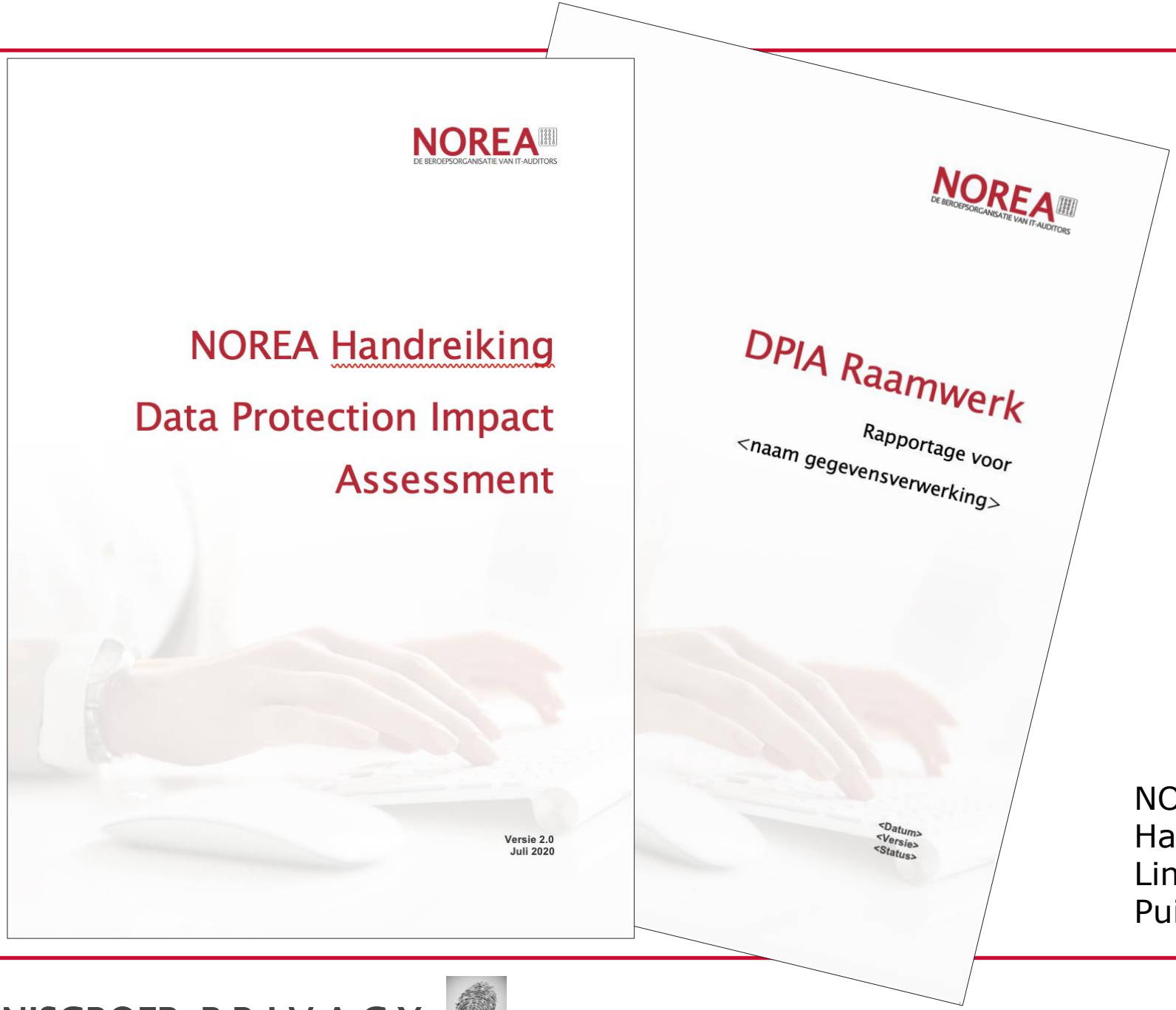


NOREA-werkgroep DPIA:
Han Boer, Jan de Heer, Henk van der Linde, Winfried Nanninga, Jeroen van Puijenbroek en Ed Ridderbeekx

NOREA WEBINAR DPIA 2.0

- Blok 0. Opening
- Blok 1. Inleiding
- Blok 2. Opbouw en Structuur Handreiking/Raamwerk
- Blok 3. Risicobeoordeling met BowTie
- Blok 4. Afsluiting

NOREA WEBINAR DPIA 2.0

- Graag je microfoon op *mute* tijdens de presentatie
- Stel eventuele vragen in de chat
- Aan het einde zullen we die (zoveel mogelijk) behandelen
- Dit webinar is goed voor 1 PE punt
- Presentatie komt naderhand beschikbaar via NOREA website (link wordt gestuurd)

- Sprekers namens de Werkgroep DPIA:

  Henk van der Linde en Jeroen van Puijenbroek

NOREA WEBINAR DPIA 2.0

- Blok 0. Opening
- Blok 1. Inleiding
- Blok 2. Opbouw en Structuur Handreiking/Raamwerk
- Blok 3. Risicobeoordeling met BowTie
- Blok 4. Afsluiting

NOREA WEBINAR DPIA 2.0

Waarom een nieuwe versie

1. Verouderde NOREA PIA 1.2 (2015 – gebaseerd op Wbp)
2. Voldeed niet meer aan de vereisten van de AVG en het Richtsnoer van de European Data Protection Board (EDPB) inzake DPIA's
3. Vragenlijst was te uitgebreid
4. Risico–analyse was een "black–box"
5. Geen samenhang met NOREA Privacy Control Framework

Ongewijzigd (versie 1.2 en 2.0)

1. Doelgroep: opdrachtgevers en opdrachtnemers van DPIA's (IT–auditor als adviseur)
2. Handreiking is geen normenkader voor het beoordelen van uitgevoerde DPIA's

