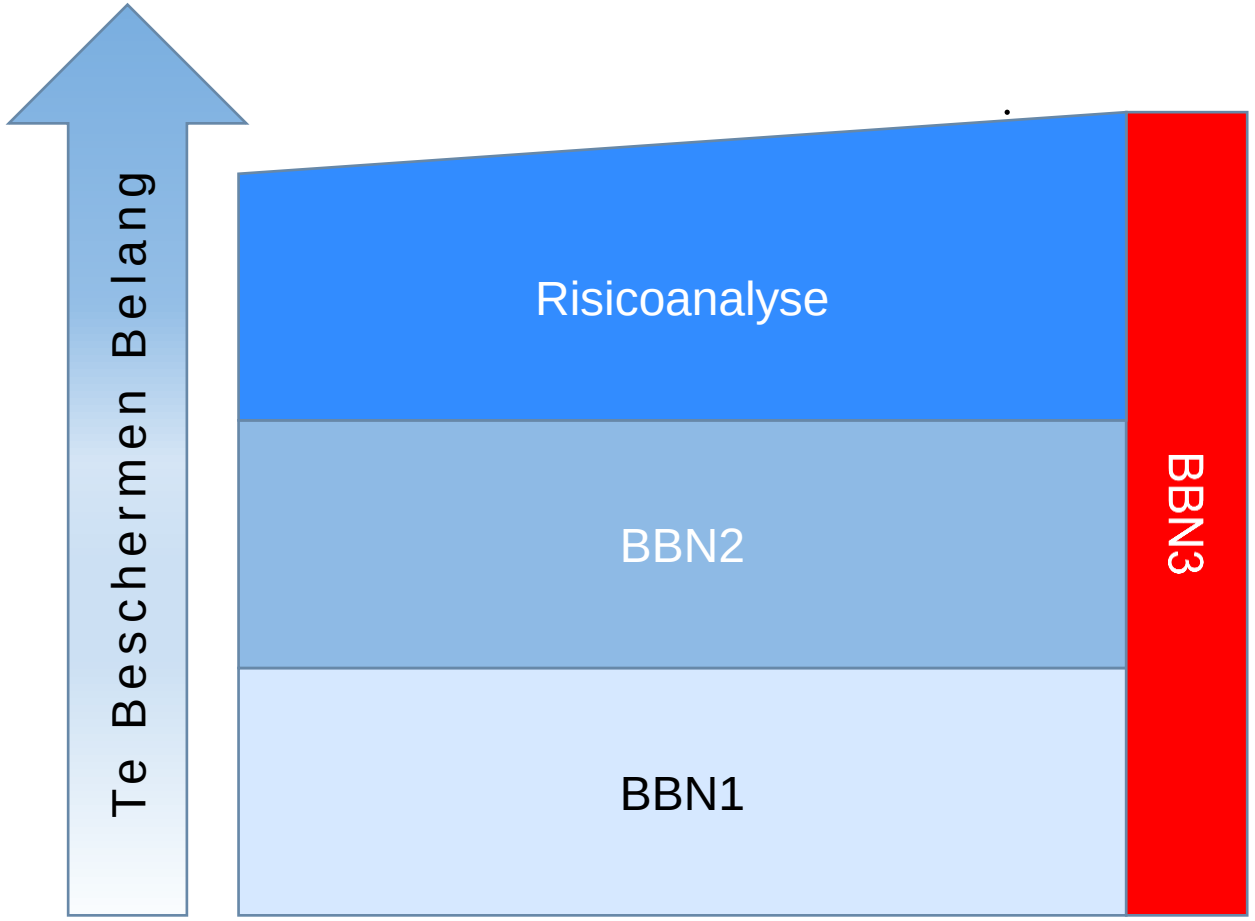
- Missie en Visie
- Organisatiedoelstellingen
- Hoofdprocessen
- Sub processen
- Procedures
- Activiteiten
- Taken
- Instructies





