

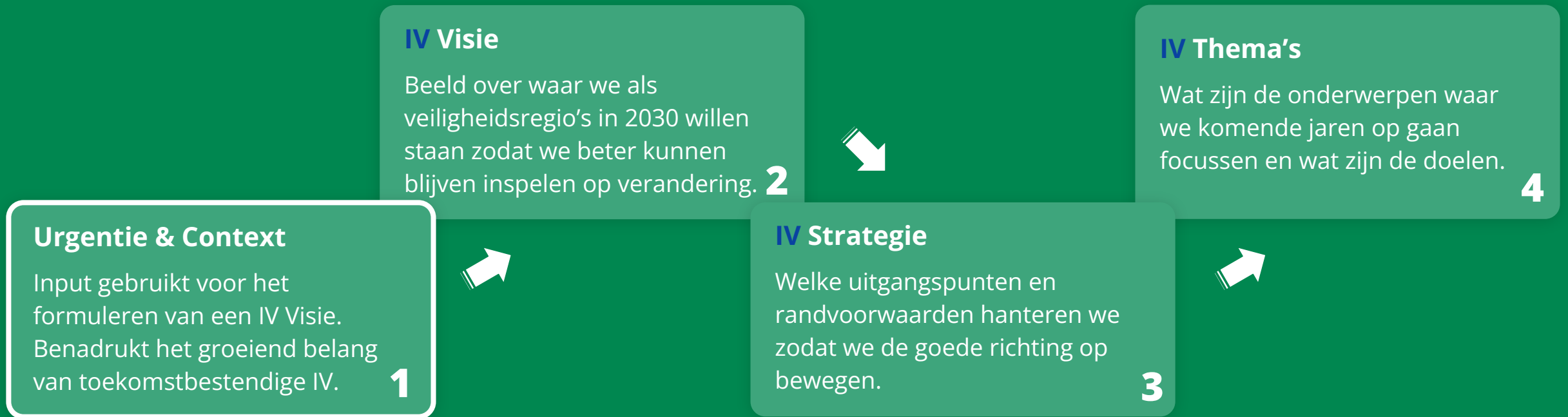
IV* Visie 2026 - 2030



** Informatievoorziening & ICT*



Aanpak



Digitale Ontwrichting

*Digitale verstoring is geen ICT-probleem.
Het is een veiligheidsprobleem.*

Dreiging

- Cyberaanvallen op overheden stijgen explosief
- Aanvallen richten zich steeds vaker op lokale en regionale overheden
- Datalekken en ketenaanvallen raken vitale processen
- Steeds meer aanvallen op hulpdiensten in EU-lidstaten



Noodzaak & Rol IV

- Digitale weerbaarheid wordt behandeld als brandveiligheid: structureel, periodiek, risico-gebaseerd
- Veerkrachtige infrastructuur (redundantie*, zero trust**, cloud-first***)
- Real-time inzicht op cyberdreigingen
- Ononderbroken toegang tot vitale systemen

* Reservesystemen zodat we altijd door kunnen werken.

** Toegang wordt altijd gecontroleerd, niets wordt zomaar vertrouwd.

*** Systemen staan in principe niet fysiek op onze locaties maar in de cloud.

Klimaat

IV speelt een cruciale rol in het voorbereiden, voorspellen en handelen bij extreem weer.

Dreiging

- Extreem weer neemt toe: zware neerslag, wateroverlast, hittegolven en stormschade
- Overstromingsrisico's stijgen door zeespiegelstijging en piekbelasting van waterkeringen
- Droogteperioden veroorzaken bodemdaling, natuurbranden en uitval van vitale infrastructuur
- Keteneffecten: verstoring in mobiliteit, energievoorziening en hulpdiensten



Noodzaak & Rol IV

- Geautomatiseerde monitoring: Waterstand, neerslag, wind, hitte, droogte
- Samenwerking in ketens versterken met gedeelde dashboards, meetgegevens van sensoren in het veld, landelijk datamodel en uniforme protocollen
- Voorspellende scenario's voor inzetoptimalisatie en evacuatie-routing
- Automatische alarmering & besluitvorming: drempelwaarden, triggers en handelingsperspectieven

Energietransitie

*IV is essentieel om risico's te voorspellen,
te beheersen en incidenten te voorkomen.*

