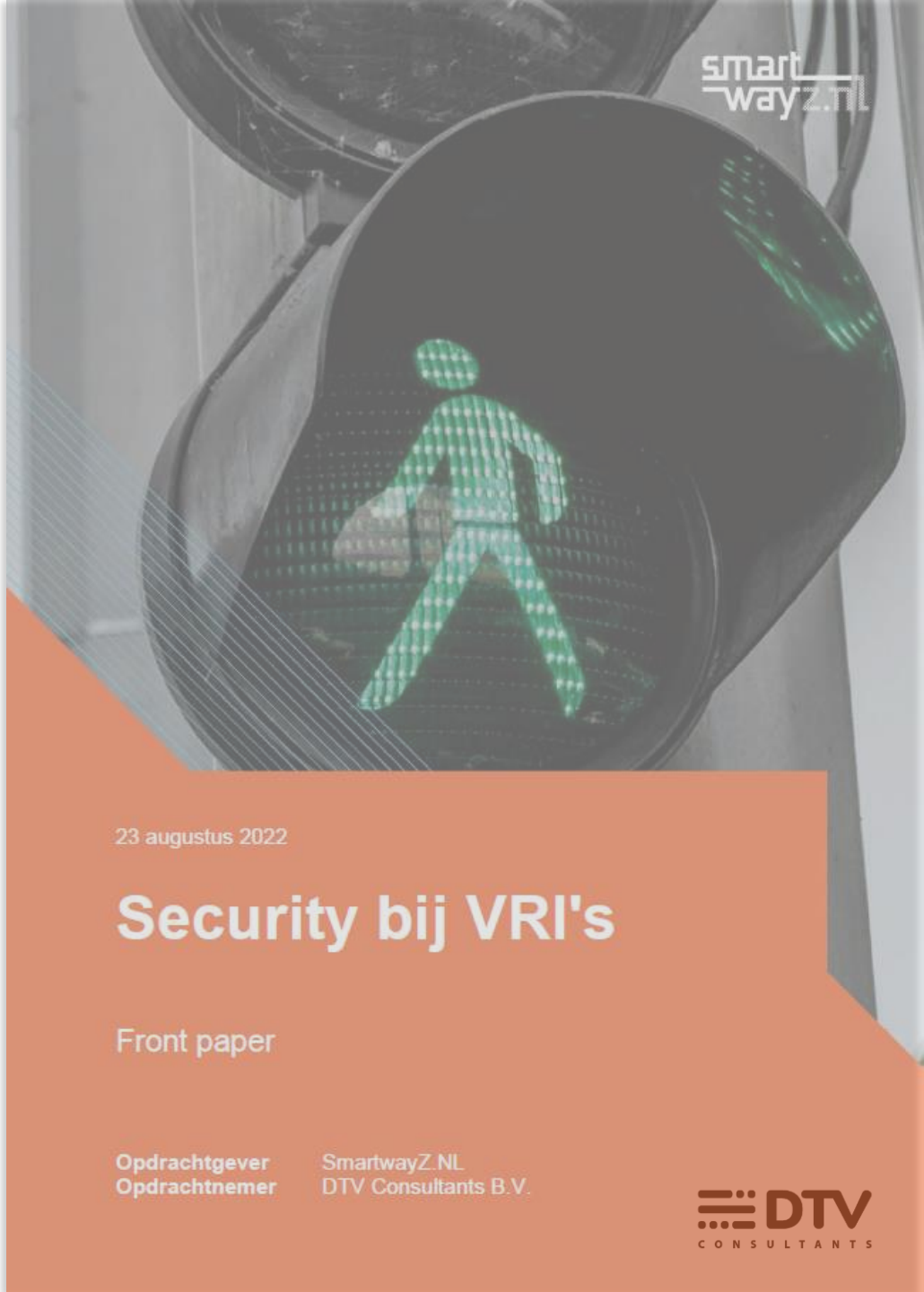
Security bij VRI’s

Front paper SmartWayZ.NL

IVERA kenniscafé
Woensdag 27 september 2023



Onderwerpen

- Aanleiding & doel
- Landschap
- Security issues