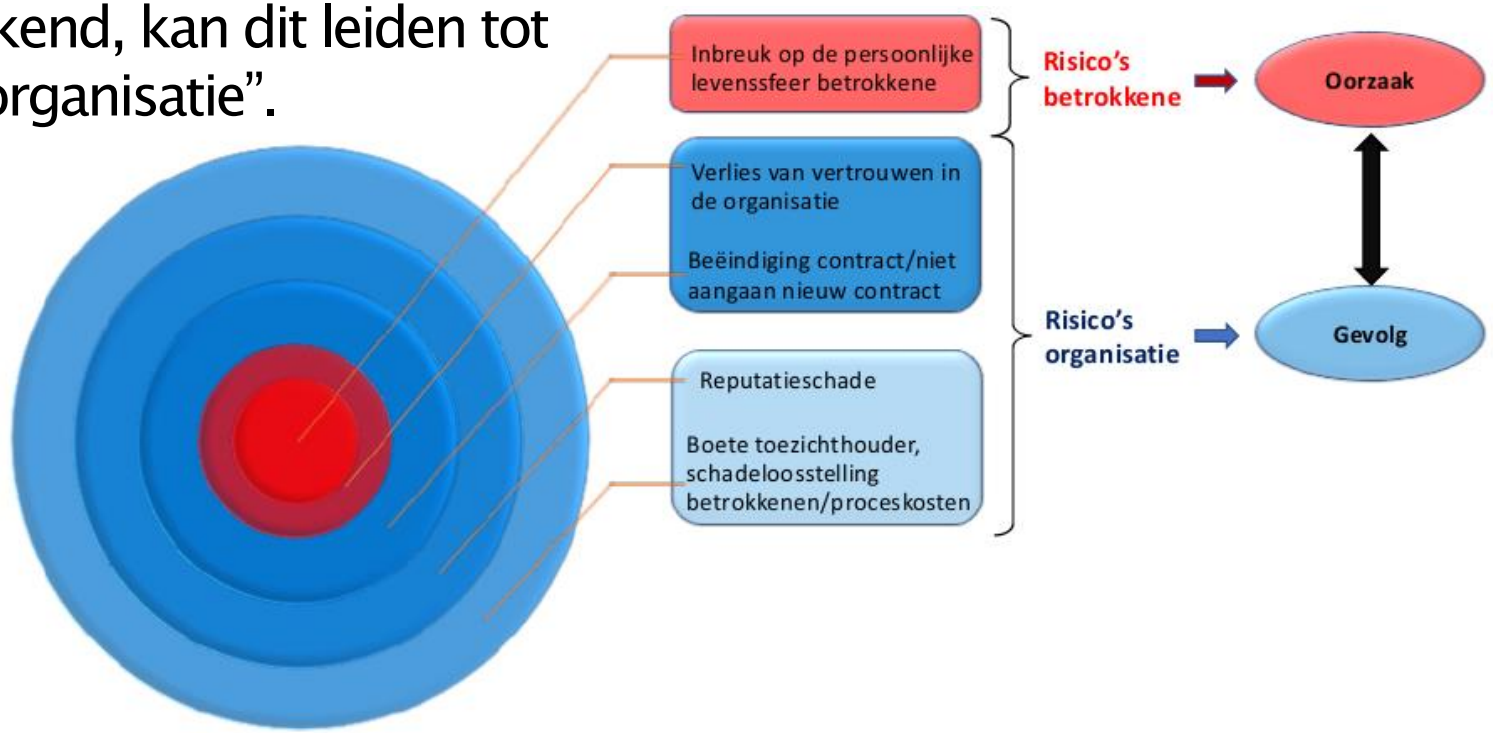
DPIA – Wat is het?

- “Een instrument om vooraf de privacyrisico’s van een verwerking van persoonsgegevens in kaart te brengen, en om daarna maatregelen te kunnen nemen om de risico’s te verkleinen.” (AP);
- “Een goed uitgevoerde DPIA geeft inzicht in de risico’s die de verwerking oplevert voor de betrokkenen, en in de maatregelen die de verantwoordelijke moet nemen om de risico’s af te dekken.” (AP);
- Artikel 35 (7) AVG.

I. Beschrijving gegevensverwerking	II. Beoordeling rechtmatigheid	III. Risicobeoordeling en -behandeling

Risico's van de gegevensverwerking:

1. AVG (art. 35): "risico's voor de rechten en vrijheden van natuurlijke personen";
2. Indien risico niet wordt onderkend, kan dit leiden tot "negatieve gevolgen voor de organisatie".



Wat is het doel van een DPIA

1. Het in een vroeg stadium vinden van privacyrisico's;
2. Voorkoming vertraging of zelfs stopzetting ontwikkelingen, dus ongewenste hoge kosten;
3. Resultaat van DPIA gebaseerd op of juist input voor Privacy by Design & by Default;
4. Biedt management betere onderbouwing voor 'risk appetite';
5. Verhogen van privacybewustzijn binnen de organisatie;
6. Door transparantie verkrijgen maatschappelijk vertrouwen;
7. Aantoonbaar aan de AVG–verplichtingen voldoen.

DPIA niet altijd verplicht maar verstandige keuze in privacybeleid door management.

NOREA WEBINAR DPIA 2.0

- Blok 0. Opening
- Blok 1. Inleiding
- Blok 2. Opbouw en Structuur Handreiking/Raamwerk
- Blok 3. Risicobeoordeling met BowTie
- Blok 4. Afsluiting

NOREA WEBINAR DPIA 2.0

Twee producten:

1. NOREA Handreiking DPIA
   - Introductie en proces (wat, waarom, wanneer, wie, …)
   - Toelichting op de vragen uit het DPIA Raamwerk
   - Bijlagen (o.a. criteria verplichte DPIA en voorbeelden risicobeoordeling)
2. NOREA DPIA Raamwerk
   - De te beantwoorden vragen in de DPIA…
   - …die na beantwoording leiden tot de DPIA–rapportage