Dreiging

- Toename van batterijbranden (elektrische voertuigen, thuisbatterijen, grootschalige energieopslag)
- Opslag van nieuwe energiedragers (o.a. waterstof, lithium) vergroot risico's bij incidenten
- Netcongestie en overbelasting van energienetten leiden tot uitval en verstoring van hulpdiensten
- Onvoldoende zicht op locaties van risicovolle installaties (PV-installaties, laadpleinen, energiehubs)



Noodzaak & Rol IV

- Regionale risicobeelden op basis van data: locaties van opslag, laadinfra, waterstofinstallaties & incidentdata
- Integratie van ketenpartners (netbeheerders, gemeenten, industrie) in één gezamenlijke manier om informatie te delen
- Voorspellende data-analyses om brandrisico, overbelasting of falen van installaties vroegtijdig te signaleren
- Realtime monitoring van kritieke infrastructuur (temperatuur, spanning en belasting)

Landelijke & EU IV Agenda

Strategisch belang IV

Urgentie Complexe Crises
Veiligheidsberaad Thema's

VR

Masterprogramma IV
Vakraad IV

VR

6 Prio's Digitaliseringsstrategie
Rijksoverheid



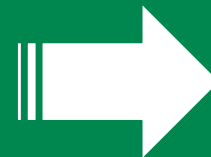
Beleidsplan 2025-2028
VrZW

VR

Digital Decade
EU



Vitaal aanbieder verklaring
JnV



Uit de input links destilleren we de belangrijkste kenmerken voor een toekomstbestendige veiligheidsregio:

Preventief
Proactief
Continu lerend
Onderdeel van Netwerk
Digitaal
Robuust

Spelregels IV *

BIO2



NIS2



AI Act



Woo



Archiefwet

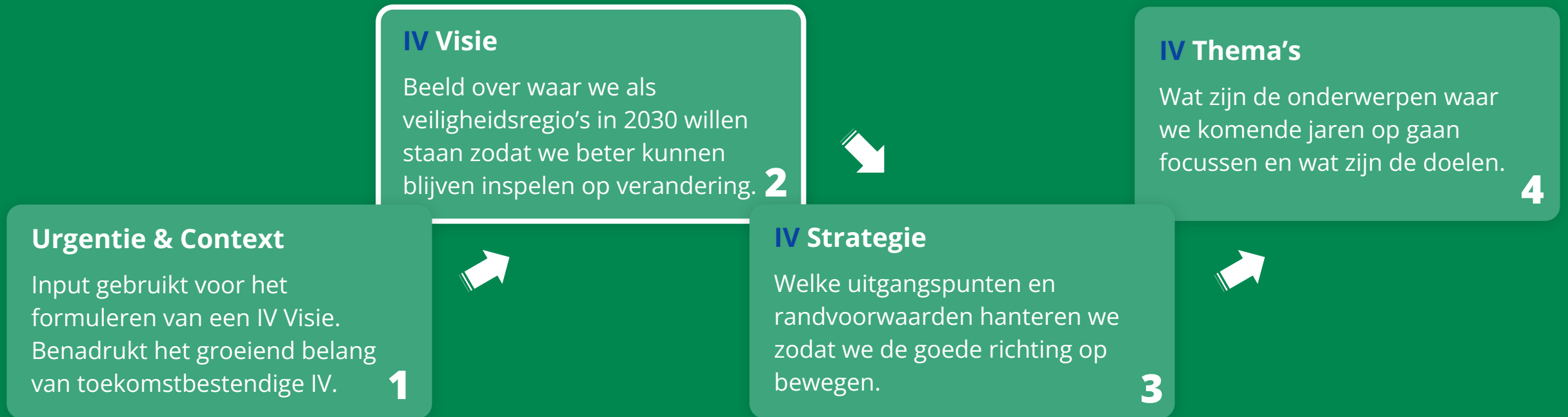


AVG



* **BIO**: Baseline Informatiebeveiliging Overheid. Verplichte beveiligingskader voor overheden.
NIS2: Network and Information Security. Aangescherpte Europese kaders die de cybersecurity-eisen voor bedrijven en organisaties in vitale sectoren verhoogt.
AI Act: Beoogt (vanuit EU) veilige en betrouwbare AI te stimuleren, innovatie te bevorderen en fundamentele rechten van burgers te beschermen.
Woo: Wet Open Overheid. Wet die het recht op toegang tot publieke informatie regelt.
Archiefwet: Het hoofddoel is om informatie duurzaam toegankelijk te houden voor verantwoording, rechtsvinding en cultureel erfgoed.
AVG: Algemene Verordening Gegevensbescherming. Europese privacywet die bepaalt hoe bedrijven en organisaties moeten omgaan met persoonsgegevens.