- Vervolg: wat kun je ermee

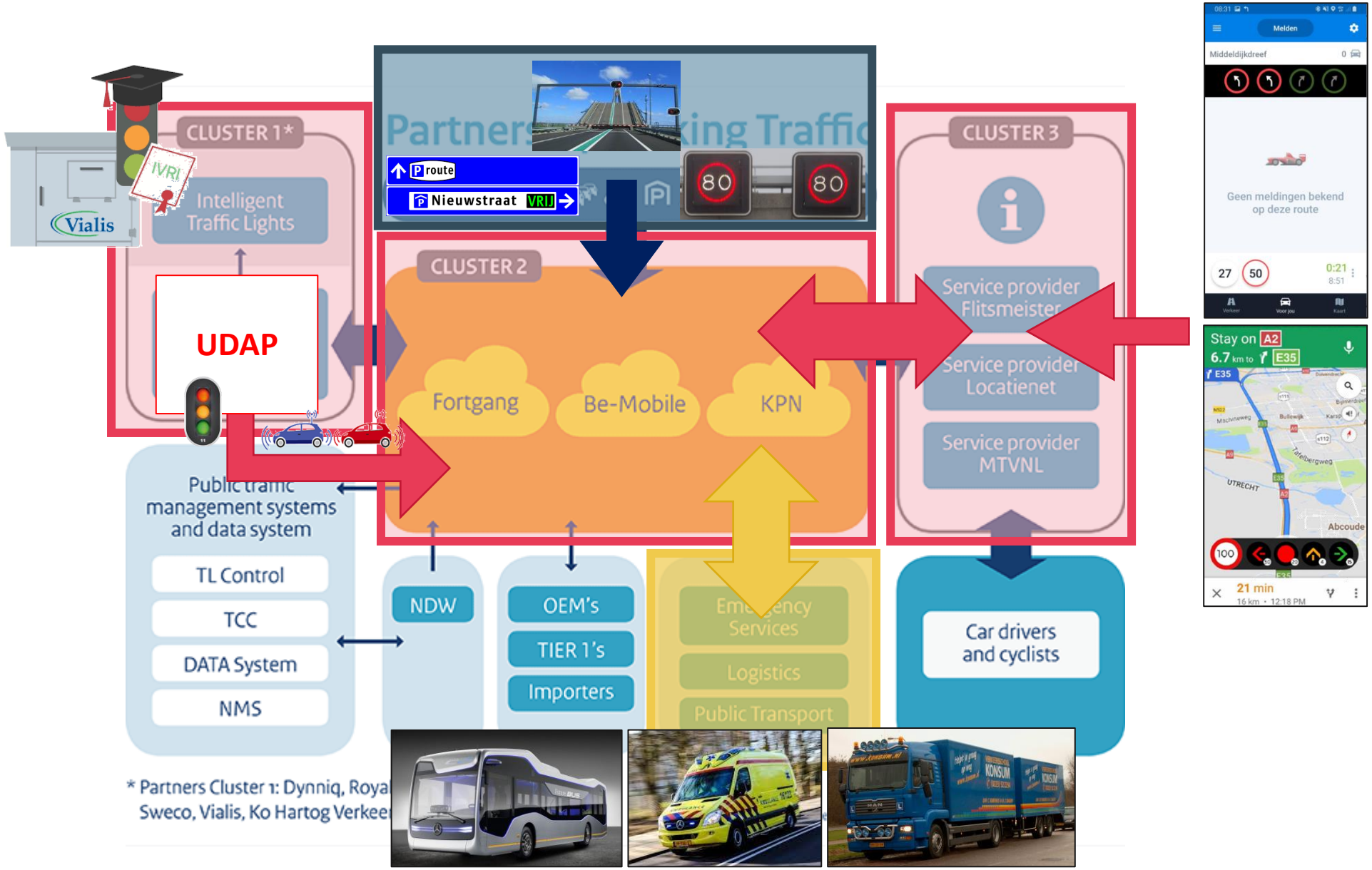
DTV CONSULTANTS

Aanleiding

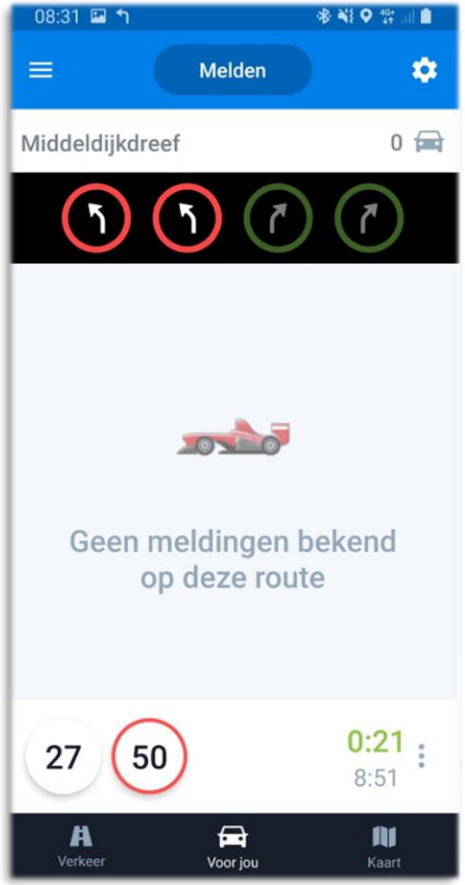
Met komst van de iVRI

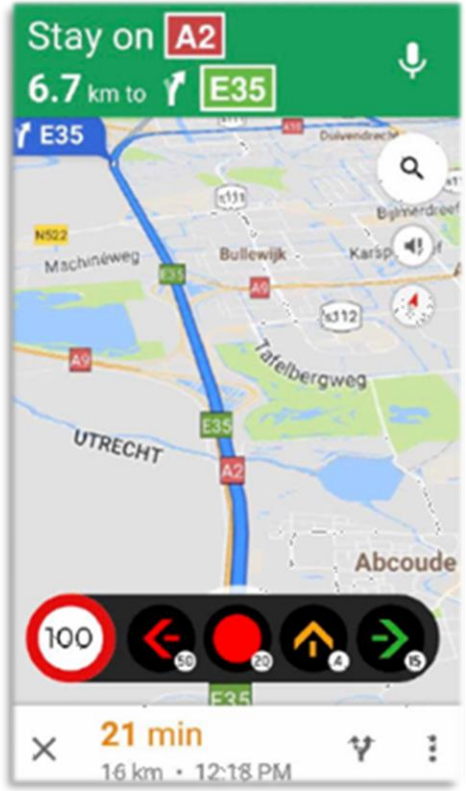