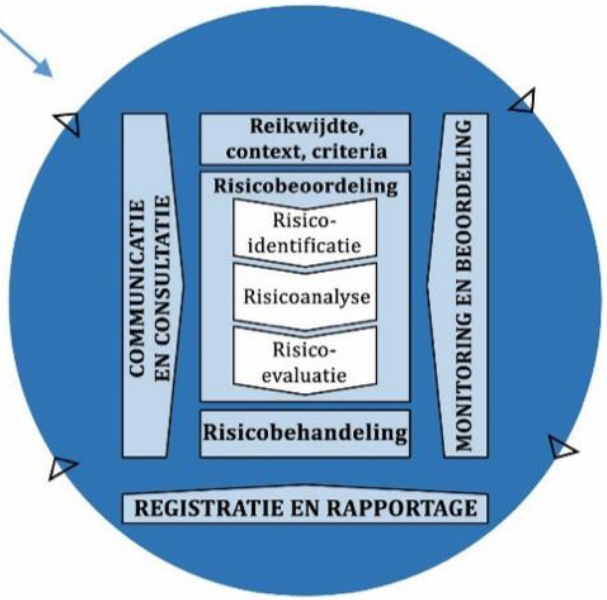
NOREA WEBINAR DPIA 2.0

ISO 31000: Risicomanagement

1. Wereldwijde standaard
2. Inbedding van risicomanagement in de organisatie
3. PDCA-cyclus

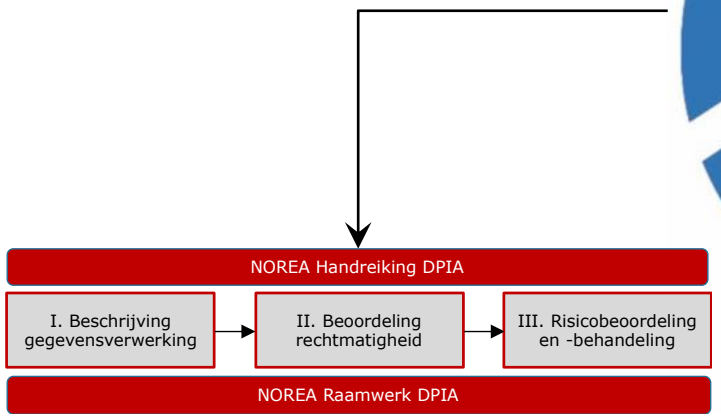
Principes

Raamwerk



Proces

Bron: NEN-ISO31000:2018 Risicomanagement - Richtlijnen



NOREA WEBINAR DPIA 2.0

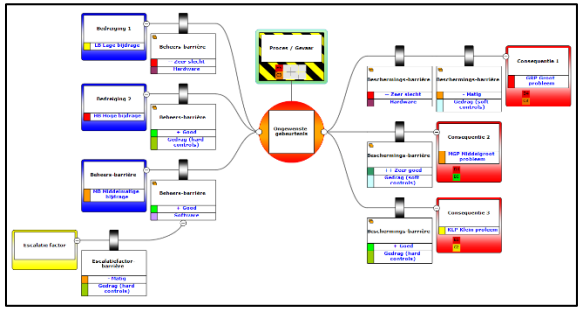
Structuur

Handreiking DPIA

I. Beschrijving gegevensverwerking	II. Beoordeling rechtmatigheid	III. Risicobeoordeling en -behandeling

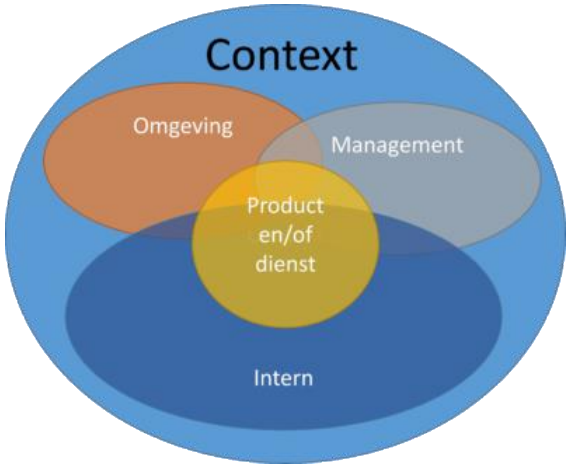
Raamwerk DPIA

Structuur volgens informatielevenscyclus uit Privacy Control Framework	- Grondslag - Noodzaak en evenredigheid - Rechten van betrokkenen	Proces conform ISO 31000; Risicobeoordeling uitgewerkt o.b.v. BowTie (ISO31010)



