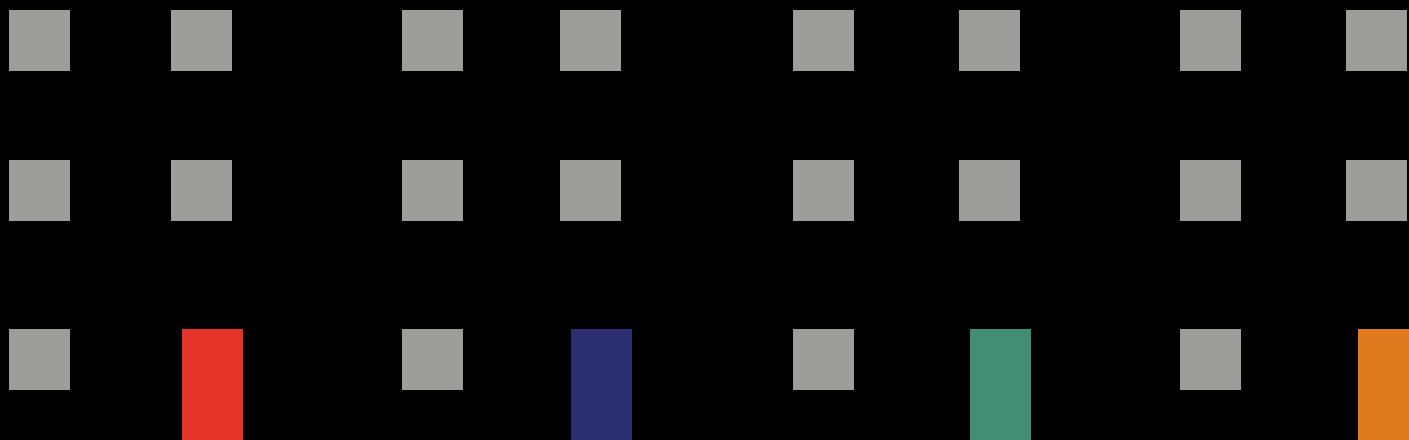
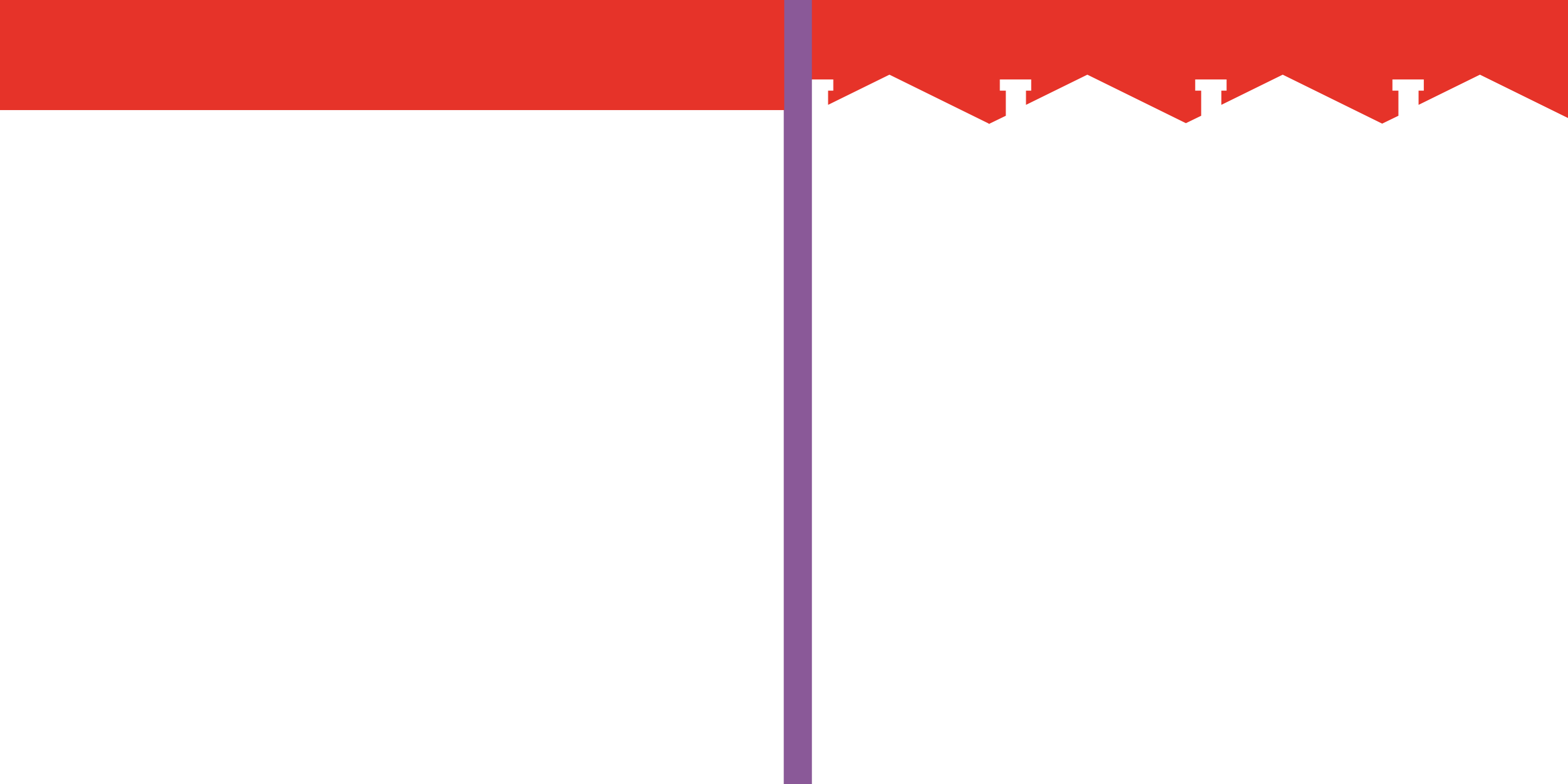




Veiligheidsregio Referentie Architectuur

Samenwerking door samenhang in
informatievoorziening binnen de veiligheidsregio's





Voorwoord

Voor u ligt de tweede versie van de Veiligheidsregio Referentiearchitectuur: de VeRA, een prestatie om trots op te zijn. De ontwikkeling van de VeRA is al in 2011 gestart door een kernteam van informatiemanagers. De eerste VeRA versie is in 2012 vastgesteld in het Veiligheidsberaad. Deze eerste versie eindigde met de belofte dat er een nadere uitwerking zou volgen in de VeRA 2.0. Deze belofte is nu ingelost, VeRA 2.0 is op 20 maart 2015 door het Veiligheidsberaad vastgesteld.

VeRA geeft invulling aan artikel 22 van de Wet Veiligheidsregio's. Die wettekst was echter niet de reden om met de VeRA te starten. Veiligheidsregio's zijn relatief jonge organisaties, sterk in ontwikkeling, die veel in ketens werken. Ze kennen veel uitdagingen en zoektochten, zeker op het gebied van de informatievoorziening. Informatiemanagers uit diverse veiligheidsregio's hebben dat ingezien en besloten om een gezamenlijke architectuur te schrijven. Hiermee willen ze het hebben en delen van informatie binnen en tussen veiligheidsregio's en met haar partners uniform inrichten en verbeteren.

De VeRA staat niet op zichzelf. Zij is gebaseerd op de NORA (Nederlandse Overheid Referentiearchitectuur) en heeft zussen als de Petra (Provinciale Referentiearchitectuur) en de Gemma (Gemeentelijke Modelarchitectuur). Gelijktijdig met de ontwikkeling van de VeRA hebben ook de RUD's (RUDI) en de GGD'en (PURA) hun eigen sectorale architectuur geschreven.

De VeRA heeft haar toegevoegde waarde inmiddels bewezen. Het ontwerp van een nieuw Nationaal Meldkamersysteem (NMS) is getoetst aan de VeRA. Betrokkenen onderschrijven dat architectuur juist in deze complexe materie een uniform uitgangspunt biedt. De VeRA wordt ook gebruikt door enkele veiligheidsregio's die er hun eigen bedrijfsarchitectuur van hebben afgeleid. Tot slot is zij als basis opgenomen in het programmaplan informatievoorziening veiligheidsregio's 2015 – 2020. Het Veiligheidsberaad heeft bij de vaststelling van de VeRA 2.0 aan alle regio's gevraagd om het in de eigen regio te gaan toepassen.

De VeRA is door en voor informatiemanagers uit de veiligheidsregio's gemaakt. Daarnaast moeten ook hun regionale managers en procesverantwoordelijken met de VeRA aan de slag. Bij de aanschaf van nieuwe software, bij het delen van gegevens tussen processen en bij het investeren in de kennis en kunde van de informatiemanager hebben zij immers een doorslaggevende rol. De VeRA is daarbij geen blauwdruk en ook geen lesboek; het levert kaders om professioneel te werken aan de informatievoorziening.

We hopen dat deze collega's met dit document gaan werken in de geest waarmee aan VeRA begonnen is. Namelijk: een voor en door veiligheidsregio's geschreven referentiedocument dat hen helpt om de gedachten rond de inrichting van de informatievoorziening te kunnen vormen en de juiste keuzes te kunnen maken.

Er hebben veel mensen geholpen bij het schrijven en compleet maken van de VeRA, onze dank gaat naar hen uit. Bijzondere dank gaat uiteraard uit naar de leden van het kernteam VeRA die onvermoeid zijn blijven discussiëren, schrijven, presenteren en redigeren: Sandra McEwan, Eurydice van Vliet, Bart den Dulk, Rob Peters en Edith Langerak.