Is het landschap veranderd

Onderdeel dataketen



Nieuwe functionaliteiten (use cases)

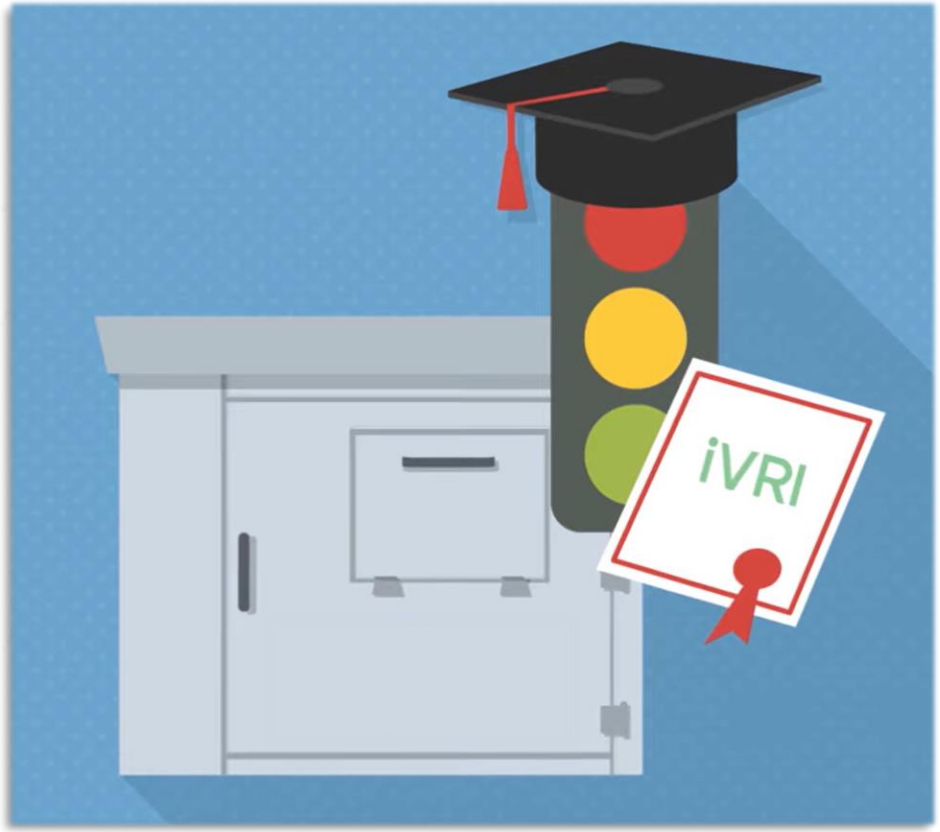




Meer aandacht security (en privacy)