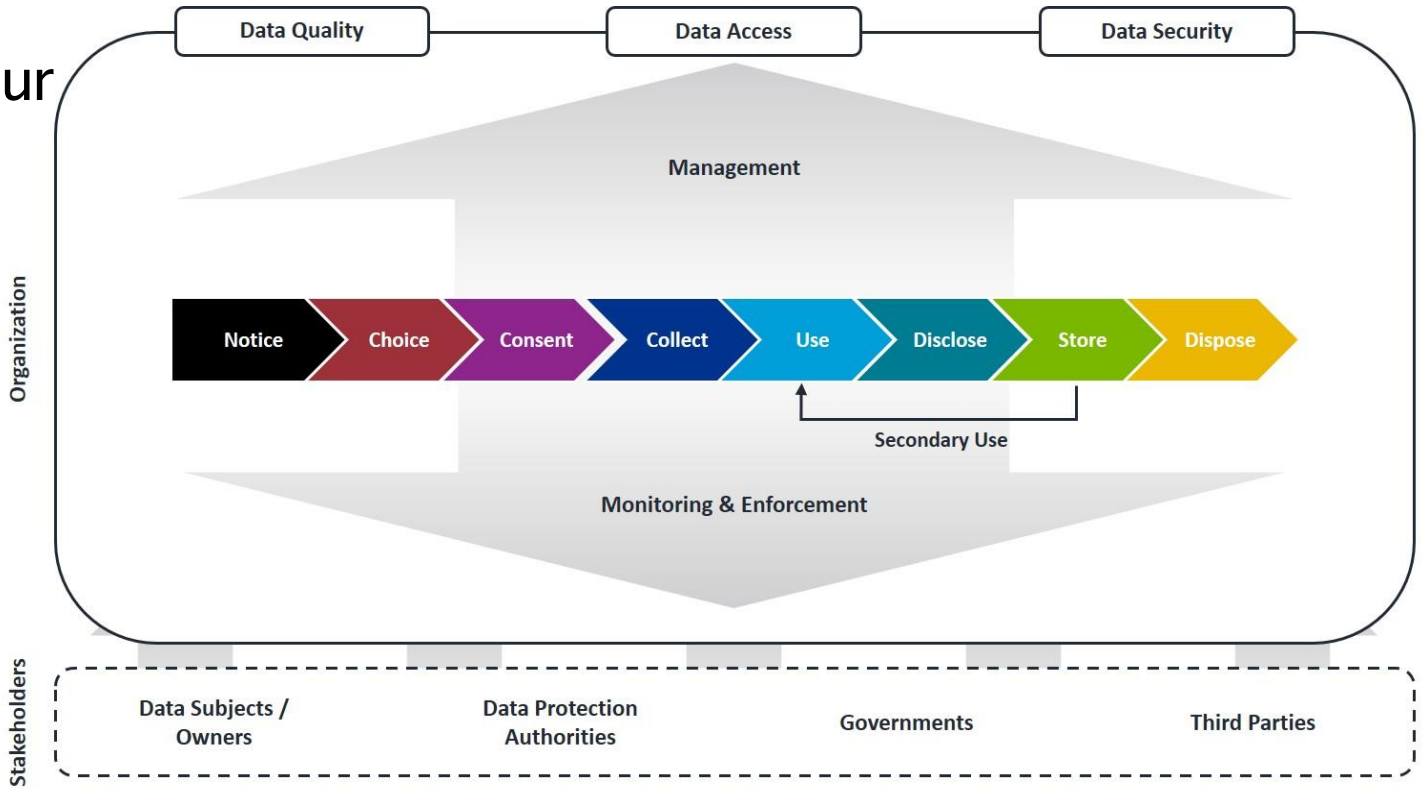
Raamwerk

1. **Beschrijving gegevensverwerking**
   - **Contextanalyse DPIA:**
     - Beschrijving hoofdlijnen project / systeem / applicatie;
     - Doelen van en eisen aan project / systeem / applicatie;
     - Beschrijf relevante bedrijfsprocessen en gegevensstromen;
     - Gerelateerde IT-systemen en/of interfaces naar andere platforms
     - Beschrijf van toepassing zijn de wetgeving(en);



Raamwerk: 1. Beschrijving gegevensverwerking (vervolg)

- **Informatielevenscyclus:**
  - Als ondersteuning en structuur bij de beschrijving van de verwerking;
  - Zie ook PCF 2.0



I. Beschrijving gegevensverwerking

Raamwerk: 2. Rechtmatigheidsbeoordeling

- Grondslag:
  - Toestemming
  - Overeenkomst
  - Wettelijke verplichting
  - Vitaal belang
  - Taak algemeen belang
  - Gerechtvaardigd belang
- Noodzaak en evenredigheid
- Uitoefening rechten betrokkene

Zorg
Wabvpz
WGBO

Financieel
Wft
Pensioen
Wwft

Gemeenten
Jeugdwet
WMO
Schuldhulp

Handhaving
Wpg
Ondermijning

lex specialis derogat legi generali

Indien 'Wettelijke Verplichting' of 'Taak Algemeen Belang':

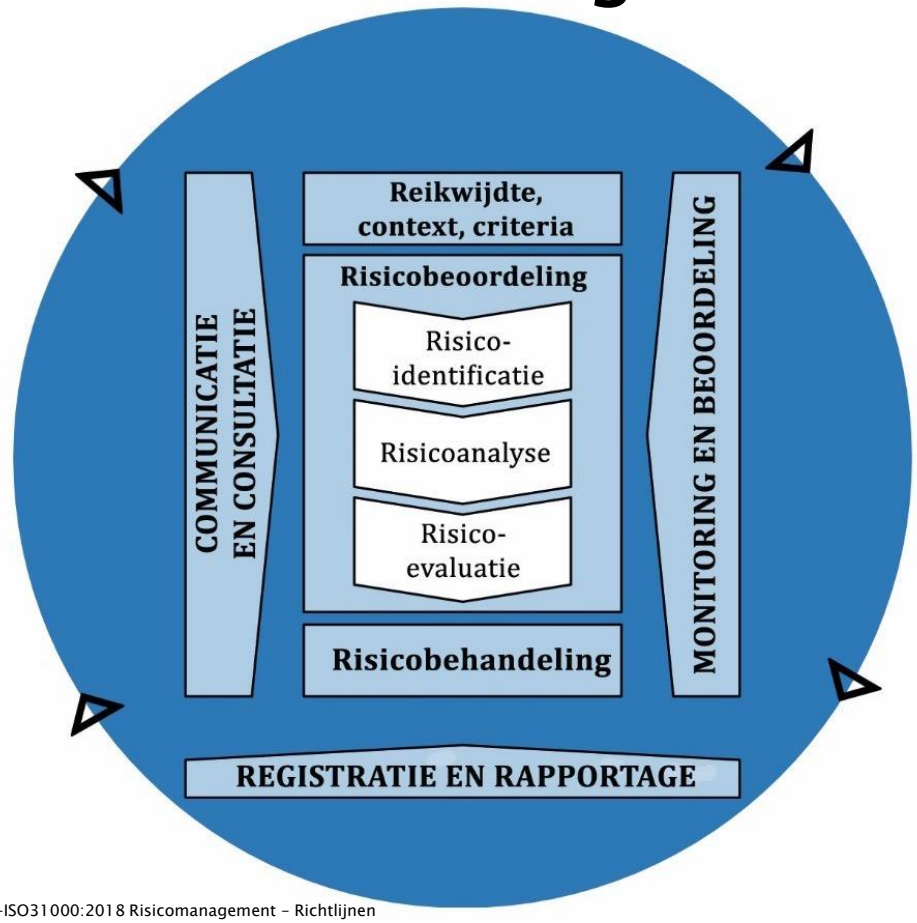
- "Lex specialis versus lex generalis", wet stelt Sectorale wetgeving boven Algemene wetgeving;
- Let ook op specifieke Sectorale standaarden.