Aanpak



IV Visie 2030

Veiligheidsregio's werken als
EEN robuust, digitaal
immuunsysteem; preventief,
proactief en continu lerend.



Aanpak

IV Visie

Beeld over waar we als veiligheidsregio's in 2030 willen staan zodat we beter kunnen blijven inspelen op verandering. **2**

Urgentie & Context

Input gebruikt voor het formuleren van een IV Visie. Benadrukt het groeiend belang van toekomstbestendige IV. **1**

IV Strategie

Welke uitgangspunten en randvoorwaarden hanteren we zodat we de goede richting op bewegen. **3**

IV Thema's

Wat zijn de onderwerpen waar we komende jaren op gaan focussen en wat zijn de doelen. **4**

IV Strategie 2026 - 2030

Om als organisatie preventiever, proactiever en innovatiever te werken, moet onze IV betrouwbaar, veilig en vernieuwend zijn. Daarom professionaliseren we onze IV organisatie met duidelijke IV basisprincipes en heldere randvoorwaarden.

IV Basisprincipes

Dit gaat over hoe we werken.

Uitgangspunten die ons helpen om meer preventief, proactief en innovatief te worden. Ze zullen de basis gaan zijn voor het IV Beleid.

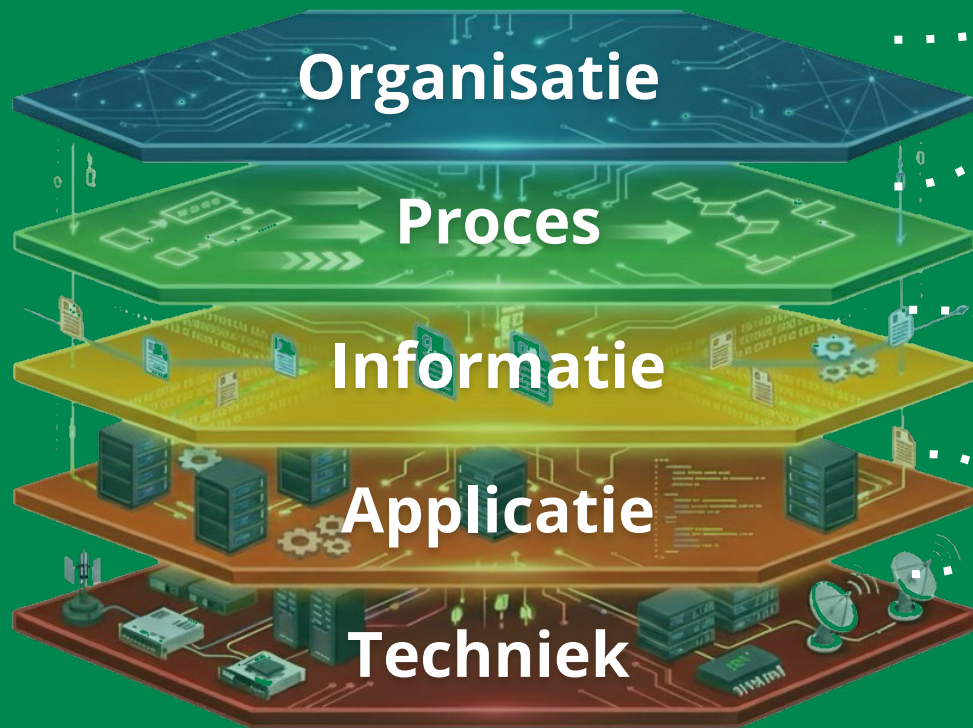
IV Randvoorwaarden

Dit gaat over de veiligheidsgaranties die we altijd waarborgen.

Randvoorwaarden om onze IV veilig, uniform en betrouwbaar te houden, vandaag én in de toekomst.

IV Basisprincipes

IV zit in elke laag en bepaalt ons vermogen om te voorspellen, reageren en leren.



Sturing is datagedreven, impact van initiatieven is meetbaar.

