INFORMATIE
BEVEILIGINGS
DIENST

Bespreekuur praktische toepassing Risicomanagement (op basis van de Baselinetoets, Diepgaande Risicoanalyse)

24 september 2020

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

Privacyverklaring

De IBD stelt Zoom privacyvriendelijk in (privacy by default)

Tijdens de interactieve online bijeenkomsten maakt de IBD:

- gebruik van wachtwoorden om aan vergaderingen deel te nemen.
- gebruik van unieke vergader ID’s om vergaderingen af te schermen.
- geen gebruik van:
  “Cloud recording” en neemt de videoconferentie niet op.
  “local Recording”
  “automatically Transcribe Cloud Recordings”
  “attendee attention tracking”

INFORMATIE
BEVEILIGINGS
DIENST

Even voorstellen

- Frits Grotenhuis (IB adviseur IBD, moderator
- Kees Hintzbergen (senior IB adviseur IBD)
- John van Huijgevoort (senior IB en P adviseur IBD, notulist)

INFORMATIE BEVEILIGINGS DIENST

Doel van deze bijeenkomst

- Korte introductie in het onderwerp: Praktische toepassing Risicomanagement (op basis van de Baselinetoets, Diepgaande Risicoanalyse).
- Niet diepgaand – daarvoor is de groep te groot – maar vooral om uitleg te geven over wat Risicomanagement is in relatie tot de BIO.
- Vragen ophalen
- Discussie

INFORMATIE BEVEILIGINGS DIENST

Programma

- Doel van bijeenkomst
- Programma toelichten
- Even voorstellen aan elkaar
- Praktische toepassing Risicomanagement (op basis van de Baselinetoets, Diepgaande Risicoanalyse). Een korte presentatie, begripsvorming
- Gelegenheid voor vragen daarna afsluiten

INFORMATIE BEVEILIGINGS DIENST

Vragen vooraf

Wie heeft er ervaring met:

- Risicoanalyse
- Baselinetoets
- Diepgaande risicoanalyse

Wat zijn jullie ervaringen?

INFORMATIE BEVEILIGINGS DIENST

Wat is risicomanagement?

Risicomanagement is een middel om op een gestructureerde manier risico's in kaart te brengen, te evalueren en te beheersen:

1. Identificatie van risico's
2. Analyse en beoordeling van risico's > risicoanalyse
3. Analyse van huidige beheersmaatregelen > maatregelen
4. Ontwerpen en uitvoeren actieplannen > IB plan
5. Controleren, evalueren en rapporteren > eenvoudig GAP, audit, toolkit
6. Resultaten integreren in de bedrijfsvoering

INFORMATIE BEVEILIGINGS DIENST

Wat is risicomanagement?