Raamwerk: 3. Risicobeoordeling en –behandeling

NOREA WEBINAR DPIA 2.0

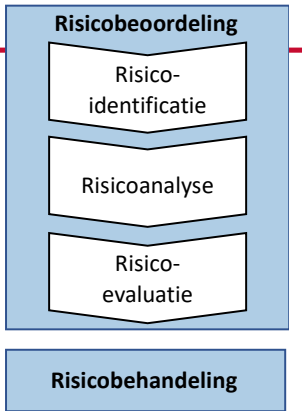
- Blok 0. Opening
- Blok 1. Inleiding
- Blok 2. Opbouw en Structuur Handreiking/Raamwerk
- Blok 3. Risicobeoordeling en behandeling met BowTie
- Blok 4. Afsluiting

Risicicobeoordeling en –behandeling



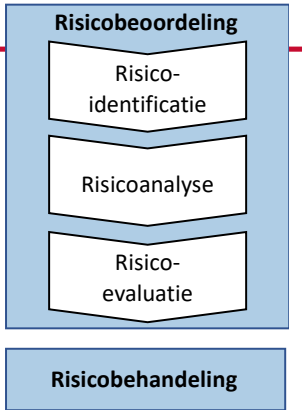
Bron: NEN-ISO31000:2018 Risicomanagement - Richtlijnen

- Handvatten opgenomen voor het uitvoeren ervan
- Het staat het DPIA-team vrij om een bepaalde techniek te kiezen voor de risicobeoordeling
- In ISO31010 zijn diverse technieken opgenomen
- Uitwerking opgenomen op basis van BowTie-techniek
  - Krachtig instrument om expliciet de negatieve gevolgen van risico's te analyseren en in kaart te brengen
  - Betere maatregelen getroffen
  - Visualisatie bewerkstelligt groter draagvlak bij stakeholders



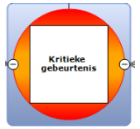
Uitwerking BowTie methode a.d.h.v. voorbeeld

- Gegevensverwerking t.b.v. wagenparkbeheer
  - Wagenparkbeheer wil een applicatie inzetten voor de volgende doeleinden:
    - Fiscaal sluitende ritregistratie (personenauto's)
    - Real–time track en trace (bestelauto's ten behoeve bezorgdienst)
    - Vergroening (stimuleren rijgedrag leaserijders)
    - Vloot en wagenparkbeheer
    - Managementinformatie



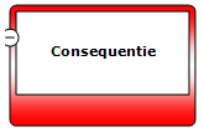
BowTie methode – Begrippen:

Risicobron/Gevaar (Proces)



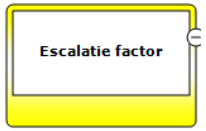
Kritieke gebeurtenis

Bedreigingen (Oorzaken)

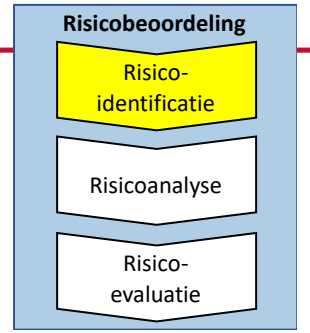


Consequenties (Negatieve gevolgen)

Barrieres (Maatregelen: beheers/herstel)



Escalatie factor

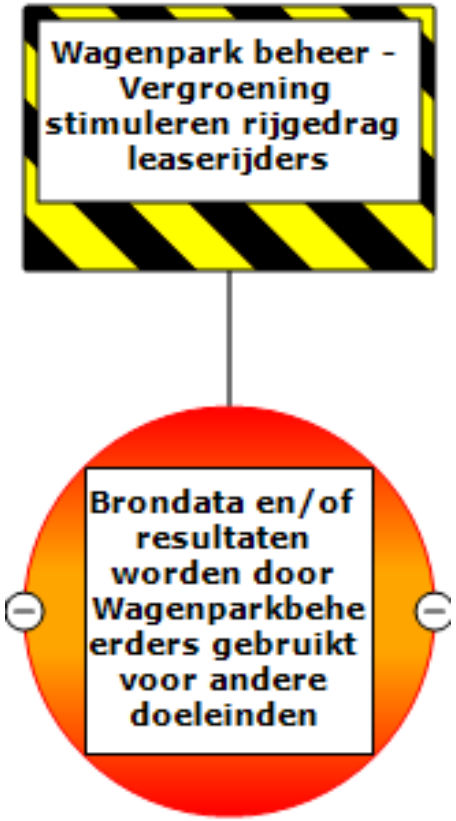


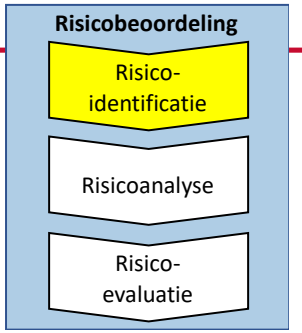
Risicobeoordeling: Risico–identificatie

1. Stel de Risicobron/Gevaar (Proces) vast
2. Stel de Kritieke gebeurtenis per Risicobron vast

Voorbeelden Kriteke gebeurtenissen o.b.v. beheersdoelstellingen PCF:

- Persoonsgegevens zijn niet toereikend, ter zake dienend of te beperkt;
- Persoonsgegevens zijn niet juist en/of volledig;
- Persoonsgegevens worden verwerkt voor andere doeleinden dan wel verstrekt aan andere derden dan die zijn geformuleerd;
- Betrokkenen kunnen hun rechten niet/niet volledig uitoefenen;
- Er vindt ongeautoriseerde toegang, verstrekking of inbreuk plaats van persoonsgegevens;
- Er vindt onopzettelijke of ongeautoriseerde wijziging van persoonsgegevens plaats;
- Er vindt onopzettelijke verlies of ongeautoriseerde verwijdering van persoonsgegevens plaats.