INFORMATIE BEVEILIGINGS DIENST

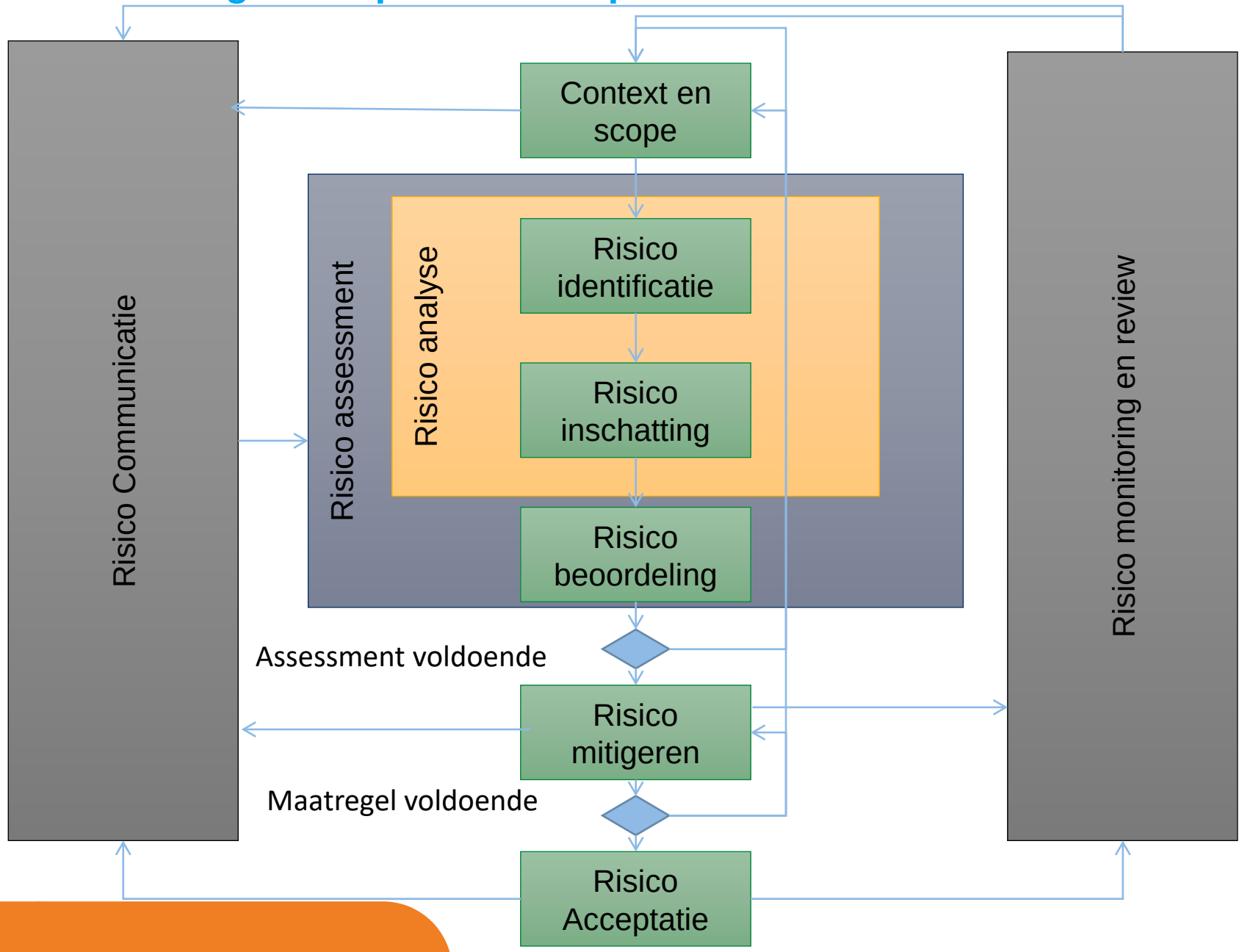
Te Beschermen Belang



Bescherming tegen statelijke of vergelijkbare actoren: Passief Actief

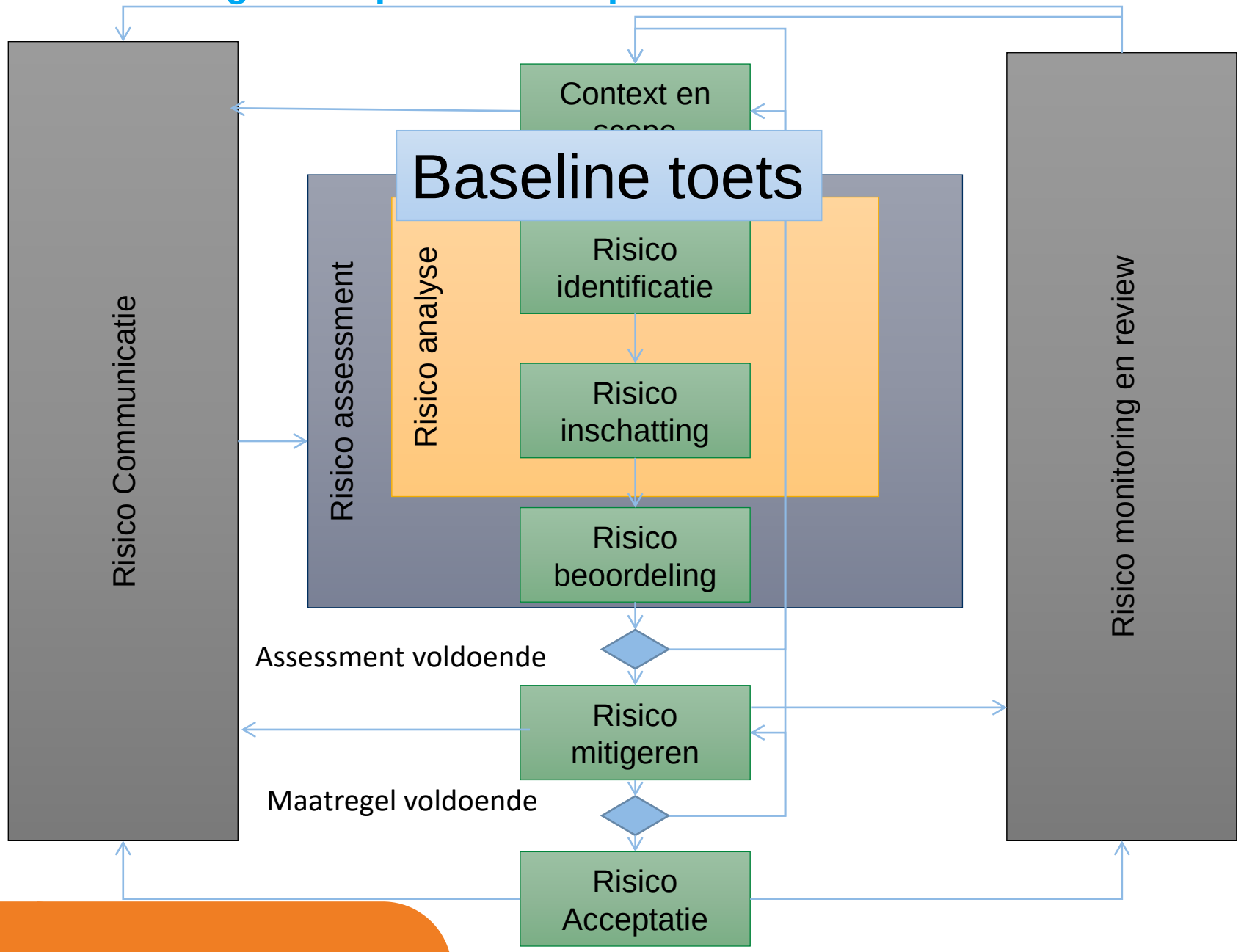