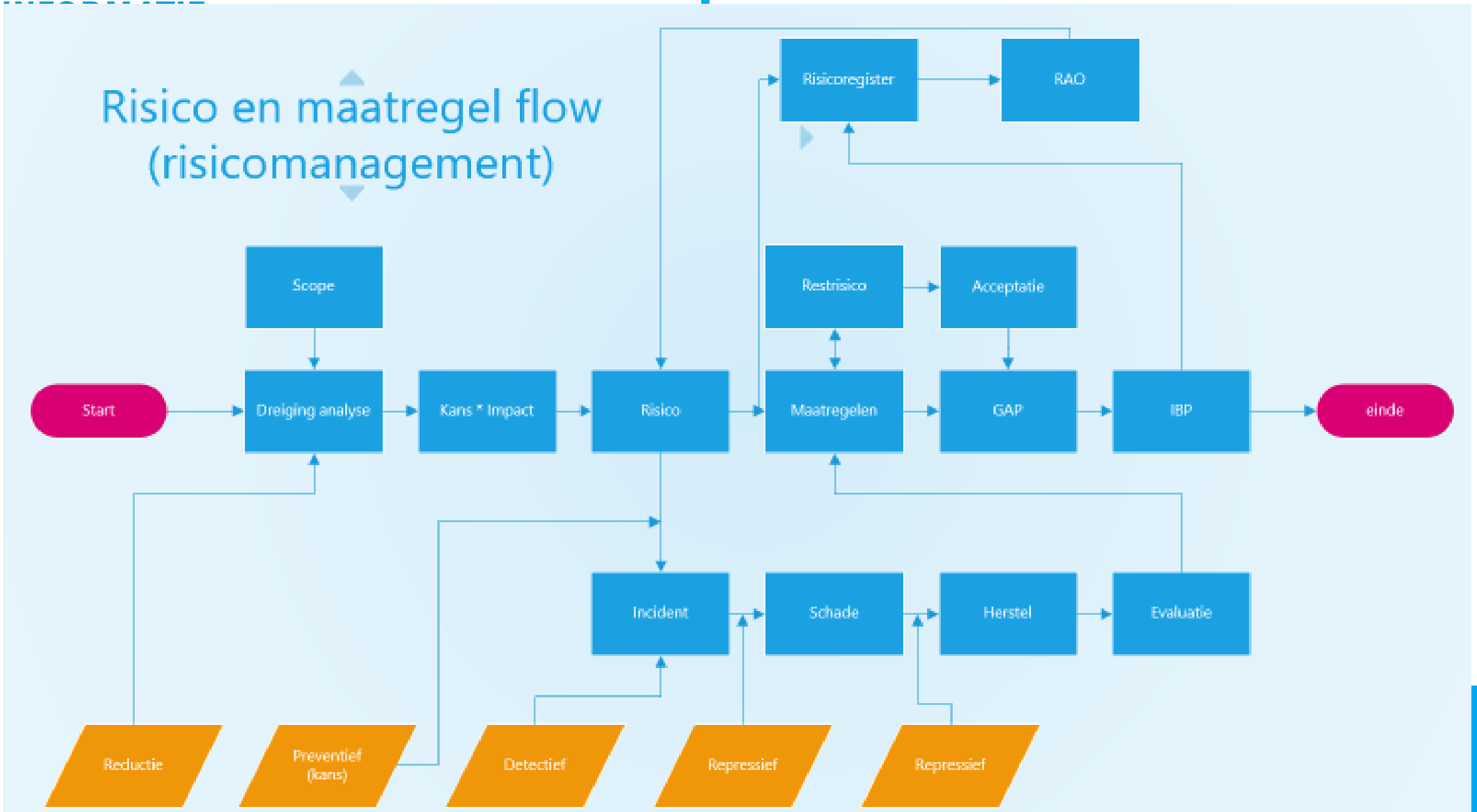
INFORMATIE BEVEILIGINGS DIENST

Wat is het verschil met de BIO

De BIO is een best practice verplichtende baseline met controls en maatregelen om de meest voorkomende risico's te beheersen langs de lijn van de ISO 27002:

1. De BIO bevat geen risico's
2. Maatregelen zijn ingevuld op basis van een dreiginganalyse
3. Waardering op basis van geleden schade (= resultaat incident)
4. Niveau bepaling op basis van baselinetoets

Context speelveld



INFORMATIE BEVEILIGINGS DIENST

Baselinetoets

Doel: bepalen benodigd beveiligingsniveau en vervolgstappen aan de hand van business impact (mini BIA)

Vier manieren/aanpakken:

1. Pagina 21 BIO (deel 2, BBN-toets) < meest eenvoudig
2. baselinetoets IBD < standaard aanpak
3. Baselinetoets Rijk < meest complex
4. Eenvoudig hulpmiddel (eenvoudige baselinetoets, gebaseerd op 2) < meest eenvoudig, meest praktisch

INFORMATIE BEVEILIGINGS DIENST

Diepgaande Risicoanalyse

- Doel: gestructureerd en methodisch onderzoek naar risico's en definiëren van maatregelen om de risico's te beheersen.
- Voordelen: gestructureerd, aantoonbaar, herleidbaar, diepgaand, methodisch risico's vinden, en passende maatregelen selecteren, bewustzijn verhogend effect
- Nadelen: legio
  - Wordt bijna nooit goed uitgevoerd
  - Wordt bijna nooit uitgevoerd
  - Bij gelijkblijvende organisaties niet altijd gelijke risico's en bijna nooit gelijke maatregelen
  - Veel werk, tijdrovend
  - Duur in doorloop en interne resources
  - Specialistische kennis nodig
  - Veel processen
  - Schijn nauwkeurigheid door missen risico's

- DUS!! Alleen gebruiken indien noodzakelijk!

INFORMATIE BEVEILIGINGS DIENST

Praktisch, hoe dan?

Eigenschappen gemeenten:

- We hebben er 355 plus nog heel veel aanverwante organisaties
- We doen allemaal hetzelfde, zelfde processen, vergelijkbare besturing
- Zwaartepunt ligt op maximaal automatiseren om met minimale mensen passende wettelijk voorgeschreven producten en diensten te leveren

Dus:

- Standaardiseren
- Centrale aanpak, centrale risicoanalyse
- Zwaartepunt: maatregelen best practice, clustering processen op afdeling en BBN
- Delen

INFORMATIE BEVEILIGINGS DIENST

Hoe dan?

Wat zijn jullie ervaringen of aanpak?

DISCUSSIE

INFORMATIE BEVEILIGINGS DIENST

Samenvatting

Eenvoudige aanpak

TOP 10 (dreigingen, processen, risico’s)

IRPA!

Clustering

GAP-O en GAP-P

Voorbeeld maatregelen

Alleen BIO maatregelen zijn verplicht!

Delen!

INFORMATIE BEVEILIGINGS DIENST

Handige links

- https://www.informatiebeveiligingsdienst.nl/product/handreiking-risicomanagement-door-lijnmanagers/
- https://www.informatiebeveiligingsdienst.nl/product/handreiking-bio-voor-kleine-gemeenten/
- https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/
- https://www.informatiebeveiligingsdienst.nl/product/introductie-aanpak-bio/
- https://www.informatiebeveiligingsdienst.nl/nieuws/implementatie-van-de-bio-hoe-pakken-gemeenten-dat-aan/
- https://www.informatiebeveiligingsdienst.nl/blog/ontneem-managers-hun-verantwoordelijkheid-niet/
- https://www.informatiebeveiligingsdienst.nl/product/handreiking-risicoregister-en-risico-acceptatie-overeenkomst-rao/
- https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-processen/
- https://www.informatiebeveiligingsdienst.nl/product/eenvoudig-hulpmiddel-voor-bepalen-maatregelen-bbn-en-schade-voor-betrokkenen/

INFORMATIE
BEVEILIGINGS
DIENST

Vragen?