Diemer Kransen	Raad van Brandweer Commandanten
Aart Schoenmaker	Raad van Directeuren Publieke Gezondheidszorg
Arjen Littooi	Raad van Directeuren Veiligheidsregio



Inhoudsopgave

	Voorwoord	5	3	Bedrijfsarchitectuur	20
	Inhoudsopgave	6	3.1	Producten en diensten	21
1	Inleiding	7	3.1.1	Wat zijn Producten en diensten	21
1.1	Veiligheidsregio's en informatievoorziening	7	3.1.2	Producten en diensten van een veiligheidsregio	21
1.2	De VeRA als gezamenlijk vertrekpunt	8	3.1.3	Beschrijving van de producten en diensten van de veiligheidsregio's	23
1.3	De VeRA in groter verband	10	3.2	Bedrijfsprocessen	27
1.4	De architectuurproducten van de VeRA	10	3.2.1	Wat zijn bedrijfsprocessen?	27
1.5	Domeinen	12	3.2.2	Relaties met andere (procesgerichte) kaders	28
1.6	Leeswijzer	14	3.2.3	Bedrijfsprocessen van een veiligheidsregio	28
2	Visie en principes	12	3.2.4	Beschrijving bedrijfsprocessen	30
2.1	Inleiding	12	3.3	Bedrijfsfuncties	32
2.2	Visie	12	3.3.1	Wat zijn bedrijfsfuncties?	32
2.2.1	Visie op architectuur	12	3.3.2	Beschrijving bedrijfsfuncties van een veiligheidsregio	34
2.2.2	Van eilandautomatisering naar informatiedeling	13	3.3.3	Definities bedrijfsfuncties	35
2.3	Principes	16	3.4	Ketensamenwerking	36
2.3.1	Informatiekundige architectuurprincipes	16	3.4.1	De Veiligheidsregio en de Politie	38
2.3.2	Beveiliging en Privacy architectuurprincipes	18	3.4.2	De Veiligheidsregio en de GGD	40
2.3.3	Beheer principes	18	3.4.3	Impact van de brede samenwerking met Politie en GGD op de informatie uitwisseling	42
2.3.4	Service gerichte architectuurprincipes	19			

4	Informatiearchitectuur	43	5	Beheer	58
4.1	Inleiding tot informatiearchitectuur	43	5.1	Waarom beheer	58
4.2	Applicatieve functies	45	5.2	BISL	58
4.2.1	Besturende applicatieve functies	45	5.3	Wat is beheer?	59
4.2.2	Primaire applicatieve functies	46	5.4	Functioneel beheer	60
4.2.3	Secundaire applicatieve functies	47	6	Actuele en toekomstige ontwikkelingen	61
4.3	Gegevens	49		Bijlage A:	65
4.3.1	Basisregistraties	49		wettelijke taken en bevoegdheden veiligheidsregio's	
4.3.2	Externe gegevensbronnen	50		Dankwoord	67
4.3.3	Eigen kernregistraties	51		Afkorting	68
4.3.4	Interne gegevensbronnen	51		Begrippen	69
4.3.5	Geografische informatie	51			
4.4	Gegevensuitwisseling	53			
4.4.1	Typen gegevens uitwisseling	53			
4.4.2	Standaarden voor gegevens uitwisseling	54			
4.5	Samenhang bedrijfsarchitectuur en informatie architectuur	56			



1 Inleiding

1.1 Veiligheidsregio's en informatievoorziening

Nederland heeft 25 veiligheidsregio's, waarin brandweer en GHOR met partners zoals politie, Ambulancezorg en gemeenten samenwerken aan het voorkomen en bestrijden van incidenten en rampen. In het verleden coördineerde een kleine regionale brandweerorganisatie de crisisbeheersing in samenwerking met gemeentelijke brandweerkorpsen. Op 1 oktober 2010 is de Wet veiligheidsregio's (Wvr, 2010)¹ van kracht geworden. In de Wvr zijn onder meer opgenomen de bestuurlijke inbedding en de basisvereisten voor de organisatie van de hulpverleningsdiensten, de taken van het bestuur van een veiligheidsregio, de minimumeisen voor hulpverleners als de regionale brandweer en geneeskundige diensten en het materieel dat ze gebruiken. Voor de VeRA relevante Wvr-artikelen zijn in de bijlage opgenomen.

De veiligheidsregio is georganiseerd als verlengd lokaal bestuur.

Personeel, taken en budgetten zijn overgeheveld van gemeenten naar de veiligheidsregio's, die de primaire en ondersteunende processen regionaal organiseren.

Informatievoorziening² is een belangrijk aspect voor de veiligheidsregio's, zowel in het dagelijks werk ('koud') als in crisissituaties ('warm'). Informatie is nodig bij het adviseren over vergunningen, bij het betalen van salarissen, bij het maken van roosters voor operationeel personeel, bij het bestrijden van een brand etc.

¹ Wet van 11 februari 2010, houdende bepalingen over de brandweerzorg, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening (Wet veiligheidsregio's). Staatsblad van het Koninkrijk der Nederlanden, jaargang 2010.

² In het Besluit Veiligheidsregio's is §4 volledig gewijzigd aan Informatiemanagement.

Iedere veiligheidsregio heeft de uitdaging de informatiehuishouding vorm te geven tot een regionale, geoliede machine die de interne processen en de relaties met ketenpartners optimaal ondersteunt. In deze keten³ neemt de behoefte toe aan het gezamenlijk gebruik van gegevens. Dit betekent dat deze gegevens in de keten beheerd moeten worden en dat hierover afspraken gemaakt moeten worden. Intussen is de omgeving ook in beweging: er vindt samenvoeging plaats van meldkamers, regio's moeten wettelijk verplicht gebruik maken van basisregistraties, en er zijn landelijke projecten die invloed hebben op de interne informatievoorziening. Intern moeten kernregistraties ingericht worden: gegevensbronnen die door meerdere processen en applicaties kunnen worden gebruikt. Op bestuurlijk niveau is de aandacht voor informatievoorziening groot en uit meerdere rapportages blijkt dat dit aspect bij de veiligheidsregio's nog onvoldoende op orde is. Informatiemanagers van de veiligheidsregio's voelen door al deze ontwikkelingen de behoefte om samen te werken aan een basis voor de informele voorziening van alle regio's. Daarmee is de VeRA geboren.

1.2 De VeRA als gezamenlijk vertrekpunt

De VeRA is de referentiearchitectuur voor veiligheidsregio's. Een referentiearchitectuur is een beproefd instrument om samenhang aan te brengen in de informatiehuishouding van een overheidssector en mogelijke samenwerking vorm te geven. De VeRA geeft regio's een richtlijn voor de inrichting van de integrale informatiehuishouding. Zonder informatiedeling kan de veiligheidsregio haar inwoners niet goed tegen risico's beschermen.

³ "Keten" in de zin van een netwerk van samenwerkingsverbanden.

Eerder (2008) heeft een werkgroep de Informatie Architectuur Sector Veiligheid opgesteld, de IASV. De IASV is een informatiearchitectuur specifiek voor de opgeschaalde situatie. De scope van de VeRA is breder dan de opgeschaalde situatie. In de VeRA worden producten opgeleverd die betrekking hebben op de bedrijfs- en informatiearchitectuur, op het niveau van de administratieve organisatie, de koude voorbereiding van inzet van hulpverlening en opgeschaalde crisisbeheersing binnen een veiligheidsregio en op het niveau van de landelijke voorzieningen zodat optimale informatiedeling kan plaatsvinden. Bij het opstellen van de VeRA is rekening gehouden met de IASV.

Een Veiligheidsregio heeft vanuit bedrijfskundig perspectief een aantal bijzondere kenmerken. Het is een ambtelijk-bureaucratische instelling met -onder het regime van verlengd bestuur- minstens twee en vaak drie lagen democratische verantwoording. Dit stelt hoge eisen aan de verantwoording en de transparantie van de besluitvorming. Het is een professionele organisatie in transitie van vakmanschap naar een 'machine bureaucracy'⁴ met steeds meer centraal georganiseerde ontwerptaken voor de professionele processen. Dit vergt veel van de organisatie op het gebied van standaardisatie en motivatie. Een Veiligheidsregio is bij een incident een flexibele commando-gevoerde top-down uitvoeringsorganisatie. De in de wet vastgelegde factor tijd speelt daarbij een belangrijke rol qua leiding en coördinatie, dekking, aanrijtijden en het totaalbeeld op het gebied van informatiemanagement. Het merendeel van de dagdagelijkse taken van een Veiligheidsregio bestaat echter uit het voorbereiden op deze incident- en crisissituatie. De preventieve, preparatieve fase en de onderhandelingen over de opgeschaalde situatie hebben een sterk

⁴ Volgens Henry Mintzberg.

netwerkkarakter en doen een beroep op de netwerkvaardigheden van de medewerkers.

Van oudsher hanteert men het onderscheid 'Koud' en 'Warm', en 'Mono' en 'Multi' om de werkzaamheden van een Veiligheidsregio aan te geven en te organiseren. Vanuit het perspectief van informatiedeling werkt deze indeling een verregaande fragmentatie in de hand. Voor de VeRA wordt uitgegaan van een keten- en netwerkperspectief en ligt de focus op een gebiedsgerichte en objectgerichte aanpak. De visie op informatiemanagement is dat de informatie over een object, zoals een school, een kinderdagverblijf, een tunnel of een schip voor alle partijen in de keten proportioneel gedeeld moet kunnen worden. Dit geldt voor koud, warm, Mono, Multi en de verschillende actoren in de regio.

De doelstelling van de VeRA is het bevorderen van de samenwerking tussen veiligheidsregio's onderling en met ketenpartners, door het benoemen van generieke elementen in de informatiehuishouding van veiligheidsregio's. Omdat de veiligheidsregio's erg van elkaar verschillen qua inrichting, richt de VeRA zich juist op de gemeenschappelijke kenmerken, principes en uitgangspunten. Via 'praatplaten' helpt de VeRA beslissers op het gebied van informatiemanagement, informatiemanagers, architecten en inhoudelijk specialisten om het gesprek aan te gaan. De VeRA richt zich nadrukkelijk op deze eerste twee groepen betrokkenen.

Informatiemanagers en -architecten in veiligheidsregio's kunnen de VeRA ook als basis gebruiken om intern een bedrijfsreferentiearchitectuur op te stellen. Dit helpt bij het standaardiseren van initiatieven op het gebied van informatiearchitectuur binnen de veiligheidsregio's, wat samenwerking

vereenvoudigt.