INFORMATIE BEVEILIGINGS DIENST

Risicomanagement proces ten opzichte van BIO



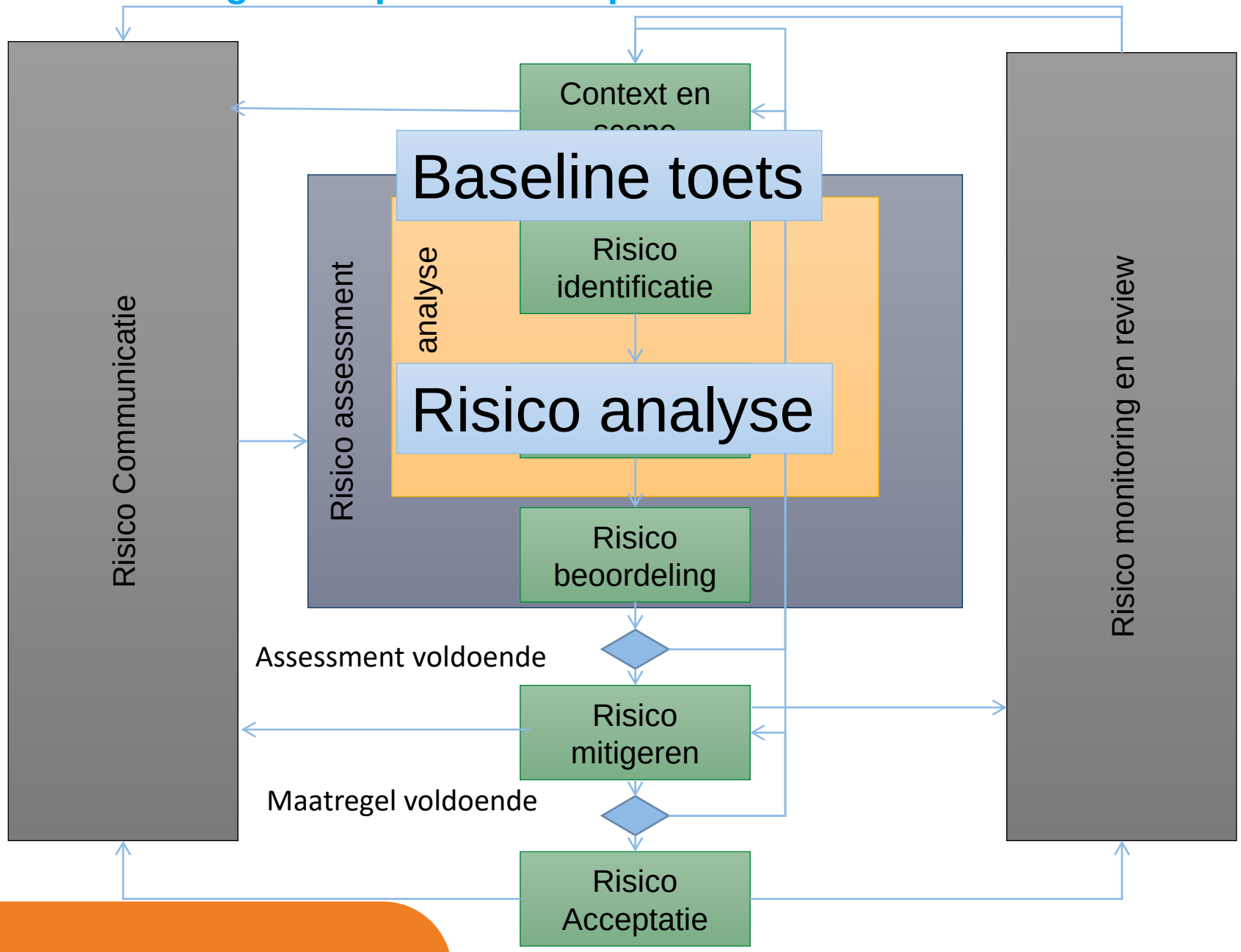
INFORMATIE BEVEILIGINGS DIENST