DTV CONSULTANTS

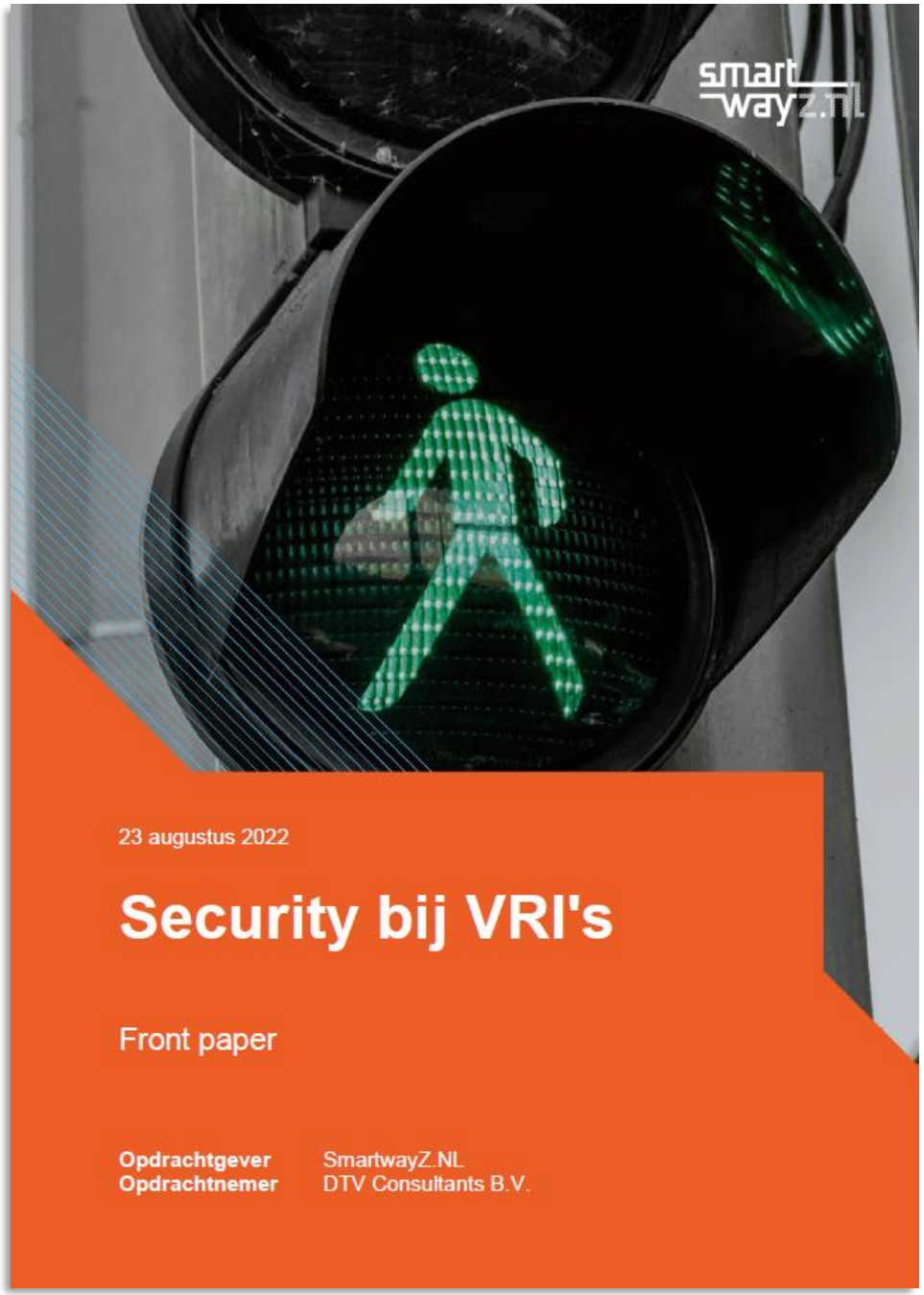
Overheid is eigenaar en beheerder



Meer specialistische kennis nodig

Specialisten samen optrekken

Opstellen front paper Security bij VRI’s



Doel

Doel

- Generieke front paper
- Waarmee betrokken overheden hun management kunnen informeren over security's rondom (i)VRI's