Concreet kunnen veiligheidsregio's de VeRA toepassen bij het:

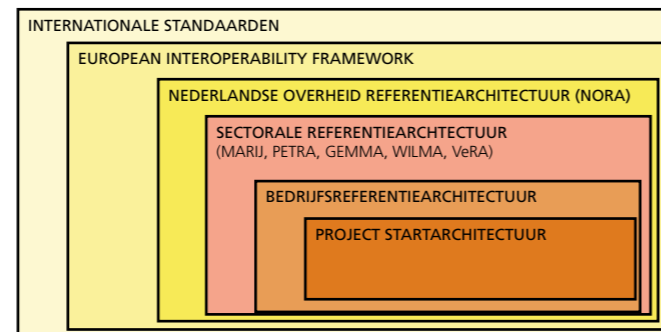
- Vormgeven van samenwerking tussen veiligheidsregio's;
- Inrichten van informatie-uitwisseling met ketenpartners;
- Bediscussiëren van informatieketens in de organisatie;
- Inrichten van het gebruik van basisregistraties;
- Kiezen van sectorale of regionale oplossingen voor informatievoorzieningen;
- Kiezen van landelijke voorzieningen;
- Aanschaffen van software;
- Opstellen van bestekken voor aanbestedingen;
- Opstellen of geven van opleidingen rondom informatiemanagement¹;
- Indelen van beheertaken.

De VeRA omvat brandweer en GHOR, de bijbehorende meldkamerprocessen en de ondersteunende afdelingen. De politie valt organisatorisch buiten de veiligheidsregio's; zij is daarom geen onderdeel van de scope van de VeRA. Ook de GGD is geen onderdeel van de VeRA. De GGD heeft een eigen referentiearchitectuur (PURA). Op dit moment is de meldkamer nog een onderdeel van een Veiligheidsregio. In de nabije toekomst zullen de activiteiten van de meldkamer overgaan naar de Landelijke Meldkamer Organisatie (LMO). De LMO wordt daarmee ketenpartner en de daarbij behorende bedrijfsfuncties, producten, bedrijfsprocessen etc. zullen moeten gaan aansluiten op de architectuur van de LMO.

¹ Hiermee wordt niet het operationele informatiemanagement bedoeld.

1.3 De VeRA in groter verband

De VeRA is een uitwerking van de Nederlandse Overheid Referentie Architectuur (NORA). De NORA bevat inrichtingsprincipes, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid. Het accent ligt daarbij op het mogelijk maken van samenwerking tussen overheidsorganisaties in ketens en netwerken. Onder de NORA bestaan een aantal sectorale referentiearchitecturen, zoals de EAR (Enterprise Architectuur Rijksoverheid), PURA (Publieke gezondheid Referentie Architectuur), PETRA (Provinciale EnTerprise Referentie Architectuur), GEMMA (GEMEentelijke Model Architectuur) en WILMA (Waterschap Informatie Logisch Model Architectuur). De VeRA hoort ook in dit rijtje thuis. De sectorale referentiearchitecturen zijn landelijke referentiemodellen waarin de generieke aspecten van een bepaalde sector beschreven worden en die de basis vormen voor eigen bedrijfsarchitecturen. Als een organisatie werkt onder architectuur, dan wordt per project een project-startarchitectuur (PSA) opgesteld die is afgeleid van de bedrijfs-referentiearchitectuur.



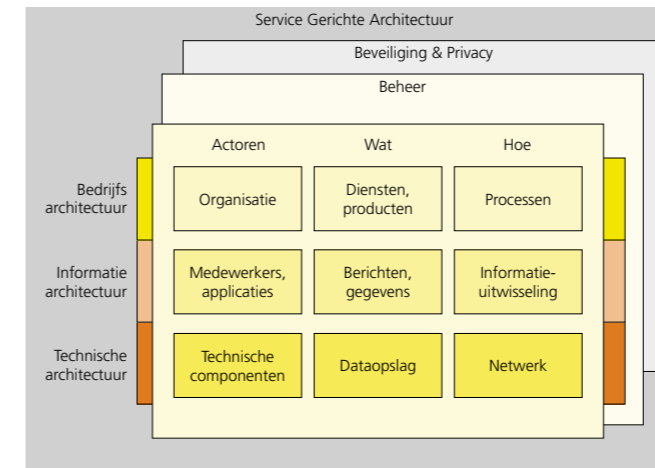
Figuur 1.1. Hiërarchie van architecturen

1.4 De architectuurproducten van de VeRA

Als verfijning van NORA gebruikt de VeRA hetzelfde architectuurraamwerk als NORA, zie figuur 1.2.

Het raamwerk heeft drie architectuurlagen: Bedrijfsarchitectuur, Informatiearchitectuur en Technische architectuur. Er zijn ook drie kolommen:

- Actoren: Wie neemt actie: organisaties, informatieverwerkers (personen en applicaties) en machines/computers;
- Wat: Wat wordt geleverd: diensten, berichten, gegevens
- Hoe: Hoe gebeurt dit: processen, communicatie, integratie en netwerk.



Figuur 1.2. Architectuurraamwerk NORA

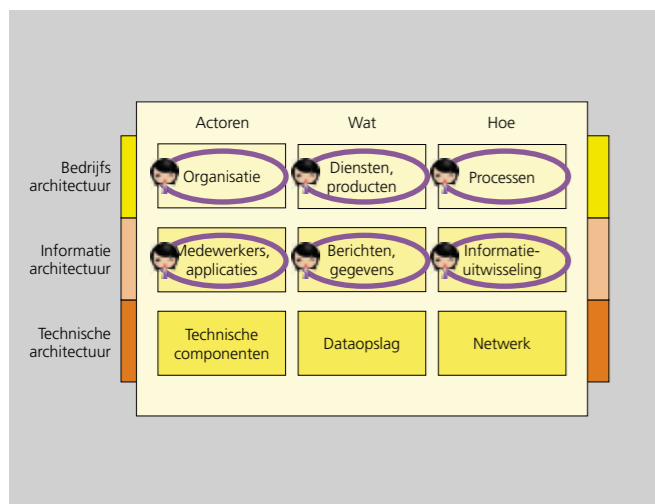
Organisaties werken met elkaar samen op basis van afspraken. Het moet daarom duidelijk zijn welke functie iedere organisatie heeft als onderdeel van de samenwerkende overheid. De diensten en producten die organisaties aan burgers en bedrijven leveren, zijn het resultaat van de samenwerking tussen organisaties (en van afdelingen). Diensten zijn het resultaat van bedrijfsprocessen.

Medewerkers voeren processen uit met behulp van applicaties. Berichten met gegevens zijn de (elektronische) documenten die in het kader van dienst- en serviceverlening worden uitgewisseld tussen medewerkers via applicaties. Informatie-uitwisseling vindt plaats met behulp van applicaties.

Technische componenten zijn machines of platforms waarop de applicaties en databases draaien. Gestructureerde data wordt opgeslagen in databases en ongestructureerde gegevens in een digitaal archief. Het netwerk verzorgt het fysieke transport van de berichten, informatie en data. Beheer, beveiliging en privacy hebben invloed op alle genoemde aspecten.

De VeRA beschrijft de volgende architectuurelementen:

- 1 Een set basisprincipes voor het inrichten van de informatieomgeving van de veiligheidsregio;
- 2 De bedrijfsarchitectuur laag;
- 3 De informatiearchitectuur laag.



Figuur 1.3. Architectuurraamwerk NORA met de invulling van de VeRA 2.0

Deze producten komen in de volgende hoofdstukken uitgebreid aan bod.

1.5 Domeinen

In de NORA is een Basisarchitectuur overheidsorganisaties vastgesteld. VeRA maakt hier, als verfijning van de NORA, ook gebruik van. Zie figuur 1.4.

De Basisarchitectuur bestaat uit de volgende domeinen:

- **Contacten:** hier worden de belangrijkste ketenpartners, leveranciers en/of klanten (lees: burgers en instellingen) van een overheidsorganisatie weergegeven.

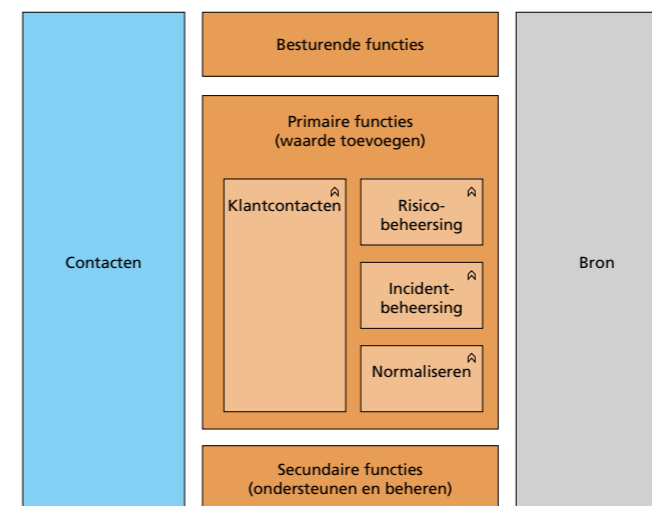
- **Besturende functies:** de bedrijfsfuncties in dit domein geven weer hoe de organisatie zichzelf richting geeft, zichzelf bijstuurt en zichzelf ontwikkelt.
- **Primaire functies:** de bedrijfsfuncties in dit domein gaan over het feitelijke werk van de organisatie. Deze functies leveren een directe bijdrage aan de producten en diensten die een organisatie levert. Met andere woorden: deze functies leveren primair de toegevoegde waarde van de organisatie. Ten behoeve van Veiligheidsregio's zijn deze primaire functies verder verfijnd in de categorieën: Klantcontacten, Risicobeheersing, Incidentbeheersing en Normaliseren (met uitzondering van Klantcontacten conform Aristoteles)
- **Secundaire functies:** hierbij gaat het om de zogenaamde PIOFACH¹-functies. Deze bedrijfsfuncties ondersteunen de overige bedrijfsfuncties en kunnen worden gezien als generieke functies die in elke willekeurige organisatie te herkennen zijn.
- **Bronnen:** Naast de domeinen waarbinnen bedrijfsfuncties worden onderkend en het contacten domein, is er ook een specifiek domein Bronnen. Het spreekt voor zich dat een bedrijfsfunctie gebruik maakt van gegevens. Sterker nog, de samenwerking tussen bedrijfsfuncties vindt voor een belangrijk deel plaats door uitwisseling van gegevens. De elementen in dit domein worden in hoofdstuk 4 nader gedefinieerd. Ook zal het belang van dit domein duidelijk worden bij de verdere uitwerking van de VeRA.