Risicomanagement proces ten opzichte van BIO



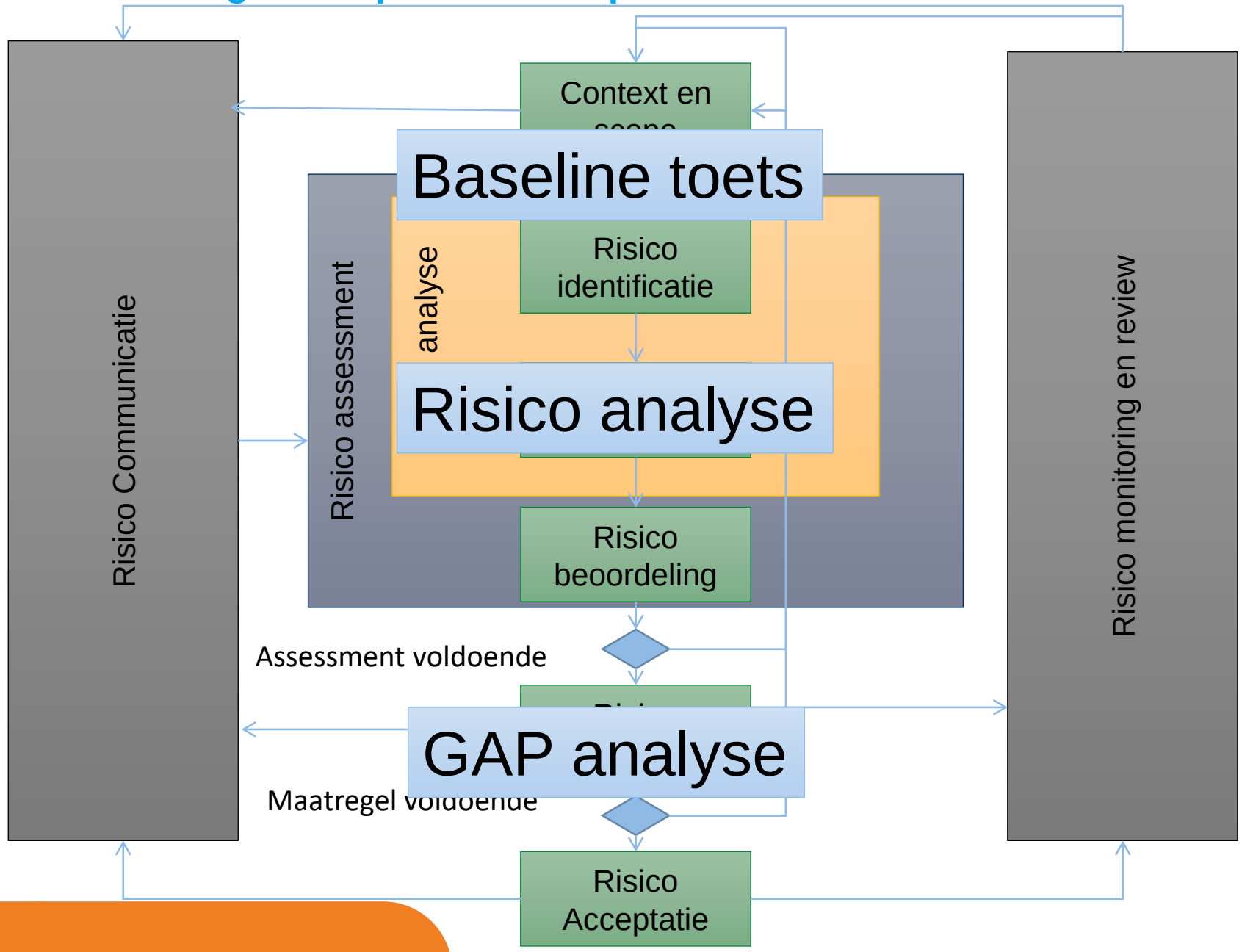
INFORMATIE BEVEILIGINGS DIENST

Risicomanagement proces ten opzichte van BIO



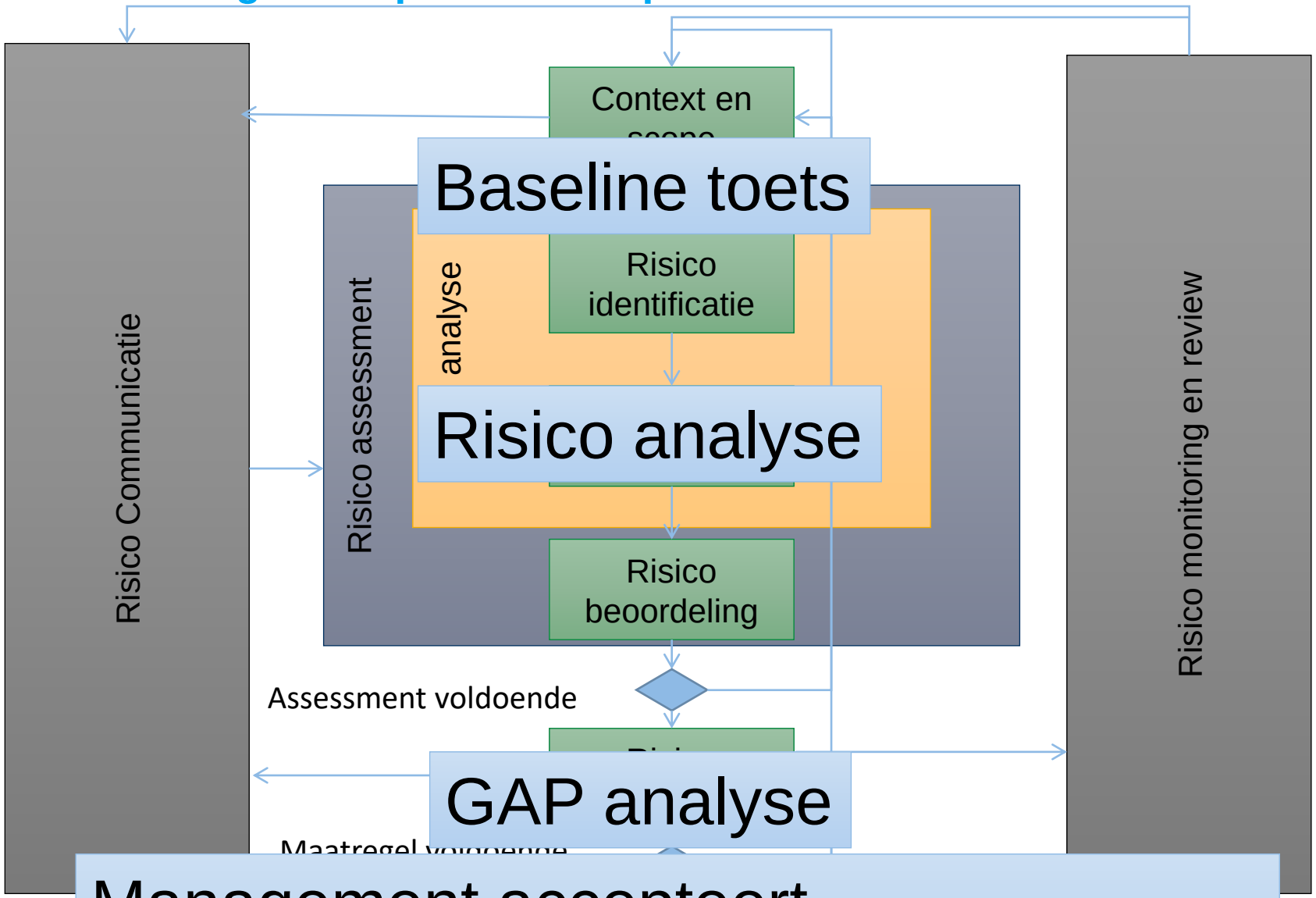