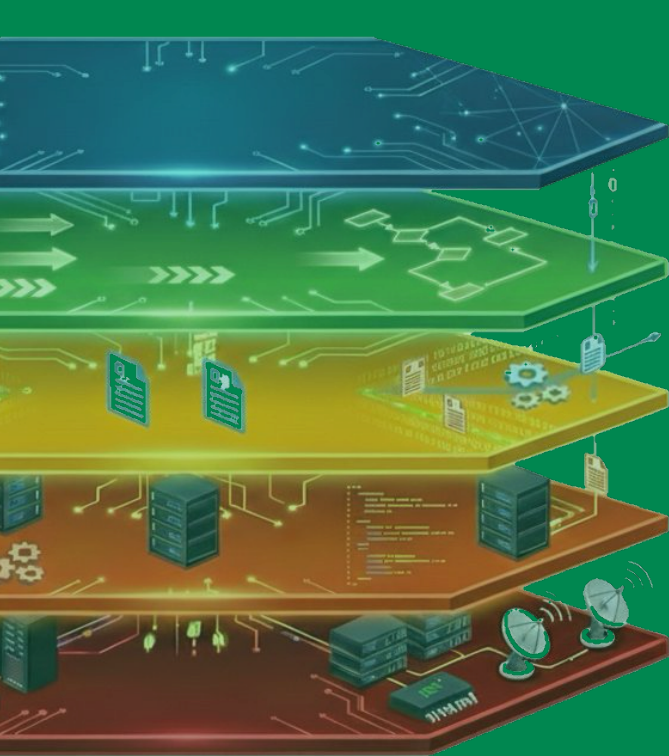
Processen zijn levend, hebben een eigenaar, prestatie is meetbaar, innoveren is de norm. Je werkt niet alleen **IN** maar ook **AAN** processen.

Iedereen draagt bij aan informatie. Iedereen is daarom verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van de onderliggende data.

Applicaties en techniek zijn standaard en veelal een commodity. Met andere regio's werken we toe naar uniformiteit zodat kennis en kunde uitwisselbaar is.

IV Randvoorwaarden

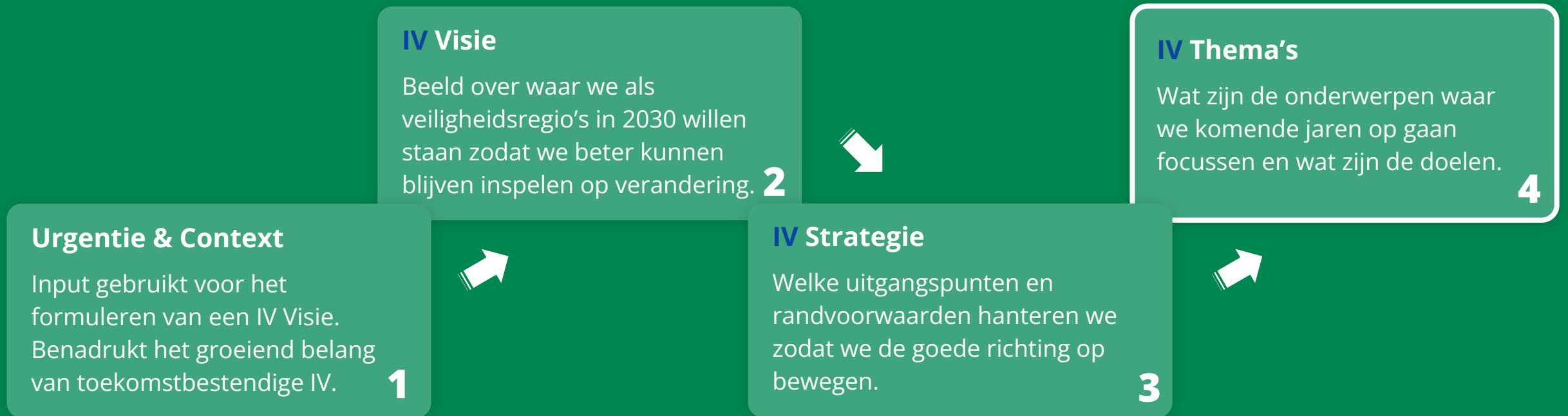
Over alle lagen heen gelden randvoorwaarden die beschikbaarheid, integriteit, veiligheid en wendbaarheid van IV versterken.



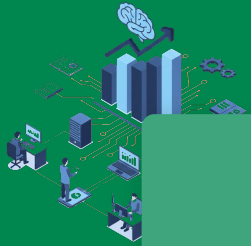
• **Digitale weerbaarheid** als randvoorwaarde voor operationeel optreden. Beveiliging en privacy zijn vanaf het begin ingebouwd in alles wat we doen.

• **Informatie als strategisch middel:** Eenduidig, vindbaar, betrouwbaar en duurzaam toegankelijk. Geen maatwerk, maar standaardisatie van processen, informatiemodellen en archivering.