1.6 Leeswijzer

Dit document bestaat uit zes hoofdstukken. Hoofdstuk 2 beschrijft de visie op de informatievoorziening en de bijbehorende principes. In hoofdstuk 3

¹ PIOFACH is een acroniem dat alle bedrijfsvoering functies omvat: Personeel, Inkoop, Organisatie, Financiën, Automatisering, Communicatie en Huisvesting

wordt de bedrijfsarchitectuur beschreven in termen van bedrijfsfuncties, producten en processen. Hoofdstuk 4 geeft een beschrijving van de hierbij behorende informatiearchitectuur. Hoofdstuk 5 geeft richtlijnen voor een adequaat beheer van de informatiearchitectuur. Tot slot worden in hoofdstuk 6 de vervolgstappen beschreven: welke ambities hebben de opstellers van de VeRA nog; welke volgende stappen dienen in elk geval nog genomen te worden.



Figuur 1.4. Basisarchitectuur raamwerk VeRA (gebaseerd op raamwerk voor overheidsorganisaties)



2 Visie en principes

2.1 Inleiding

Principes zijn richtinggevende afspraken over de wijze waarop de gewenste situatie bereikt kan worden. Het is de bedoeling dat de mensen die zich bezighouden met de organisatie-inrichting zich aan deze principes houden. Binnen de NORA zijn veel principes opgesteld die te maken hebben met diensten en interoperabiliteit. Dit sluit aan bij het doel van de NORA: stimuleren van samenwerking tussen overheidsorganisaties.

In 2009 heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties het Informatiebeleid Veiligheid (IBV) opgesteld¹. Daarin zijn de volgende doelen geformuleerd:

- **Beter:** verbeteren prestatievermogen van de veiligheidssector door de juiste gegevens op de juiste tijd bij de juiste gebruiker te krijgen;
- **Robuust;** informatiesystemen zijn robuust juist bij rampen en crises; gegevensuitwisseling en communicatie mogen dan niet uitvallen;
- **Beheersbaar;** (informatiesystemen) implementeren in kleinere delen(modules); geen grand designs, grote masterplannen of grote systemen die nauwelijks te beheersen zijn;
- **Goedkoper;** gezamenlijk gebruik van informatievoorzieningen; niet steeds het wiel opnieuw uitvinden, maak gebruik van wat anderen al hebben ontwikkeld, eventueel door ze aan te passen aan de eigen situatie in plaats van dat ieder voor zich alles zelf ontwikkelt.

¹ Manifest Principes Informatiebeleid Veiligheid, opgesteld december 2009 door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bij het Informatiebeleid Veiligheid hoort een manifest met dertig principes, opgedeeld in de volgende categorieën: organisatie & bestuur, juridisch, financieel, beheersmatig, informatiekundig en technisch.

In de VeRA worden de principes benoemd voor de informatiehuishouding van een veiligheidsregio, met de principes uit NORA en IBV als leidraad. De VeRA wil inzicht en begrijpelijkheid toevoegen aan bovengenoemde doelen.

2.2 Visie

2.2.1 Visie op architectuur

De VeRA gaat uit van de volgende visie op architectuur:

Architectuur dient om de informatievoorzieningen van de veiligheidsregio in samenhang te laten werken voor de verschillende kolommen en situaties (administratief, warm en koud) om zo betere samenwerking binnen de eigen veiligheidsregio, tussen veiligheidsregio's en met ketenpartners te faciliteren.

2.2.2 Van eilandautomatisering naar informatiedeling

Bij veel veiligheidsregio's is elke applicatie als een eiland, met eigen gegevensopslag en met een eigen gebruikersinterface. De gebruikersinterfaces zijn ontworpen voor mensen die ze vaak gebruiken en missen de vanzelfsprekendheid die incidentele gebruikers nodig hebben om ermee overweg te kunnen. Koppelingen tussen de applicaties zijn vaak één-op-één opgezet en dragen alleen gegevens over, niet hun betekenis of een kwaliteitsaanduiding. Er is geen terugkoppeling als de

Eilandautomatisering



fromage!

kaas!

cheese!

Een analogie

De verschillen tussen eilandautomatisering, informatiedeling en geüniformeerde informatiedeling kunnen worden uitgelegd door middel van een analogie: het kopen van kaas.

Bij eilandautomatisering moet je voor elke soort kaas naar een daarin gespecialiseerde winkel. De winkels liggen op een afstand van elkaar en elke winkel heeft zijn eigen taal en gewoontes. Eigenlijk hebben de winkels niets met elkaar te maken.

geboden gegevens foutief blijken te zijn. Stuurinformatie is overwegend een bijproduct van de individuele applicaties en bestaat dus ook uit eilanden. We spreken hier van eilandautomatisering. Eilandautomatisering stimuleert gegevensdeling in en tussen veiligheidsregio's niet. Gegevens kunnen alleen gedeeld worden door applicaties voor anderen open te stellen of door (vaak dure

Informatiedeling



kaas!

fromage!

cheese!

Een analogie

Bij gegevensdeling kan je gewoon naar je eigen kaaswinkel gaan en daar allerlei soorten kaas kopen. Je hoeft niet de gewoonten van het land van herkomst van de kaas te kennen, je wordt altijd op dezelfde manier bediend, ongeacht welke kazen je koopt.

Maar de gegevens op de verpakking is in de taal en conform de gewoontes van het land van herkomst. Als je dat niet begrijpt heb je pech. En als je het wel begrijpt, dan kan je nog geen producten vergelijken, want op de Nederlandse kaas staat het vetpercentage, op de Engelse de streek en op de Franse de streek en welke kant van de heuvel de koeien grazen.

maatwerk) koppelingen tussen applicaties te bouwen. Hierbij neemt de complexiteit snel toe als er meer partijen betrokken raken. Vaak leiden deze obstakels ertoe dat gegevens uiteindelijk opnieuw ingevoerd worden in verschillende applicaties. Daarbij kennen de afnemers de kwaliteit van de gegevens vaak niet en is het melden van fouten bij de bron (terugkoppeling) meestal niet ingericht.

Eilandautomatisering is het logische gevolg van de manier waarop veel software is aangeschaft: een afdeling heeft een wens en zoekt software die daar zo goed mogelijk bij aansluit. Hierbij wordt vaak onvoldoende rekening gehouden met de informatievoorziening van de organisatie als geheel. Bij de veiligheidsregio's is dit heel herkenbaar bij applicaties die door gemeentelijke brandweerkorpsen werden gebruikt en bij de overgang naar de veiligheidsregio zijn 'meegenomen'.

Hoe het beter kan: Gegevensdeling

Gegevensdeling betekent dat een gebruiker precies die gegevens overzichtelijk gepresenteerd krijgt die hij nodig heeft voor zijn werk. Zonder dat de gebruiker het merkt worden gegevens uit meerdere gegevensbronnen opgehaald en weergegeven. Een goed voorbeeld van gegevensdeling is een informatie-infrastructuur zoals Google Earth, waarbij de gebruiker zelf kan aangeven welke gegevens hij op een kaart gepresenteerd wil zien. De complexiteit van de software kan beperkt blijven door gebruik te maken van webservices die voldoen aan de facto standaarden. De presenterende applicatie kan eenvoudig worden gehouden indien de applicatie niet alleen de gegevens overdraagt, maar daarbij ook vertelt hoe de gegevens gepresenteerd moet worden. Dat is hoe het werkt in de nieuwe standaard voor overheid-IT: webservices, conform de landelijke koppelvlakstandaard.

Bij gegevensdeling heeft de bronhouder een spilpositie: iedereen die zijn gegevens gebruikt moet deze bij hem ophalen. Constateert iemand een fout of een afwijking, dan moet die dat melden aan de bronhouder die hier vervolgens zorgvuldig mee moet omgaan. De bronhouder moet zorgen dat de gegevens die hij levert bruikbaar zijn voor afnemers, zowel inhoudelijk als technisch. Een voorbeeld van een bronhouder is de afdeling HRM die vaak het beheer voert over de personeelsgegevens die op veel plaatsen binnen de veiligheidsregio worden gebruikt, zoals bij het maken van het rooster.

Afnemende applicaties presenteren de opgehaalde gegevens, eventueel gefilterd en gesorteerd. Het kan bijvoorbeeld belangrijk zijn te filteren op alle bronnen van bluswater in een gebied en die vervolgens op een kaart te tonen. De presenterende applicatie moet bijvoorbeeld kunnen herkennen of een gegeven een bluswaterbron is en zo ja, waar deze zich bevindt. Standardisatie moet zorgen dat ondubbelzinnig duidelijk is hoe de applicatie dit moet doen. De bronhouder moet kwaliteitsaanduidingen meegeven met de gegevens, zodat de afnemer zelf een oordeel over de kwaliteit kan vormen (actualiteit, nauwkeurigheid).

Als een applicatie gekoppeld is met een andere en er wijzigt iets in de programmatuur, dan is de kans groot dat de andere applicatie of de koppeling ook gewijzigd moet worden. Een groot voordeel van gegevenskoppelingen is dat de betrokken applicaties kunnen wijzigen zonder elkaar 'last' te bezorgen, zolang de koppeling maar ongewijzigd blijft.

Gegevensdeling ondersteunt samenwerking in en tussen regio's en hun partners. De veiligheidsregio kan gegevens, zoals actuele operationele gegevens, delen met elke partner die webservices conform de overheidsstandaarden toepast. Als meer partijen aansluiten neemt de complexiteit niet toe; de architectuur geeft deze flexibiliteit. Het maakt daarbij niet uit of de partijen dezelfde applicaties gebruiken, als er maar overeenstemming over de gegevens is.

Er worden in toenemende mate eisen gesteld aan bedrijfsvoering en hulpverlening. Deze eisen worden ondersteund doordat de medewerkers toegang tot meer gegevens krijgen, terwijl de kwaliteit van deze gegevens beter geborgd is en inzichtelijker is. Dat geldt voor zowel de bedrijfsvoering zelf als de sturing daarvan. De initiële kosten worden beheersbaar gehouden omdat er minder afspraken gemaakt

Geüniformeerde informatiedeling



Nederlandse kaas!

Franse kaas!

Engelse kaas!

Een analogie

Bij geüniformeerde informatiedeling is ook de informatie over de kaas geüniformeerd. Van elke kaas is het vetpercentage en de streek weergegeven. Op welke kant van de heuvel de Franse koeien grazen is niet meer te achterhalen. Dat vinden wij niet erg, wij hebben met elkaar afgesproken dat deze informatie niet nodig is.

hoeven te worden en omdat deze afspraken relatief eenvoudig kunnen zijn. De terugkerende kosten zijn lager omdat de meeste aanpassingen van de applicaties van partners geen aanpassing van eigen applicaties vergt. Gegevensdeling is het logische gevolg van de verandering van focus op applicaties naar focus op gegevens. Moderne technieken als webservices en semantiek dragen hieraan bij. In selectietrajecten krijgen functionaliteit en koppelbaarheid evenveel waarde toegekend.