INFORMATIE BEVEILIGINGS DIENST

Risicomanagement proces ten opzichte van BIO



INFORMATIE BEVEILIGINGS DIENST

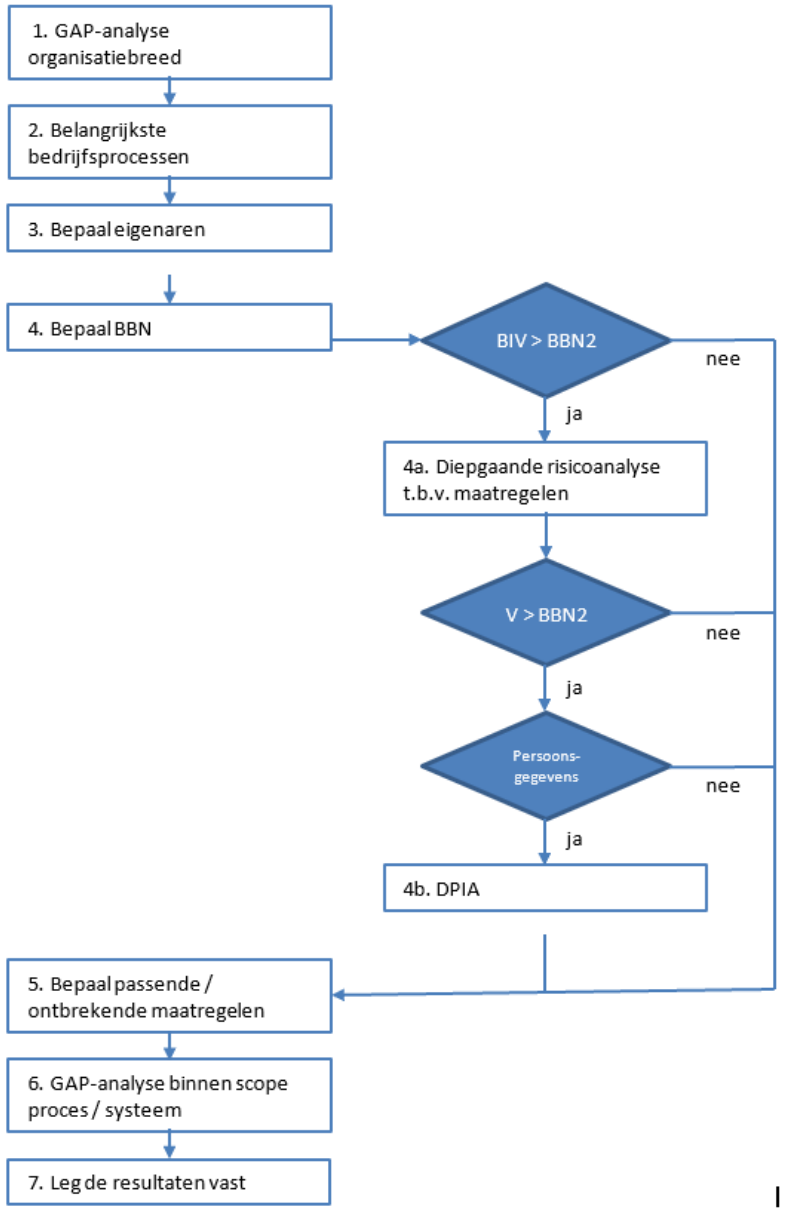
Risicomanagement proces ten opzichte van BIO



Management accepteert beveiligingsplan met restrisico

INFORMATIE BEVEILIGINGS DIENST

Pragmatische aanpak



INFORMATIE BEVEILIGINGS DIENST

Hulpmiddel van de IBD

Wat kun je ermee?