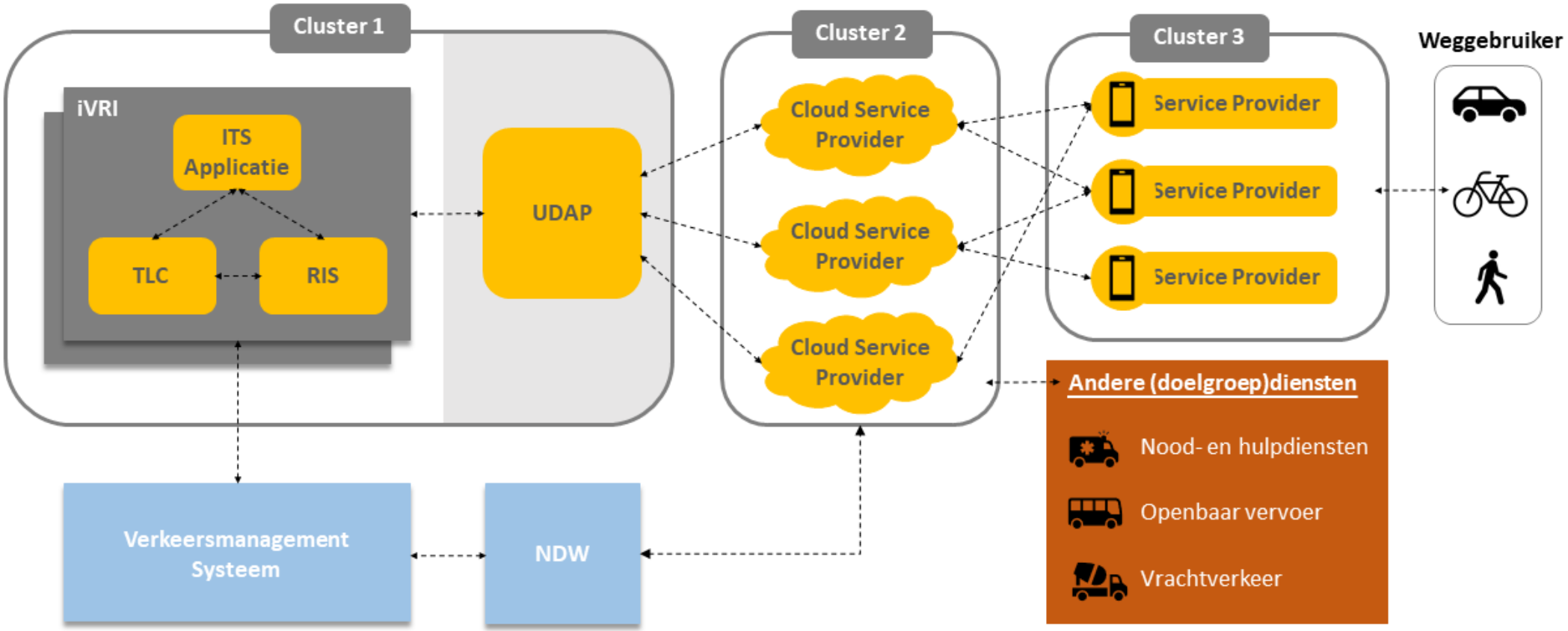
- Richten op gemeenschappelijke onderdelen voor alle overheden
- Niet op specifieke individuele onderdelen