Geüniformeerde gegevensdeling

Om gegevens te delen wordt de betekenis en de codering van de gegevens slechts geüniformeerd voor zover dat nodig is voor eenvoudige selecties en ordening. In de huidige situatie zien we dat bronnen verschillende keuzes maken. Om een voorbeeld te geven, waterleidingbedrijf A geeft van een brandkraan de XY-coördinaten en de waterdruk aan, terwijl waterleidingbedrijf B de XY-coördinaten, de minimale en de maximale waterdruk en de locatie van de pompinstallatie levert. Bij geüniformeerde informatiedeling worden er afspraken gemaakt over welke gegevens op welke wijze wordt gedeeld.

2.3 Principes

Architectuurprincipes dragen bij aan de visie op de informatievoorziening. Principes zijn richtinggevende afspraken die een overtuiging weergeven over de wijze waarop de gewenste situatie (de visie) bereikt kan worden.

Binnen de NORA is een groot aantal principes opgesteld met als focus diensten en interoperabiliteit. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft voortgeborduurd op NORA 2.0 met het Informatiebeleid Veiligheid (IBV). Met dit informatiebeleid wordt gestreefd naar een betere informatievoorziening voor individueel en gemeenschappelijk optreden van veiligheidspartners. Bij het Informatiebeleid Veiligheid hoort een manifest met principes. De belangrijkste principes voor de VeRA staan hieronder benoemd en toegelicht. Ze zijn gerubriceerd conform het architectuurraamwerk van NORA. Voor de beveiliging- en privacyprincipes heeft het beveiligingskatern van NORA als basis gediend.

2.3.1 Informatiekundige architectuurprincipes

IA.1 Gebruik gemeenschappelijke modulaire systemen

Veiligheidspartners maken gebruik van gemeenschappelijk ICT-aanbod indien functionaliteit, beveiliging en kosten gelijkwaardig zijn.

Uit het oogpunt van efficiency en kwaliteit verdient het immers de aanbeveling om zoveel mogelijk gemeenschappelijke modulaire systemen te gebruiken die aansluiten op de benoemde applicatieve functies. Oftewel: bestaande functionaliteit dient zoveel mogelijk hergebruikt te worden. Hergebruik van functionaliteit gaat versnippering van voorzieningen tegen.

De voorkeur wordt in eerste instantie gegeven aan standaardpakketten van de markt (mits voor en door ons te configureren) gevolgd door maatwerk. Bij maatwerk wordt de voorkeur gegeven aan maatwerk ontwikkeld voor meerdere Veiligheidsregio's boven regionaal maatwerk.

IA.2. Gegevens hebben één (herleidbare) bron

Partijen stellen eigen gegevens ter beschikking aan anderen. Eigen gegevens zijn samenhangende sets van oorspronkelijke gegevens, al dan niet gecombineerd met gegevens van derden.

Op deze manier verbetert de kwaliteit van de gegevens in de keten. Het beheren van dezelfde gegevens op meerdere plekken leidt tot verschillen in gegevens binnen de organisatie. Dit vermindert de kwaliteit en integriteit van de processen en de dienstverlening aan klanten. Gegevens die gebruikt worden in meerdere processen, worden zoveel mogelijk op één centrale plek beheerd (de authentieke bronregistratie). Deze gegevens zijn leidend. De gegevens kunnen decentraal worden hergebruikt.

Gegevens komen zoveel mogelijk van een authentieke bron of bij een gemeenschappelijk distributiepunt. Een Veiligheidsregio maakt gebruik van basisregistraties en identificeert haar kernregistraties van waaruit de verschillende informatiesystemen worden ondersteund. Dit is één van de belangrijkste basisprincipes binnen de VeRA en volgt hiermee ook het verplicht gebruik van basisregistraties voor de publiekrechtelijke taken van overheidsinstanties en het gebruik van kernregistraties binnen een Veiligheidsregio. De VeRA volgt het principe van basisregistraties: eenmalige vastlegging, meervoudig gebruik.

IA.3 Gegevens hebben een verantwoordelijke

De gebruikers van gegevens moeten er op kunnen vertrouwen dat de gegevens aangeleverd door applicaties correct zijn. Alleen gegevens waarvan een verantwoordelijke is aangewezen worden uitgewisseld tussen veiligheidspartners.

Correcte gegevens zijn cruciaal in alle processen en daarom van vitaal belang voor de Veiligheidsregio's. Alle gegevensverzamelingen dienen daarom een verantwoordelijke te hebben, die zorg draagt voor de betrouwbaarheid van de gegevens in termen van actualiteit, beschikbaarheid, juistheid, tijdigheid en volledigheid van de gegevens. Deze is aanspreekbaar op de kwaliteit van de gegevens.

Veiligheidsregio's moeten normen vaststellen voor de gewenste kwaliteit van gegevens. Deze wordt als norm vastgesteld en bekendgemaakt. Vervolgens moeten er processen worden ingericht om de norm te handhaven en er wordt gerapporteerd over de behaalde resultaten. Waar de kwaliteit kan variëren, wordt bij de informatie vermeld wat het actuele kwaliteitsniveau is (bijvoorbeeld wanneer de informatie voor het laatst is gecontroleerd).

IA.4. Gebruik open standaarden (voor gemeenschappelijke voorzieningen)

De Veiligheidsregio gebruikt zoveel mogelijk gemeenschappelijke voorzieningen die koppelvlakken bieden op basis van open standaarden of de facto standaarden.

De Veiligheidsregio hanteert open standaarden en richtlijnen om haar informatievoorziening in te richten. Open standaarden spelen een belangrijke rol in het verbinden van (modulaire) bedrijfsfuncties en applicatieve functies en maken uitwisseling (koppelvlakken) van gegevens tussen veiligheidspartners eenvoudiger. Het gebruik van open standaarden voorkomt dat elke veiligheidsregio afzonderlijk oplossingen bedenkt voor generieke vraagstukken. Open standaarden dragen tevens bij aan interoperabiliteit (uitwisselbaarheid). Open standaarden verbeteren de digitale communicatie tussen overheden onderling en ook tussen overheid, bedrijven en burgers. Daarnaast zorgen open standaarden ervoor dat keuzevrijheid is geborgd. Open standaarden zijn naar hun aard namelijk niet software specifiek en kunnen door iedere leverancier worden ingebouwd.

Het generieke koppelvlak dat voor in gebruik zijnde systemen toegang biedt tot de gemeenschappelijke informatievoorziening, biedt in ieder geval ook een 'open' toegangswijze. Systemen die al een koppelvlak hebben naar de overheid service bus moeten deze kunnen hergebruiken voor toegang tot de gemeenschappelijke informatievoorziening.

2.3.2 Beveiliging en Privacy architectuurprincipes

BP.1 Gegevens moeten worden uitgewisseld, tenzij...

Gegevens worden uitgewisseld tussen veiligheidspartners, ook internationaal conform vigerende wetgeving.

Vrije uitwisselbaarheid van gegevens en kennis ligt aan de basis van een crisisbeheersingsorganisatie. Bij de uitwisseling van gegevens dient rekening gehouden te worden met het wettelijke kader en de noodzakelijke daarvan afgeleide vertrouwelijkheid van gegevens. De informatieorganisatie dient hier zoveel mogelijk in te faciliteren. Dit uitwisselen van gegevens is belangrijk binnen de verschillende kolommen van één veiligheidsregio, maar ook tussen de verschillende veiligheidsregio's en met andere ketenpartners.

Veiligheidspartners stellen geen extra voorwaarden aan gegevensuitwisseling met veiligheidspartners in andere landen en met andere internationale organisaties zolang deze gegevensuitwisseling geschiedt binnen de kaderstelling van nationale en internationale verdragen, de vigerende wet- en regelgeving, de bestuurlijke en verantwoordelijkheidslijnen, of in het geval dat het belang van de operationele taakuitvoering wordt geschaad. De leverende partner moet erop kunnen vertrouwen dat de Veiligheidsregio deze gegevens beheert conform het vertrouwelijkheidsniveau dat hier volgens de aanleverende partij voor geldt.

Bij het ontvangen van gegevens van externe partijen dient vastgelegd te worden wat de vertrouwelijkheid is van de gegevens en de Veiligheidsregio dient te borgen dat deze regels gehandhaafd worden. Gegevens kunnen ingedeeld worden in vijf niveaus van vertrouwelijkheid¹ en worden beheerd conform deze classificaties. Gegevens worden niet langer bewaard dan noodzakelijk.

¹ Zie https://nl.wikipedia.org/wiki/Geclassificeerde_informatie_voor_de_vijf_niveaus.

2.3.3 Beheer principes

B.1. Zorg voor systemen die in alle omstandigheden bruikbaar zijn

De veiligheidspartners gebruiken onder normale en bijzondere omstandigheden (crisissituatie) dezelfde systemen. Op deze manier zullen gebruikers voldoende ervaring hebben in het gebruik van systemen doordat zij de systemen onder normale omstandigheden en dus vaker gebruiken.

Dit principe betekent dat dezelfde informatiesystemen zowel in koude als warme situaties gebruikt moeten worden. Informatiesystemen en bijbehorende beheerorganisaties zijn hiervoor 24x7 beschikbaar. Dit stimuleert ketenintegratie tussen bedrijfsvoering, preparatie en crisisbeheersing.

B.2 Eis hoge beschikbaarheid tijdens buitengewone omstandigheden

Systemen worden alleen gebruikt als er een hoge mate van zekerheid is dat de noodzakelijke beschikbaarheid en capaciteit van de systemen beschikbaar is, ook in buitengewone omstandigheden. De meeste informatiesystemen worden niet alleen gebruikt onder normale omstandigheden, maar ook in ramp- en crisissituaties. Daarom moeten deze bijvoorbeeld ook werken buiten kantooruren, vanaf niet-traditionele werkplekken (bijvoorbeeld op mobiele apparaten) en bestand zijn tegen onverwachte situaties. Kortom een schaalbare, flexibele en beschikbare informatievoorziening.