- BBN-classificatie bepalen per proces
- Met de uitkomst van de classificatie bepalen welke maatregelen genomen moeten/kunnen worden

Hoe bepaal je de BBN-classificatie? Drie mogelijkheden:

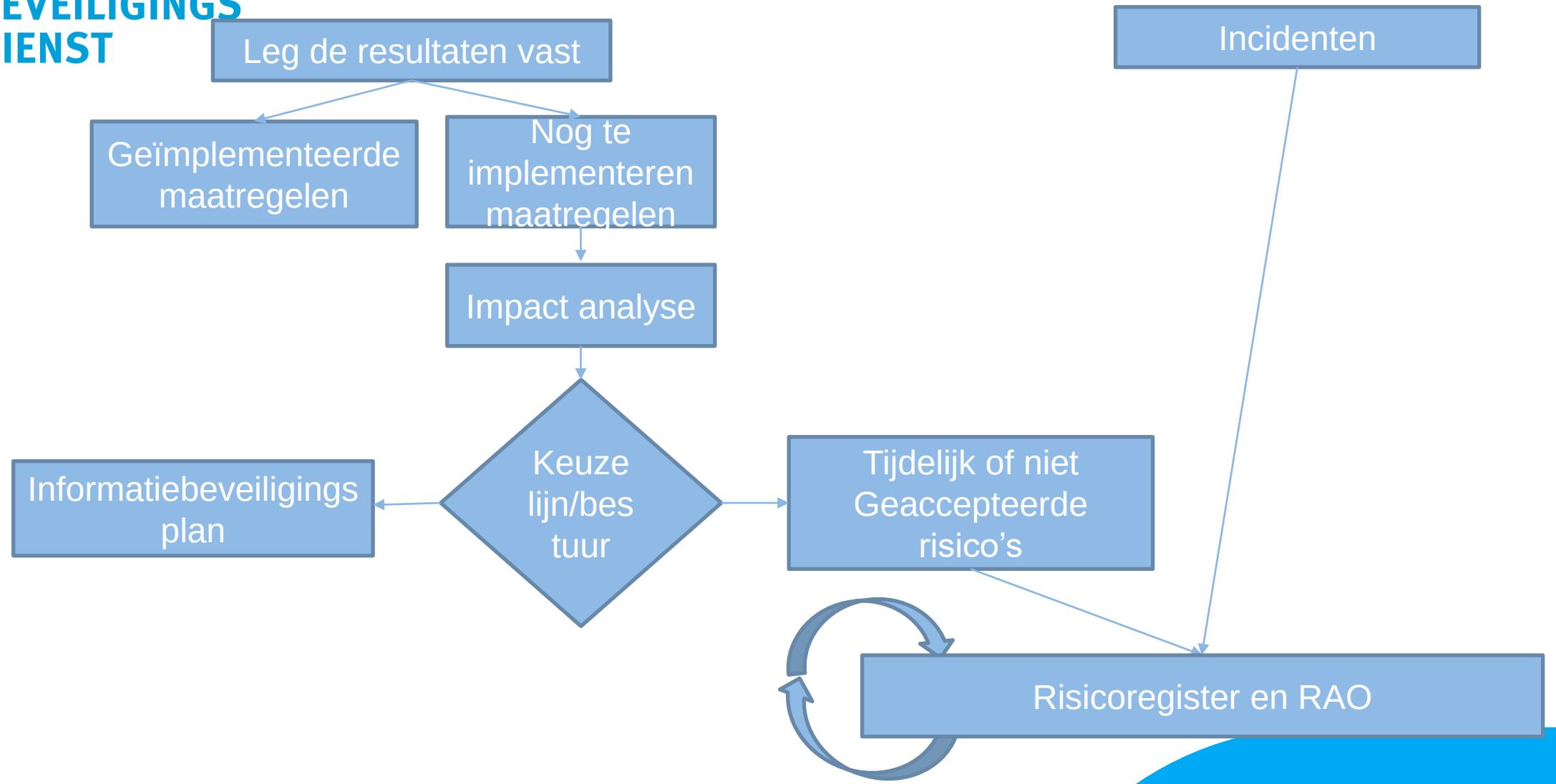
1. Beoordelen maximale schade voor organisatie en burger bij ongewenste gebeurtenissen (tab 2)
2. Classificatie ontlenen aan GEMMA-referentiecomponent (tab 4)

Praktisch alternatief:

3. Classificatie ontlenen aan verwerkingsregister

Risicoregister

INFORMATIE BEVEILIGINGS DIENST



INFORMATIE BEVEILIGINGS DIENST

Risico-register: hoe ziet het er uit?