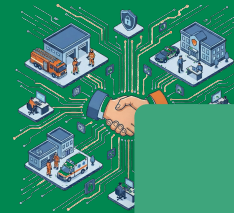
Aanpak



IV Thema's 2026 - 2030



Professionalisering IV



Samenwerken



Informatiebeveiliging & DIV



Innovatie

Professionalisering IV

In 2030

Een organisatie waarin informatievoorziening strategisch, integraal en toekomstbestendig is georganiseerd. Onze IV basisprincipes en IV randvoorwaarden worden toegepast.

Er is een volwassen team dat de IV koers bepaalt, standaarden bewaakt en digitale veiligheid borgt. IV rollen zijn ingebed in de teams en vormen samen met architectuur en security één samenwerkend netwerk.

● 2026 (basis op orde)

- ✓ Klein strategisch team dat de IV koers bewaakt
- ✓ IV rollen harmoniseren
- ✓ Een overleg dat beslist over prioriteiten in IV-projecten
- ✓ Implementeren IV beleid

2027 .. 2030 (tbd)

Informatiebeveiliging & DIV

In 2030

De veiligheidsregio heeft een volwassen en gecertificeerd systeem voor informatiebeveiliging en informatiebeheer. We werken datagedreven: realtime inzicht in risico's, kwetsbaarheden en dreigingen ondersteunt besluitvorming.

Risico's zijn vroegtijdig inzichtelijk door continue monitoring en analyses, waardoor we proactief kunnen handelen. Dankzij hoge digitale vaardigheid en goede ketensamenwerking zijn informatie en documenten betrouwbaar en duurzaam toegankelijk.

● 2026 (basis op orde)

- ✓ Implementeren BIO* feedback
- ✓ BIO2* Gap analysis
- ✓ Robuust DIV**
- ✓ Cybersecurity Awareness verhogen

● 2027 .. 2030

- ✓ Inrichten ISMS
- ✓ ISO 27001*** certificering
- ✓ BIO2* Compliance

* Baseline Informatiebeveiliging Overheid. Verplichte beveiligingskader voor overheden.

** Documentaire Informatievoorziening. Gestructureerd beheren, registreren, archiveren en ontsluiten van documenten.

*** Hét internationale keurmerk voor informatiebeveiliging.

Samenwerken

In 2030

In 2030 werken veiligheidsregio's digitaal als één netwerk: met vaste verbindingen, gezamenlijke inzichten en uniforme handeling. Dat vraagt om harmonisatie en gezamenlijke regie; van 25 beelden naar één beeld. Om dit mogelijk te maken werken we samen in gespecialiseerde vakgroepen. Onze veiligheidsregio is hier vertegenwoordigd en draagt bij. Op die manier borgen we kennis en zijn wij altijd op de hoogte van de laatste ontwikkelingen.

2026

- ✓ Gezamenlijk VIK* (VrZW, VrNHN, VrK)
- ✓ Standaardisatie BI** tooling (we kijken hiervoor naar andere regio's)
- ✓ Participeren in IV Netwerken: Missie Kritische Communicatie, Architectuur, Informatieveiligheid, etc.
- ✓ Kansen voor samenwerking met burens worden benut

2027 .. 2030

- ✓ Gezamenlijk VIK* (VrZW, VrNHN, VrK, VrAA)
- ✓ Standaardisatie MOI (we kijken hiervoor naar andere regio's)

* Veiligheidsinformatieknooppunt geeft 24/7 actueel beeld rondom dreigingen en kwetsbaarheden in een veiligheidsregio.

** Business Intelligence. Standaardsoftware voor inzichten en dashboards.



Innovatie

In 2030

Het blijft ook in 2030 belangrijk om nieuwe kansen op het gebied van digitalisering te benutten. We spelen goed doordacht in op nieuwe technologische ontwikkelingen. AI is integraal onderdeel van hoe wij werken. Continu leren is onderdeel van onze cultuur. Onze organisatie is in staat om snel in te spelen op nieuwe ontwikkelingen.

● 2026 (basis op orde)

- ✓ “Digitaal Fit” trainingsprogramma
- ✓ Er is ruimte voor innovatie
- ✓ Inzet AI wordt gestimuleerd

● 2027 .. 2030

- ✓ Meewerken aan landelijke AI en Augmented Reality initiatieven
- ✓ AI is integraal onderdeel van hoe wij werken