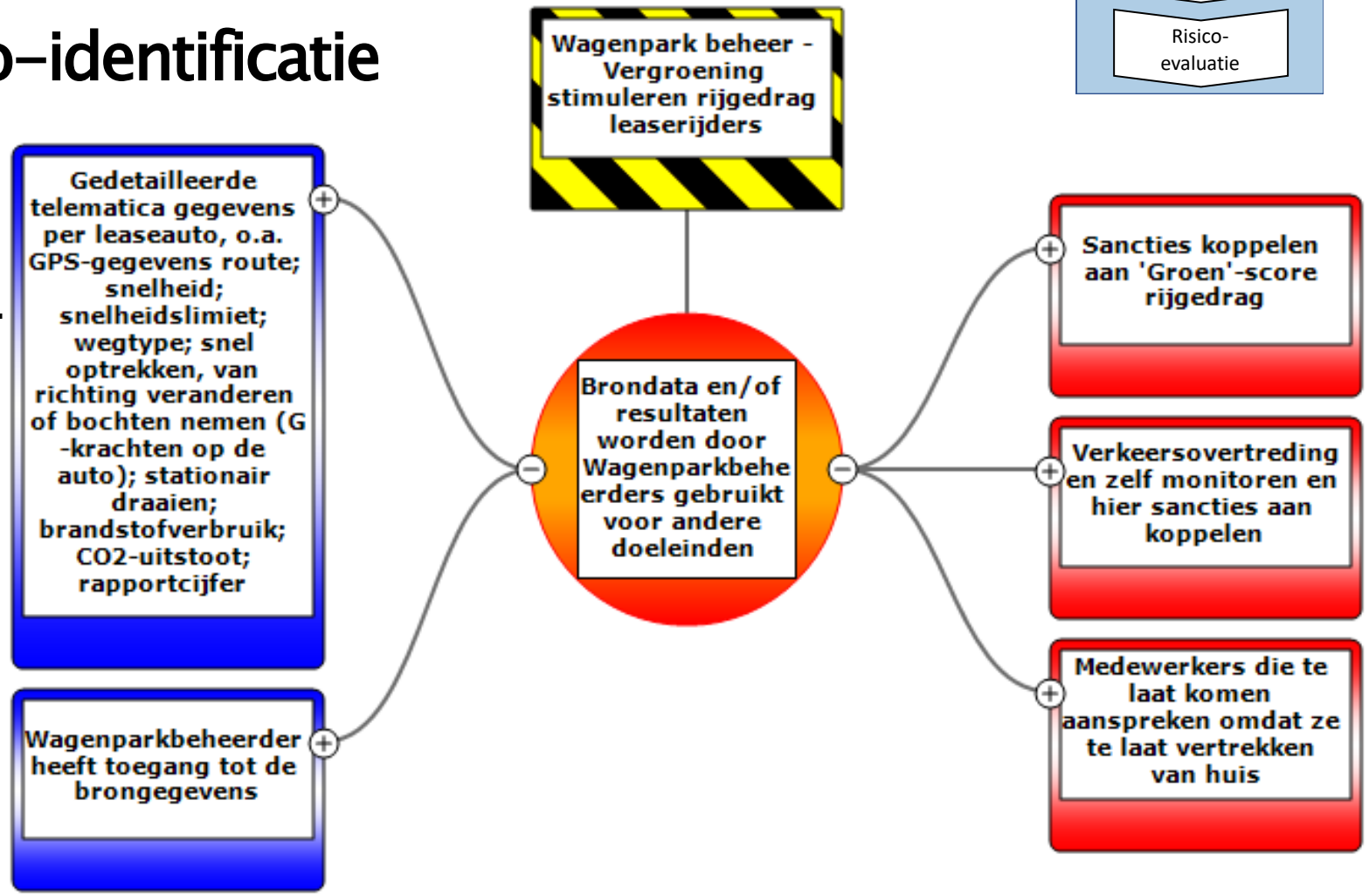


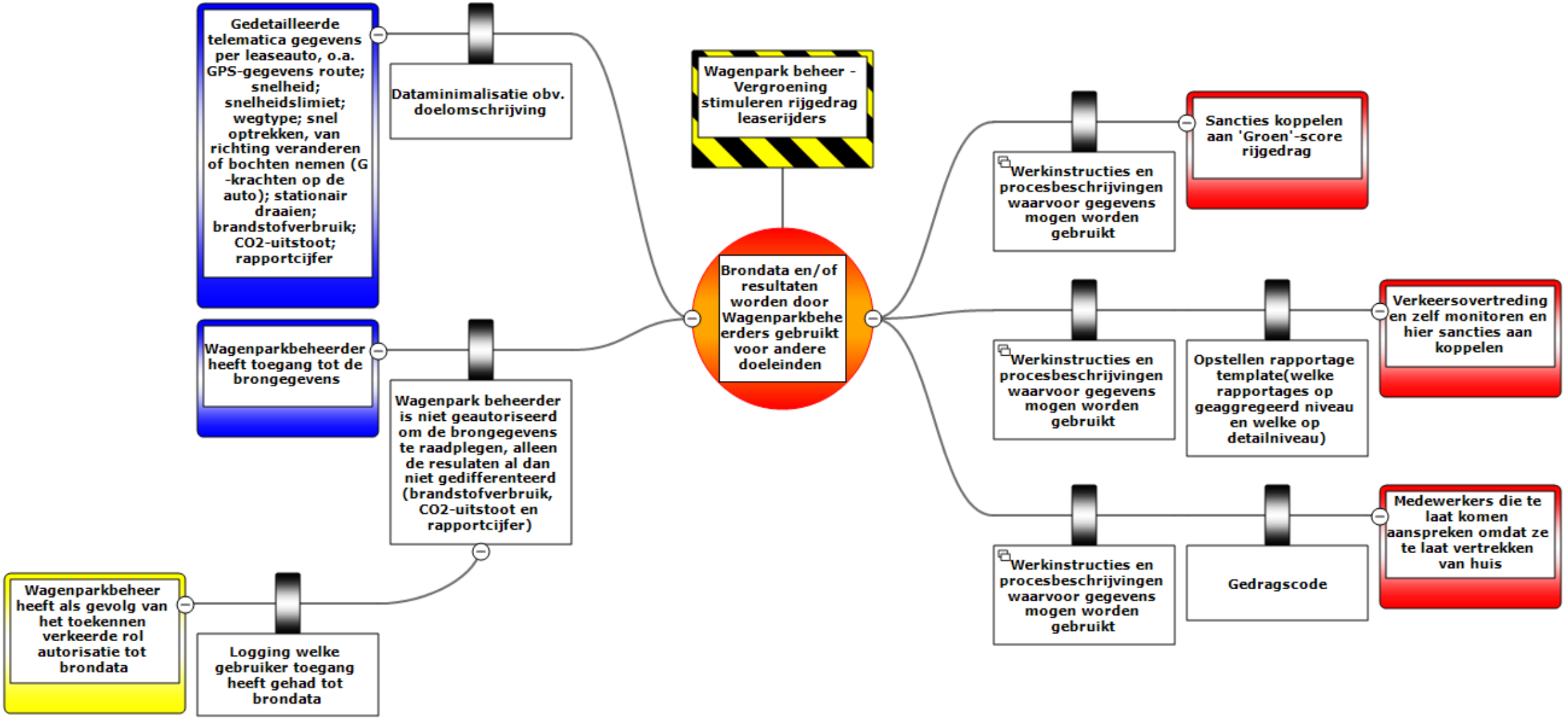
Risicobeoordeling: Risico–identificatie

3. Stel een initiële BowTie op

Per Risicobron/Kritieke gebeurtenis wordt een aparte BowTie opgesteld.

- Bedreigingen (Oorzaken);
- Consequenties (Gevolgen);
- Barrières (Maatregelen);
- Escalatie factoren