ID	Uniek volgnummer
Datum	Datum van invullen
Risico	beschrijving van risico
Privacy gerelateerd?	J/N
Veroorzaakt door/bron	Waar komt het risico vandaan? BIO maatregel/ incident/ privacy impact/ datalek/ RD melding/ enz
Proces/applicatie	welk processen of welke processen en/of applicaties zijn geraakt?
Resultaat/ impact	Wat is de maximale schade/ geleden schade/
Kans (1-4)	kans schatting
Impact (1-4)	impact schatting
Risicolevel (kans * impact)	product van kans * impact, gebruikt voor prioritering
Control (link met de BIO)	Welke BIO controls / maatregelen indien van toepassing
Acties	Uitgezette acties, welke?
Tijdelijke maatregelen	Zijn er andere tijdelijke maatregelen genomen? Welke?
Kosten	Kosten inschatting voor mitigeren
Eigenaar	Wie is de eigenaar van het risico
Geaccepteerd?	Is het risico geaccepteerd
Planning (datum)	Datum risico gemitigeerd (planning)
Gerapporteerd (datum)	Meegenomen in de bestuurlijke rapportage op datum
Risicoacceptatie overeenkomst?	Is er een RAO gemaakt voor proceseigenaar?

INFORMATIE BEVEILIGINGS DIENST

Risico acceptatie overeenkomst

- Het komt voor dat proceseigenaren, het bestuur, de organisatie maatregelen niet willen implementeren. Dan blijft die maatregel, en dus ook het risico onbehandeld en is eigenlijk de CISO probleemeigenaar geworden.

- Om ervoor te zorgen dat de CISO het balletje terug kan spelen is het belangrijk dat hij een risicoacceptatie overeenkomst maakt. Hiermee legt hij vast dat iemand een risico niet accepteert of wil (nu) behandelen en daarmee beschermt de CISO zich dus eigenlijk als het toch fout gaat.
- **Let op: een manager kan geen risico accepteren als dit risico oplevert buiten zijn of haar proces**

- Voordelen: Probleem blijft waar het thuishoort en er is voor getekend
- Nadelen: geen

INFORMATIE BEVEILIGINGS DIENST

RAO indeling

Aan	**<verantwoordelijke voor systeem/eigenaar>**
Van	Naam, Security Officer/CISO
Afdeling	
CC	
Datum	
Onderwerp	Risico Acceptatie Overeenkomst: procesnaam/risiconaam
Applicatie	
Classificatie	
Privacy gerelateerd?	
BIO control	
Geldig tot	
Volgnummer	

Inleiding
Beschrijving Risico
Voorgestelde oplossingen
Advies
Verklaring ondergetekenden

INFORMATIE BEVEILIGINGS DIENST

RAO: Aanpak

1. Door het uitwerken van het risico kunnen de hoogste risico's het eerst geadresseerd worden!
2. Ga in discussie waarom het belangrijk is dat er gecommuniceerd wordt in risico's
3. Probeer risico's te linken aan BIO controls en maatregelen!
4. Vertaal risico's naar bedrijfsproblemen

INFORMATIE
BEVEILIGINGS
DIENST

vragen

INFORMATIE BEVEILIGINGS DIENST

Links naar documenten

https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

https://www.informatiebeveiligingsdienst.nl/product/handreiking-bio-voor-kleine-gemeenten/

https://www.informatiebeveiligingsdienst.nl/product/eenvoudig-hulpmiddel-voor-bepalen-maatregelen-bbn-en-schade-voor-betrokkenen/

https://www.informatiebeveiligingsdienst.nl/product/presentatie-regiobijeenkomst-informatiebeveiliging-najaar-2019-risicoregister-en-risicoacceptatieovereenkomst/

INFORMATIE
BEVEILIGINGS
DIENST

Nassaulaan 12
2514 JS Den Haag

CERT: 070 204 55 11(9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)

info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG
Realisatie