De implicatie is dat dit principe eisen stelt aan systemen en aan beheerafspraken waarbij rekening wordt gehouden met de onderliggende keten van afhankelijkheden (locatie, netwerk, koeling, stroomvoorziening, enz.)

2.3.4 Service gerichte architectuurprincipes

S.1. Verricht nieuwbouw volgens service gerichte architectuur

De architectuur voor nieuwe informatievoorzieningen is opgebouwd volgens Service Gerichte Architectuur. Een servicegerichte architectuur maakt een strikt onderscheid tussen functionaliteit en gegevensopslag. De architectuurproducten 'Bedrijfsfuncties' en 'Applicatieve functies' in VeRA ondersteunen dit principe.

Voor gegevensuitwisseling over de grenzen van bedrijfsfuncties heen worden uitsluitend services gebruikt. Deze services maximaliseren de onderlinge uitwisselbaarheid (interoperabiliteit), terwijl de afhankelijkheid geminimaliseerd wordt. Applicaties respecteren de grenzen van de onderkende bedrijfsfuncties. Applicaties werken niet over grenzen van bedrijfsfuncties heen. De veiligheidsregio's houden in hun implementatiestrategie voor de aanbesteding en inkoop rekening met de voorkeur voor 'service oriented' ontwikkelde software. Servicegerichte architectuur sluit aan op internationale standaarden voor applicatieontwikkeling en NORA (NORA 2.0, § 4.3.2).

S.2. Gegevens worden tijdig gepresenteerd, en alleen gerelateerd aan het beoogde doel

Gegevens worden op een begrijpelijke, consistente en herkenbare wijze gepresenteerd, overeenkomstig de daarvoor geldende richtlijnen. Dit gebeurt in lijn met de aard van de data, de context waarin deze worden gepresenteerd en rekening houdend met de beoogde doelgroep. Het tijdig presenteren van de gegevens is een aanvulling die van specifiek belang is voor de veiligheidsregio's. Immers: hoe sneller de gegevens beschikbaar zijn des te beter kan een incident of crisis effectief bestreden worden.

Gebruikers zien in eerste instantie alleen die gegevens die voor hen van belang zijn voor de uitoefening van de functie of taak. Een gegevens overkill wordt hiermee vermeden. Een portal ondersteunt het geïntegreerd presenteren van gegevens, functionaliteiten en generieke functionaliteiten. Het zorgt voor integratie op het niveau van de presentatie. Gegevens en functionaliteit uit verschillende applicaties wordt dan geïntegreerd aan de gebruiker gepresenteerd.



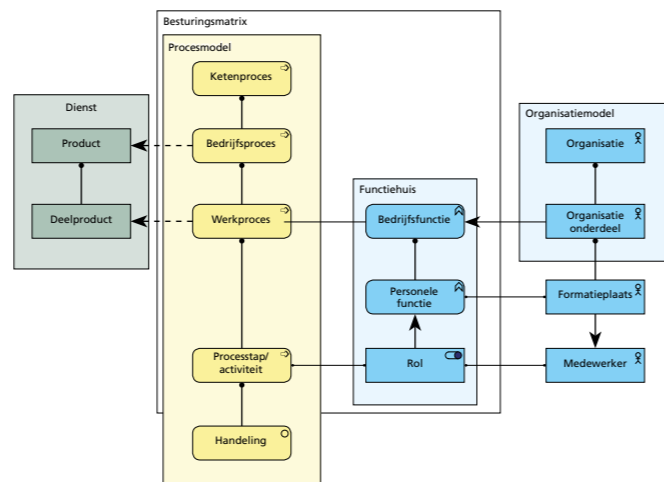
3 Bedrijfsarchitectuur

Dit hoofdstuk gaat in op de bedrijfsarchitectuur van de Veiligheidsregio's zoals die is vastgelegd in de VeRA. De bedrijfsarchitectuur wordt beschreven vanuit drie verschillende perspectieven, te weten: Producten en Diensten, Bedrijfsfuncties en Bedrijfsprocessen.

In zijn algemeenheid kunnen organisaties enerzijds beschreven worden in termen van bepaalde bedrijfsfuncties (inkoop, productie, verkoop) en anderzijds in bedrijfsprocessen gericht op de levering van een product of dienst. Om een product te kunnen leveren wordt allereerst de bedrijfsfunctie inkoop aangeroepen, vervolgens worden de aangekochte grondstoffen door de functie productie omgezet in een product. Het product wordt vervolgens verkocht door de functie verkoop.

Een bedrijfsproces ('het hoe') leidt tot de productie van een product of dienst (het 'wat') en roept hierbij meerdere bedrijfsfuncties aan. Anders gezegd; welke bedrijfsfuncties worden in welke volgorde (bedrijfsprocessen) ondernomen om een product of dienst te leveren.

In figuur 3.1 is grafisch weergegeven hoe processen en bedrijfsfuncties aan elkaar gerelateerd zijn. De essentie is dat een bedrijfsproces één of meerdere bedrijfsfuncties aanroept om een product of dienst te leveren. Tevens wordt duidelijk wat de gelaagdheid is van een procesmodel. Ook wordt de samenhang tussen het organisatiemodel en het functiehuis aangegeven. Kortom, dit is een metamodel van organisaties.

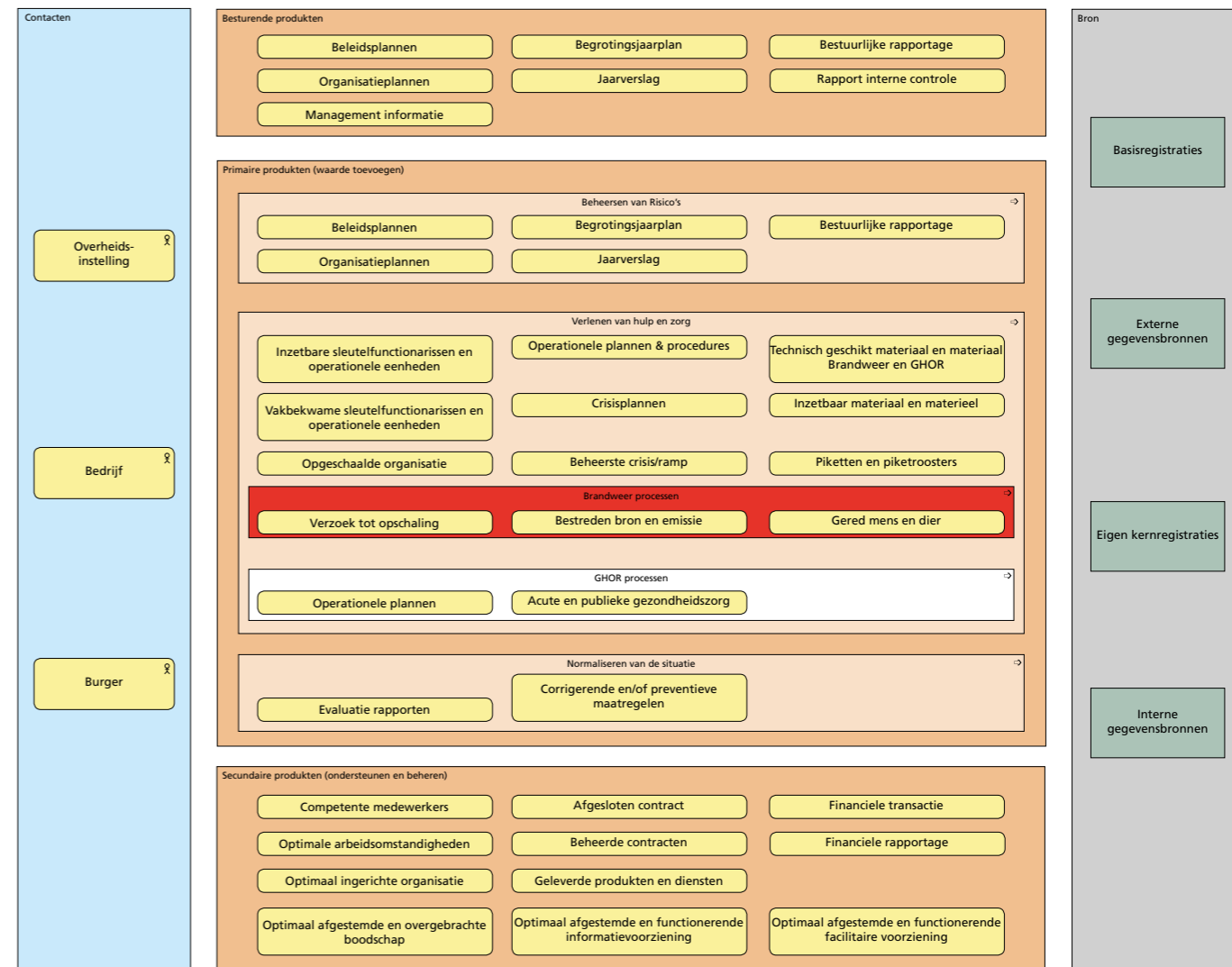


Figuur 3.1. Samenhang functies, processen en organisatie (Uit: "Bedrijfsarchitectuur, werken aan een samenhangende bedrijfsinrichting", G. Bayens e.a.)

3.1 Producten en diensten

3.1.1 Wat zijn Producten en diensten

Producten en diensten zijn feitelijk de bestaansreden van een organisatie. Zonder een duidelijke behoefte aan de geleverde producten en diensten zal een private onderneming geen inkomsten kunnen genereren. Voor overheidsorganisaties ligt dit anders. Vaak leveren zij producten en diensten waar een wettelijke taak aan ten grondslag ligt. Maar ook hier geldt dat zodra deze wettelijke taak wegvalt, de noodzaak voor het leveren van de producten en diensten ook wegvalt.



Figuur 3.2. producten en diensten van een veiligheidsregio

Voor veiligheidsregio's zal er een bestaansreden zijn zolang er sprake is van de kans op fysieke onveiligheid. Wat wel aan verandering onderhevig is (onder andere als gevolg van gewijzigde wetgeving), is welke producten en diensten zij leveren om de maatschappelijk gewenste fysieke veiligheid zo goed mogelijk te borgen. Veiligheidsregio's kunnen producten en diensten bijvoorbeeld gebruiken om op eenduidige wijze de productbegroting op te stellen, alle documenten te beheren rond een bepaald product of ten behoeve van business intelligence (analyse t.b.v. bedrijfsontwikkeling).