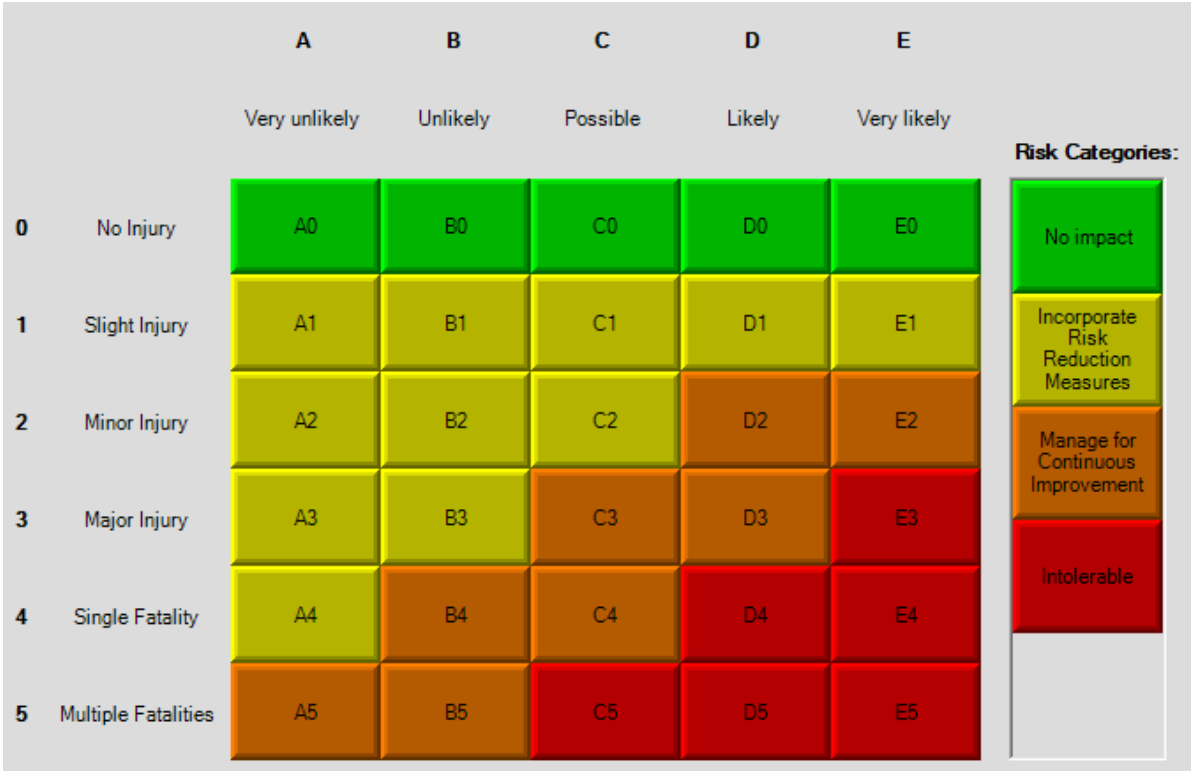


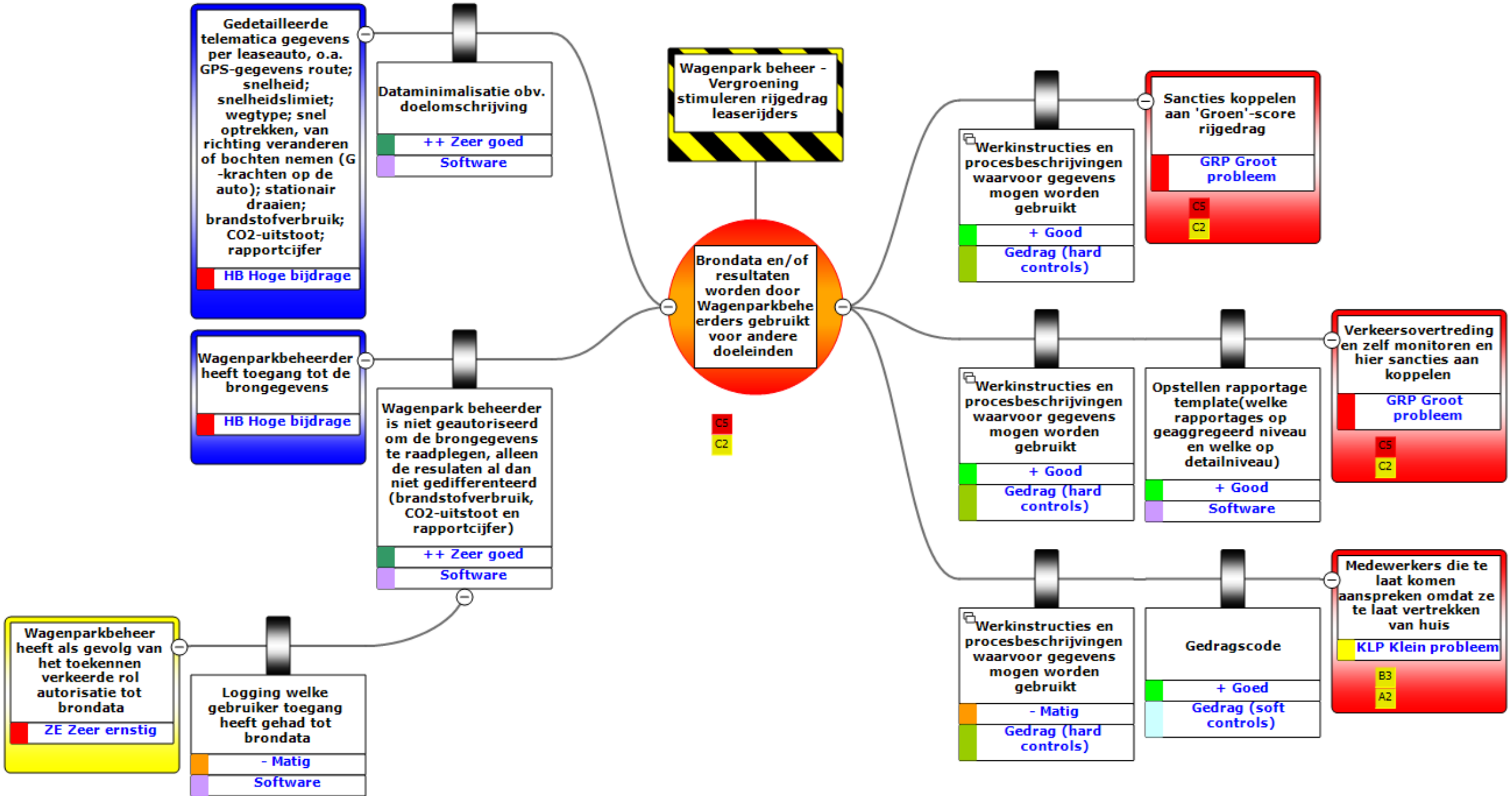
Gemaakt met BowTieXP

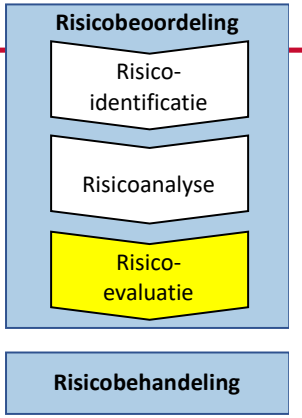
NOREA WEBINAR DPIA 2.0

Risicobeoordeling: Risicoanalyse

1. Bedreiging: bijdrage bepalen;
2. Consequenties: inherente risico's bepalen;
3. Barrières: effectiviteit maatregelen bepalen;
4. Consequenties: restrisico's bepalen.




Wagenpark beheer - Vergroening stimuleren rijgedrag leaserijders
Brondata en/of resultaten worden door Wagenparkbeheerders gebruikt voor andere doeleinden
C5
C2
Gedetailleerde telematica gegevens per leaseauto, o.a. GPS-gegevens route; snelheid; snelheidslimiet; wegtype; snel optrekken, van richting veranderen of bochten nemen (G-krachten op de auto); stationair draaien; brandstofverbruik; CO2-uitstoot; rapportcijfer
HB Hoge bijdrage
Dataminimalisatie obv. doelomschrijving
++ Zeer goed
Software
Wagenparkbeheerder heeft toegang tot de brongegevens
HB Hoge bijdrage
Wagenpark beheerder is niet geautoriseerd om de brongegevens te raadplegen, alleen de resulaten al dan niet gedifferenteerd (brandstofverbruik, CO2-uitstoot en rapportcijfer)
++ Zeer goed
Software
Wagenparkbeheer heeft als gevolg van het toekennen verkeerde rol autorisatie tot brondata
ZE Zeer ernstig
Logging welke gebruiker toegang heeft gehad tot brondata
- Matig
Software
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
+ Good
Gedrag (hard controls)
Sancties koppelen aan 'Groen'-score rijgedrag
GRP Groot probleem
C5
C2
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