- Eerste verkenning, geen handreiking

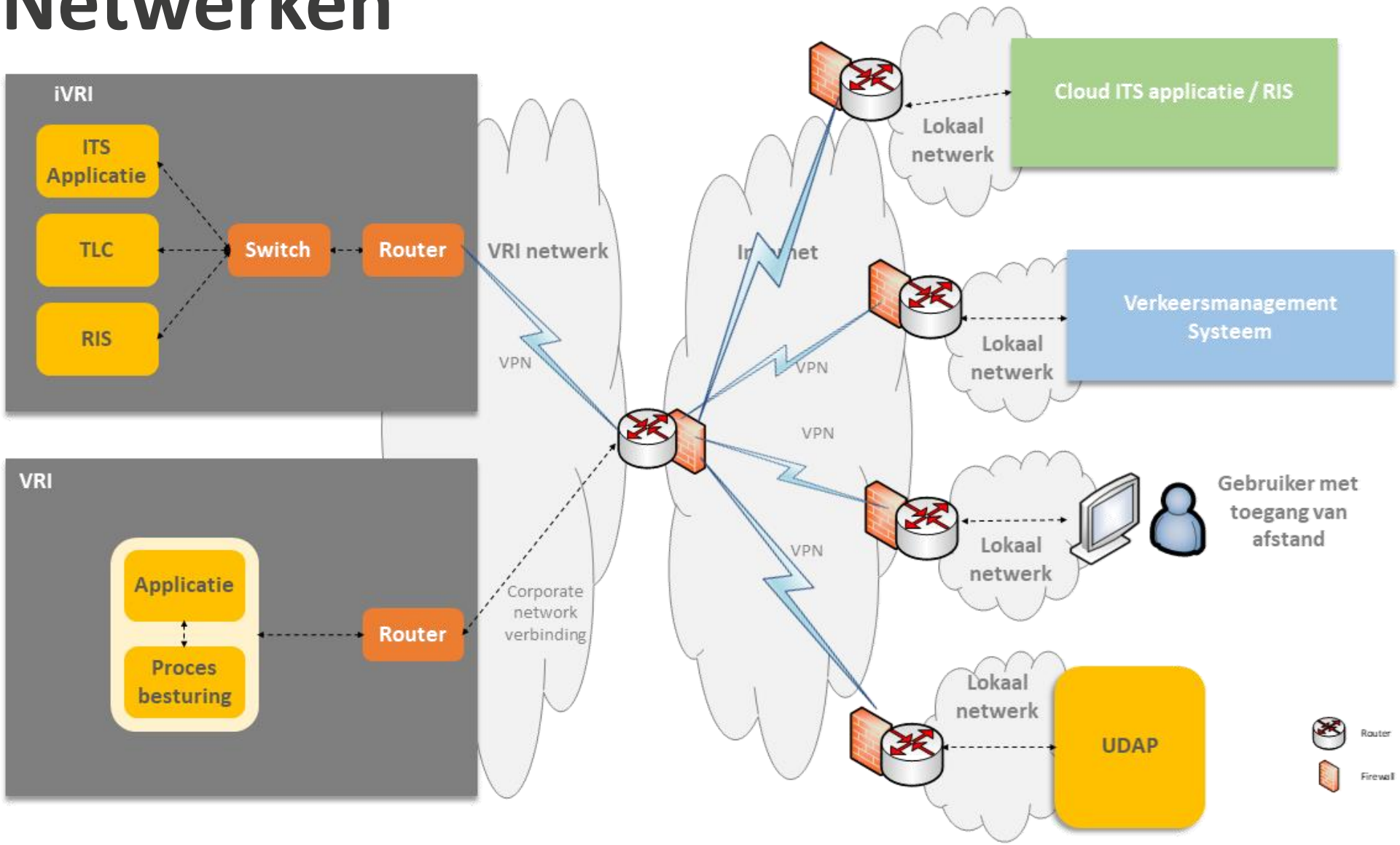
DTV CONSULTANTS

Landschap

Clusters


Cluster 1
iVRI
ITS Applicatie
TLC
RIS
UDAP
Cluster 2
Cloud Service Provider
Cloud Service Provider
Cloud Service Provider
Cluster 3
Service Provider
Service Provider
Service Provider
Weggebruiker
Andere (doelgroep)diensten
Nood- en hulpdiensten
Openbaar vervoer
Vrachtverkeer
Verkeersmanagement Systeem
NDW

Netwerken


iVRI
ITS Applicatie
TLC
RIS
Switch
Router
VRI
Applicatie
Proces besturing
Router
VRI netwerk
VPN
Corporate network verbinding
VPN
VPN
VPN
Lokaal netwerk
Cloud ITS applicatie / RIS
Lokaal netwerk
Verkeersmanagement Systeem
Lokaal netwerk
Gebruiker met toegang van afstand
Lokaal netwerk
UDAP
Router
Firewall

Security issues

Inventarisatie

DTV CONSULTANTS

Risico inventarisatie

- Interviews met VRI specialisten en CISO’s van B5 gemeenten en provincie, Ministerie I&W, VRI leverancier
- Toelichting CIBO (interprovinciaal CISO overleg)
- Literatuurstudie aangeleverde en beschikbare documenten

DTV CONSULTANTS

Risico inventarisatie

Ordening, onderverdeling naar onderwerpen:

- Toegangsbeheer
- Informatiebeveiliging
- Change management
- Incident management
- Personeel & organisatie
- Imago

DTV CONSULTANTS

Risico inventarisatie

- Per onderwerp risico's + beheersmaatregelen benoemd
- Beheersmaatregelen, toebedeeld aan:
  - Lokale/regionale overheid (gemeente, provincie, RWS)
  - Landelijke overheid (ministerie)
  - Leveranciers
- Checklist van de beheersmaatregelen opgesteld