3.1.2 Producten en diensten van een veiligheidsregio

In figuur 3.2 zijn de producten en diensten van een veiligheidsregio in relatie tot de bedrijfsprocessen gevisualiseerd.

3.1.3 Beschrijving van de producten en diensten van de veiligheidsregio's

Het overzicht op de volgende pagina toont de producten en diensten -met eventuele toelichting- in relatie tot het bedrijfsproces dat het desbetreffende product of dienst levert.

Besturende producten en diensten

Producten en diensten	Bedrijfsproces	Toelichting
Beleidsplannen Organisatieplannen	Beleid vormen	Er zijn 3 verplichte planfiguren (regionaal risicoprofiel, regionaal crisis beleidsplan, regionaal crisisplan) waarvan het beleidsplan en het crisisplan uit dit bedrijfsproces komen. Ook het dekkingsplan komt voort uit dit proces
Bestuurlijke rapportage Begroting/jaarplan Jaarverslag Rapport interne controle Management informatie	Sturen, beheersen en verantwoorden	Binnen dit bedrijfsproces hoort ook de aandacht voor de organisatorische risicoanalyse (risk management). Het is goed om te realiseren dat het rapport interne controle dus maatregelen kan opleveren voor de bijsturing van elk ander proces Management informatie is er op vele niveaus maar hier gaat het vooral over de organisatie-brede stuurinformatie

Primaire producten en diensten - Risicobeheersing

Producten en diensten	Bedrijfsproces	Toelichting
Risicoprofielen	Analyseren van risico's	Onder andere het Regionaal risicoprofiel en het Brandrisicoprofiel
Advies fysieke veiligheid Advies tot handhaving	Verlenen van adviezen	Verschillende beredeneerde aanbevelingen aan bevoegd gezag om een bepaalde keuze te maken, veelal in de vergunningsverlening
Uitgevoerd toezicht	Toezicht houden	De verzamelde informatie over de vraag of een object of evenement voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel en het eventueel naar aanleiding daarvan adviseren van bevoegd gezag (Advies tot handhaving)
Voorgelichte burger / instelling	Communiceren over risico's	Het gaat hier vooral over alle activiteiten rondom het thema Brandveilig leven. Hieronder kan ook het voorlichten van omwonenden vallen kort na een incident. Materieel en materiaal (rook cabine) en ontwikkelen communicatiemateriaal wordt uit de betreffende bedrijfsprocessen betrokken.

Primaire producten en diensten - Incidentbestrijding

Producten en diensten	Bedrijfsproces	Toelichting
Piketten en piketroosters Inzetbare sleutelfunctionarissen en operationele eenheden Inzetbaar materiaal en materieel	Organiseren van operationele beschikbaarheid	Inzetbaarheid gaat over de logistieke planmatige kant
Vakbekwame sleutelfunctionarissen en operationele eenheden	Vakbekwaam worden en blijven	
Crisisplannen, operationele plannen & procedures	Opstellen operationele plannen & procedures	Actuele rampenbestrijdingsplannen, incidentbestrijdingsplannen, bereikbaarheidskaarten, aanvalsplannen, calamiteitenplannen, handboeken en operationele procedures Let op: er vindt nadrukkelijk informatie-uitwisseling plaats met Adviseren rondom objectgegevens. Dit is echter een ander beschouwingsniveau: informatiearchitectuur versus bedrijfsarchitectuur
Technisch geschikt materieel en materiaal Brandweer en GHOR	Beheer en onderhoud brandweer & geneeskundig specifieke hulpmiddelen	
Verantwoordelijkheidsafspraken en totaalbeeld betrokken objecten	Vorbereiden op opgeschaalde situatie	Bepaling wie waar voor verantwoordelijk is (taakverdeling en regievoering binnen de keten)

Beheerste crisis/ramp	Besluitvorming t.b.v. multidisciplinaire crisisbeheersing/ rampenbestrijding	
Bestreden bron of emissie Verzoek tot opschaling	Bestrijden van brand en emissie gevaarlijke stoffen	Beperken van economische schade, in stand houden vitale infrastructuur en beperken van milieu effect schade
Gered mens en dier Verzoek tot opschaling	Redden en technische hulpverlening	
Operationele plannen Gemaakte afspraken (convenanten)	Regisseren geneeskundige opgeschaalde zorg	
Acute en publieke gezondheidszorg	Coördineren geneeskundige opgeschaalde zorg	

Primaire producten en diensten - Normaliseren

Producten en diensten	Bedrijfsproces	Toelichting
Evaluatierapport Corrigerende en/of preventieve maatregelen	Evalueren van hulp en zorgverlening	

Secundaire producten en diensten

Producten en diensten	Bedrijfsproces	Toelichting
Competente medewerkers Optimale arbeidsomstandigheden Optimaal ingerichte organisatie	Personeelsmanagement	Zorgen voor personeel en organisatie. Instroom, doorstroom, uitstroom medewerkers. Goede arbeidsvoorwaarden en arbeidsomstandigheden. Opleiding en training. Voeren van een personeelsadministratie: beheer van alle gegevens, informatie en kennis over medewerkers. BOT valt hier ook onder als werkproces
Afgesloten contract Geleverde producten en diensten Beheerd contract	Inkoop en contractmanagement	
Financiële transactie Financiële rapportage	Financieel management	
Optimaal afgestemde en functionerende informatievoorziening	Informatie & ICT management	
Optimaal afgestemde en overgebrachte boodschap	Communicatie management	
Optimaal afgestemde en functionerende facilitaire voorziening	Facilitair management	

3.2 Bedrijfsprocessen



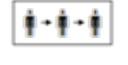

3.2.1 Wat zijn bedrijfsprocessen?

Bedrijfsprocessen verbinden de bedrijfsfuncties aan elkaar om een product of een dienst te leveren. Zij vormen daarmee een logisch geheel van activiteiten van begin tot eind die moeten worden uitgevoerd om het gewenste resultaat (product of dienst) te bereiken.

De definitie van een bedrijfsproces is:

Een bedrijfsproces is een geordende reeks werkprocessen die binnen één organisatie wordt uitgevoerd met als doel om een (combinatie van) dienst(en) te leveren aan een burger, bedrijf of andere organisatie.⁹

Voor het leveren van producten en diensten zijn processen nodig. Processen zijn een samenhangende set van activiteiten die op basis van een trigger (input) een product en/of dienst (output) leveren. Vaak zijn er meerdere competenties (bedrijfsfuncties) nodig om in één proces te komen tot een product of dienst. Ook is er sprake van processen op verschillende abstractieniveaus (zie figuur 3.2). Op het hoogste niveau kan er sprake zijn van ketenprocessen waarbij meerdere organisaties samenwerken om één product of dienst te leveren. Binnen organisaties zijn bedrijfsprocessen het hoogste niveau van definitie (zie ook paragraaf 3.1. voor de definitie van een bedrijfsproces). Op het niveau van werkprocessen zal er veel meer sprake zijn van lokale verschillen in scope, werkwijze, etc. Om die reden zullen in deze referentiearchitectuur enkel de bedrijfsprocessen worden beschreven. Zoals in figuur 3.3 is weergegeven worden processen vaak in een hiërarchie beschreven.

Niveau	Beschrijving	Voorbeeld
	Ketenproces Een geordende reeks services die door verschillende organisaties aan elkaar worden geleverd met als doel om via één organisatie een (combinatie van) dienst(en) te leveren aan een klant.	Verstrekken vergunning (verschillende belanghebbenden)
	Bedrijfsproces Een bedrijfsproces is een geordende reeks werkprocessen die binnen één organisatie wordt uitgevoerd met als doel om een (combinatie van) dienst(en) te leveren aan een burger, bedrijf of andere organisatie.	Verstrekken vergunning
	Werkproces Een werkproces is een geordende reeks van processtappen die binnen één organisatorische eenheid binnen een organisatie wordt uitgevoerd met als doel een specifieke bijdrage (prestatie) te leveren aan een dienst die uiteindelijk zal worden geleverd aan een burger, bedrijf of andere organisatie.	Intake
	Processtap Een geordende reeks handelingen die ononderbroken wordt uitgevoerd door één mens of machine (eenheid van tijd, plaats en handelen).	Registreren Zaak
	Handeling Kleinste mogelijke eenheid van werk, uitgevoerd door één persoon of machine op één plek op één moment.	Vul zaak nummer in

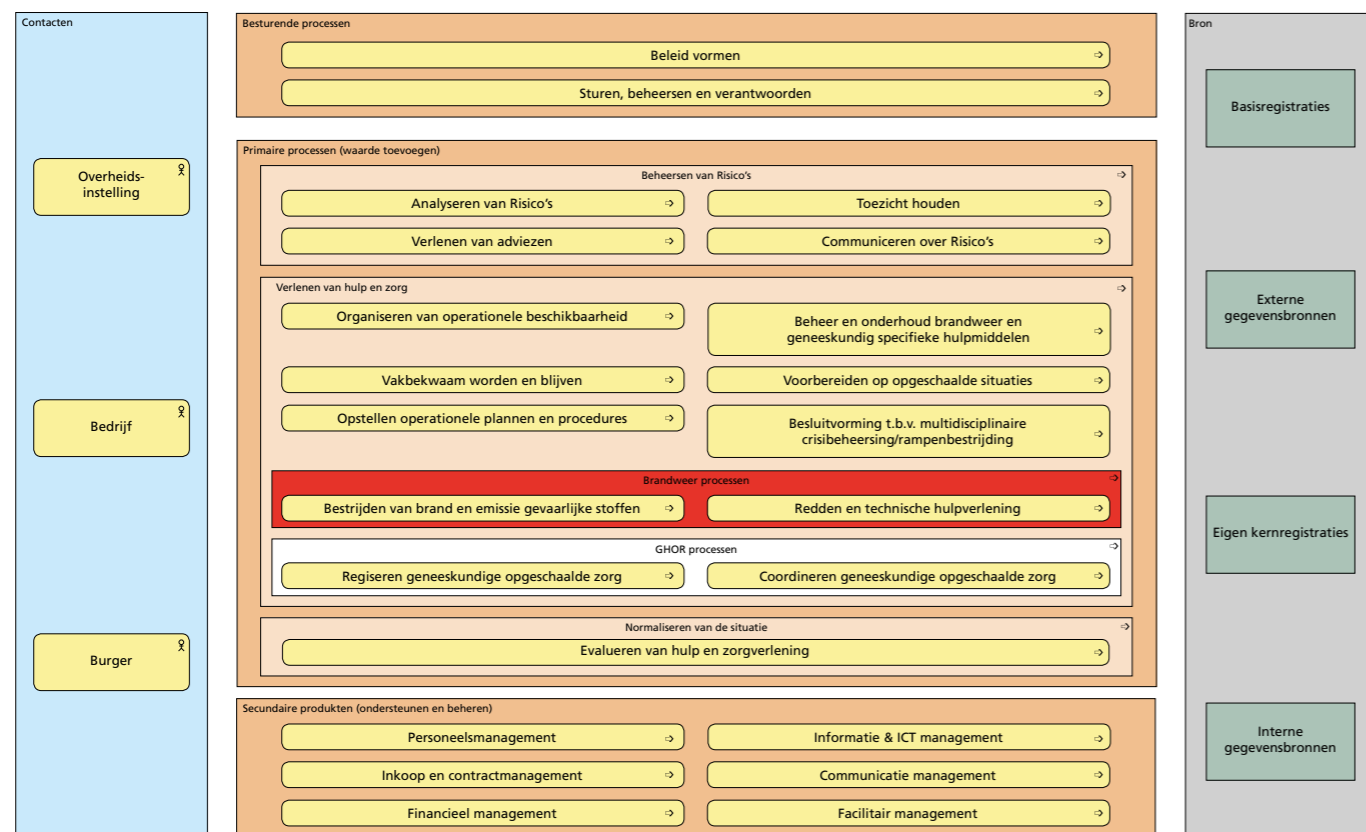
Figuur 3.3. Definities van een proces hiërarchie. Bron: Bayens & Tonissen