+ Good
Gedrag (hard controls)
Opstellen rapportage template(welke rapportages op geaggregeerd niveau en welke op detailniveau)
+ Good
Software
Verkeersovertreding en zelf monitoren en hier sancties aan koppelen
GRP Groot probleem
C5
C2
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
- Matig
Gedrag (hard controls)
Gedragscode
+ Goed
Gedrag (soft controls)
Medewerkers die te laat komen aanspreken omdat ze te laat vertrekken van huis
KLP Klein probleem
B3
A2



Risicobeoordeling: Risico–evaluatie

1. Verder niets doen (risico accepteren)
2. Na te denken over opties voor risicobehandeling (beheersen risico)
3. Doeleinden herzien (elimineren risico)

Risicobehandeling

Omvat een iteratief proces van:

- het formuleren en selecteren van opties voor risicobehandeling;
- het plannen en implementeren van risicobehandeling;
- het beoordelen of de behandeling doeltreffend is;
- het beslissen of het resterende risico aanvaardbaar is;
- het overgaan tot verdere behandeling indien dit niet aanvaardbaar is

NOREA WEBINAR DPIA 2.0

- Blok 0. Opening
- Blok 1. Inleiding
- Blok 2. Opbouw en Structuur Handreiking/Raamwerk
- Blok 3. Risicobeoordeling met BowTie
- Blok 4. Afsluiting

NOREA WEBINAR DPIA 2.0

Ter afsluiting

- Engelstalige versie DPIA 2.0 is in de maak
- Handreiking en Raamwerk zijn beschikbaar op website NOREA https://www.norea.nl/handreikingen
- Gebruik en promoot
- Deel vooral jullie ervaringen en suggesties met ons (via norea@norea.nl)

Dank voor jullie aandacht!