DTV CONSULTANTS

Beheersmaatregelen wegbeheerder				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Fysiek toegangsbeheer	3.1.1	Fysiek sleutelbeheer/sleutelplan	1A	
		Compartimentenbeheer	1A	
		Fysieke toegang ruimtes	1A	
		Apparatuur	3A	
		Mandaatbeheer	1A	
Digitale toegang/ wachtwoordbeleid	3.1.1	Beleid digitale toegang	1A	
		Toegang tot centrale verkeersmanagementsystemen	1A	
		Toegang VRI-data	1A	
		Toegang UDAP	1A	
		Mandaatbeheer	1A	
Wachtwoordbeleid	3.1.1	Wachtwoordbeleid	1A	
Netwerkscheiding VRI-communicatienetwerken	3.1.1.	Inrichten gescheiden VRI-netwerk	3A	
		Onmogelijk maken vanuit een VRI andere VRI's te benaderen	3A	
Informatiebeveiliging				
Verantwoordelijk over data in de keten	3.1.2	Voldoen aan zorgplicht ten aanzien van aansprakelijkheid	2 / 3A	
		Afsluiten verwerkersovereenkomsten	1A	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Inrichten alternatief voor delen Security-gevoelige informatie	1A	
Change management				
Software updates	3.1.3	bepaal met leverancier restrisico's van het beperkt kunnen updaten van de software op embedded systemen	3A	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	3A	
Incident management				
Draaiboek incident management	3.1.4	Implementeer a.d.h.v. VNG 'Handreiking Incident- en response management'	1A	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1A 3A	
Imago				

Beheersmaatregelen leverancier				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Credential management VRI	3.1.1	Credential management - landelijk schaalbaar - opzetten	1B	
Change management				
Software updates	3.1.3	bepaal met wegbeheerder restrisico's van het beperkt kunnen updaten van de software op embedded systemen	1B / 3B	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	1B / 3B	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1B	
Overall				
BIO-certificering	3.1.7	BIO-eisen mee te nemen in ISO27001 certificering t.b.v. 'BIO In control' verklaring	3B	
Pen-testen	3.1.7	Pentesten uitvoeren voor de fysieke VRI, het netwerk en de overige applicaties	1B	

Beheersmaatregelen Landelijke overheid				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Informatiebeveiliging				
Verantwoordelijk over data in de keten + Aansluitvoorwaarden	3.1.2 + 3.1.4	Aansluitvoorwaarden Cloud service providers (C2) toepassen	2	
		Aansluitvoorwaarden service providers (C3) toepassen	2	
		Eigendom data vastleggen	2	
Toepassing van Public Key Infrastructure (PKI) / TLS	3.1.2	Landelijk inregelen gebruik PKI/TLS certificaten	2	
		Aanstellen van de Root Certificate Authority voor uitgifte en beheer van TLS- certificaten	2	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Digitaliseren iVRI koppelvlak configuratie formulieren, bij voorkeur in UDAP	2	
Overall				
BIO-eisen vertalen naar (i)VRI BIO eisen	3.1.7	Opstellen handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders.	2	
Bewustwording creëren	3.1.7	Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.	2	

Risico inventarisatie

Belangrijkste constateringen:

- Huidige (i)VRI's + netwerken voldoen niet aan BIO
  - Huidige eisen binnen aanbestedingen niet voldoende om iVRI's aan BIO te laten voldoen (kip-ei)
  - Wegbeheerders missen praktische vertaling van BIO voor thema (i)VRI
- Wegbeheerders hebben zelf diverse zaken vaak zelf ook nog niet op orde (sleutelplan, netwerkbeveiliging, toegang en autorisatie op systemen, onderhoudscontracten etc.)

DTV CONSULTANTS

Risico inventarisatie

Belangrijkste aanbevelingen/behoeftes:

- Vertaling BIO voor (i)VRI landelijk oppakken, zo uniform mogelijk landelijk toepassen
- Bespreken met leveranciers, consensus uitwerking eisen en reëel transitiepad
- Bewustwording creëren noodzaak security en benodigde aanpassingen om aan wet- en regelgeving te blijven voldoen
- Gebruik checklist door wegbeheerders voor eigen hiaten te definiëren en acties te benoemen

DTV CONSULTANTS

Vervolg

Wat kun je ermee?

Vervolg

- Front Paper als input voor LVMB actie ‘verbeterplan/handreiking security iVRI’
- Wegbeheerders gebruiken checklist beheersmaatregelen voor inventarisatie stand zaken binnen eigen organisatie en om acties te definiëren (controlelijst)
- Relatie met (rest)risico’s en beheersmaatregelen uit DPIA iVRI
- Uitwerking BIO eisen naar (i)VRI eisen, toewerken naar eerste concept voor landelijke voorbeeld set?

DTV CONSULTANTS

Voorbeeld gebruik checklist: Breda

- Invullen checklist beheersmaatregelen
  - Bepalen wat al voldoet en wat niet
  - Actiehouders benoemen
  - Externe hulp inschakelen
- Relatie leggen met risico’s uit DPIA iVRI

DTV CONSULTANTS

Beheersmaatregelen wegbeheerder				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Fysiek toegangsbeheer	3.1.1	Fysiek sleutelbeheer/sleutelplan	1A	
		Compartimentenbeheer	1A	
		Fysieke toegang ruimtes	1A	
		Apparatuur	3A	
		Mandaatbeheer	1A	
Digitale toegang/ wachtwoordbeleid	3.1.1	Beleid digitale toegang	1A	
		Toegang tot centrale verkeersmanagementsystemen	1A	
		Toegang VRI-data	1A	
		Toegang UDAP	1A	
		Mandaatbeheer	1A	
Wachtwoordbeleid	3.1.1	Wachtwoordbeleid	1A	
Netwerkscheiding VRI-communicatienetwerken	3.1.1.	Inrichten gescheiden VRI-netwerk	3A	
		Onmogelijk maken vanuit een VRI andere VRI's te benaderen	3A	
Informatiebeveiliging				
Verantwoordelijk over data in de keten	3.1.2	Voldoen aan zorgplicht ten aanzien van aansprakelijkheid	2 / 3A	
		Afsluiten verwerkersovereenkomsten	1A	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Inrichten alternatief voor delen Security-gevoelige informatie	1A	
Change management				
Software updates	3.1.3	bepaal met leverancier restrisico's van het beperkt kunnen updaten van de software op embedded systemen	3A	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	3A	
Incident management				
Draaiboek incident management	3.1.4	Implementeer a.d.h.v. VNG 'Handreiking Incident- en response management'	1A	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1A 3A	
Imago				

Beheersmaatregelen leverancier				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Credential management VRI	3.1.1	Credential management - landelijk schaalbaar - opzetten	1B	
Change management				
Software updates	3.1.3	bepaal met wegbeheerder restrisico's van het beperkt kunnen updaten van de software op embedded systemen	1B / 3B	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	1B / 3B	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1B	
Overall				
BIO-certificering	3.1.7	BIO-eisen mee te nemen in ISO27001 certificering t.b.v. 'BIO In control' verklaring	3B	
Pen-testen	3.1.7	Pentesten uitvoeren voor de fysieke VRI, het netwerk en de overige applicaties	1B	

Beheersmaatregelen Landelijke overheid				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Informatiebeveiliging				
Verantwoordelijk over data in de keten + Aansluitvoorwaarden	3.1.2 + 3.1.4	Aansluitvoorwaarden Cloud service providers (C2) toepassen	2	
		Aansluitvoorwaarden service providers (C3) toepassen	2	
		Eigendom data vastleggen	2	
Toepassing van Public Key Infrastructure (PKI) / TLS	3.1.2	Landelijk inregelen gebruik PKI/TLS certificaten	2	
		Aanstellen van de Root Certificate Authority voor uitgifte en beheer van TLS- certificaten	2	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Digitaliseren iVRI koppelvlak configuratie formulieren, bij voorkeur in UDAP	2	
Overall				
BIO-eisen vertalen naar (i)VRI BIO eisen	3.1.7	Opstellen handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders.	2	
Bewustwording creëren	3.1.7	Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.	2	

Voorbeeld Breda

[screenshots voorbeelden Breda niet opgenomen, informatie op te vragen bij Erik van Holten en Tom Steijvers]

Inventarisatie

- Opstellen functionele VRI landschap Breda
- In kaart brengen huidige situatie
  - Toegang en autorisatie
  - Dataketen en opslag
  - Incidentmanagement
- In kaart brengen gewenste situatie
- Hiaten definiëren en beheersmaatregelen voorstellen

DTV CONSULTANTS

Voorbeeld Breda

[screenshots voorbeelden Breda niet opgenomen, informatie op te vragen bij Erik van Holten en Tom Steijvers]

LVMB ‘Hoe verder met de iVRI?’

- Weinig tot geen aandacht voor security en privacy
- Maar toch wel mogelijke handvatten:
  - Mogelijkheden bieden naar vereenvoudiging
    - Eigen snelheid kiezen
    - Standaarden en speelveld vereenvoudigen
  - Meerwaarde en financiering
    - Meerwaarde en businessmodel (kosten)
    - Herprofilering t.b.v. bijdrage
  - Governance en samenwerking
    - Ketenorganisatie structureel inrichten
    - Ketenuitwisseling en opleiding/begeleiding

Vragen?

DTV CONSULTANTS

=> Stellingen

DTV CONSULTANTS