3.2.2 Relaties met andere (procesgerichte) kaders

Binnen zowel Brandweer NL als GHOR NL zijn al eerder kaders beschreven die betrekking hebben op processen. Dit betreft zowel procesdefinities als indicatoren (normen) die verwijzen naar mogelijke processen. Om recht te doen aan deze kaders is er in de bijlage een verwijzing opgenomen naar het referentiemodel brandweer processen, Aristoteles en de HKZ-norm (Harmonisatie Kwaliteitsbeoordeling in de Zorgsector).

3.2.3 Bedrijfsprocessen van een veiligheidsregio

In onderstaande figuur zijn de bedrijfsprocessen weergegeven.



Figuur 3.4. Bedrijfsprocessenmodel VeRA

Zoals eerder is aangegeven, worden bedrijfsprocessen direct gerelateerd aan de dienst en/of product die door het proces wordt geleverd. Processen worden opgestart door een trigger of event. Deze informatie is vastgelegd maar levert te complexe visualisaties op om hier te tonen.

3.2.4 Beschrijving bedrijfsprocessen

Besturende bedrijfsprocessen

Beleid vormen: Het opstellen van beleid voor de organisatie en haar activiteiten in brede zin. Beleid op zowel strategisch, als tactisch en operationeel niveau. Van bestuursniveau tot afdelingsniveau.

Sturen, beheersen en verantwoorden: Het sturen, beheersen en verantwoording afleggen over de organisatie en haar activiteiten in brede zin. Dit omvat alle niveaus en alle gebieden: zowel strategisch als tactisch en operationeel niveau. Van bestuursniveau tot afdelingsniveau.

Primaire bedrijfsprocessen

Analyseren van risico's: het uitvoeren van analyses op het gebied van risico's voor de fysieke veiligheid in de openbare ruimte.

Verlenen van adviezen: het opstellen van adviezen t.b.v. vergunningverlening en handhaving aan bevoegd gezag gericht op fysieke veiligheid.

Toezicht houden: het uitvoeren van toezicht gericht op fysieke veiligheid.

Communiceren over risico's: coördinatie en uitvoering van de externe communicatie met burgers en bedrijven over risico's en handelingsperspectief ten tijde van incidenten of bij dreiging.

Organiseren van operationele beschikbaarheid: Het organiseren van de beschikbaarheid van sleutelfunctionarissen, operationele eenheden, materieel en materiaal ten behoeve van de hulp- en zorgverlening.

Vakbekwaam worden en blijven: Het opleiden (vakbekwaam worden), trainen en oefenen (vakbekwaam blijven) van sleutelfunctionarissen en operationele eenheden dusdanig dat zij bij een inzet in staat zijn effectief het incident te bestrijden, respectievelijk te coördineren en leiding te geven.

Opstellen operationele plannen & procedures: Het opstellen en actueel houden van operationele planvorming documenten en procedures.

Beheer en onderhoud brandweer & geneeskundig specifieke hulpmiddelen: Het beheren en onderhouden van tankauto's, hulpverleningsvoertuigen, piketauto's, geneeskundige combinatie en de in deze voertuigen aanwezige materialen, dusdanig dat inzetbaarheid is gegarandeerd.

Vorbereiden op opgeschaalde situaties: 'Het zorgdragen voor de vergaring van preparatieve informatie, wat de veiligheidsregio in staat stelt om conform artikel 2.4.1, lid 1 een totaalbeeld op te bouwen over de aard van de betrokken objecten en over de verantwoordelijkheden voor de grootschalige incidentbestrijding rond deze objecten. Daarnaast het nemen van operationele maatregelen om voorbereid te zijn op bepaalde grootschalige incidenten (bv het inrichten van een 'slapend CoPI').

Besluitvorming t.b.v. multidisciplinaire crisisbeheersing/ rampenbestrijding:

Coördinatie en leiding van een grootschalig incident vanuit CoPI, ROT, RBT (afhankelijk van de opschaling) inclusief de crisisinformatie aan burgers.

Bestrijden van brand en emissie gevaarlijke stoffen:

Naar aanleiding van een melding daadwerkelijk uitrukken en bestrijden van een brand en/of emissie van gevaarlijke stoffen.

Redden en technische hulpverlening:

Opsporen en bevrijden van slachtoffers bij een ramp, alsmede het verlenen van levensreddende eerste hulp

Regisseren geneeskundige opgeschaalde zorg:

Het regisseren van de gezondheidszorg voorafgaand aan daadwerkelijke rampen en crises, alsmede van de voorbereiding daarop, met als doel dat slachtoffers onder alle omstandigheden verantwoorde zorg kan worden geboden door een samenhangende zorgketen, in nauwe samenwerking met andere hulpdiensten.

Coördineren geneeskundige opgeschaalde zorg:

Het coördineren van de gezondheidszorg tijdens rampen en crises met als doel dat slachtoffers onder alle omstandigheden verantwoorde zorg kan worden geboden door een samenhangende zorgketen, in nauwe samenwerking met andere hulpdiensten.

Evalueren van hulp en zorgverlening:

Het evalueren van de geleverde hulp en zorgverlening n.a.v. een incident.

Secundaire bedrijfsprocessen

Personeelsmanagement: zorgen voor personeel en organisatie.

Inkoop en contractmanagement: specificeren (samen met de klant), selecteren, contracteren, bestellen en bewaken van de levering van een product of dienst waar uiteindelijk een externe factuur tegenover staat.

Financieel management: beheren en voeren van de financiële administratie en controleren en rapporteren van alle financiële gegevens, processen, transacties.

Informatie & ICT management: ontwerpen en onderhouden informatiearchitectuur, ondersteunen van gegevensgebruik, leveren van informatievoorziening diensten, en ondersteunen van het ICT-gebruik en de ICT-projecten van de organisatie.

Communicatie management: coördineren en uitvoeren van de interne en externe communicatie t.b.v. de 'branding' van de organisatie.

Facilitair management: intern verlenen van diensten, ter beschikking stellen en plannen en onderhouden van faciliteiten die nodig zijn voor de ondersteuning van de interne activiteiten.

3.3 Bedrijfsfuncties

3.3.1 Wat zijn bedrijfsfuncties?

Bedrijfsfuncties geven inzicht in wat een veiligheidsregio doet (wat de kerntaken zijn), onafhankelijk van de organisatorische inrichting ervan.

Het bedrijfsfunctiemodel toont de bedrijfsfuncties in relatie tot elkaar en biedt daarmee een uitgangspunt voor andere modellen in de VeRA.

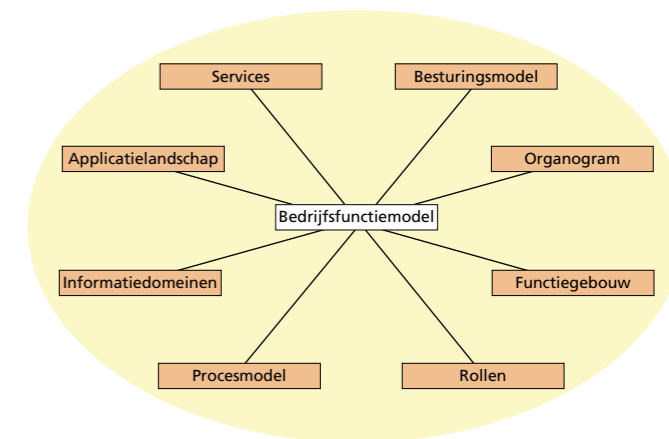
De definitie van een bedrijfsfunctie is als volgt:

Een bedrijfsfunctie is een aandachtsgebied waaraan het bedrijf structureel aandacht wil besteden (= energie in wil stoppen, structureel middelen voor wil inzetten) om zijn bedrijfsdoelstelling te realiseren. Een bedrijfsfunctie kan daarom ook gezien worden als een groepering van intern gedrag op basis van een bepaald criterium (bijvoorbeeld plaats (dezelfde afdeling), communicatie, benodigde competenties, gedeelde bronnen en gedeelde kennis). Een bedrijfsfunctie representeert een stuk toegevoegde waarde van de organisatie.¹

Het bedrijfsfunctiemodel is een inrichtingsonafhankelijke beschrijving van de taakgebieden (bedrijfsfuncties) van een veiligheidsregio die toegevoegde waarde leveren aan de omgeving en intern aan de onderdelen van de veiligheidsregio zelf. Het geeft de kernactiviteiten van de veiligheidsregio weer. Hierdoor is het bedrijfsfunctiemodel een behoorlijk stabiele afspiegeling van de organisatie. Organisaties wijzigen met grote regelmaat en daarmee wijzigt ook hun organogram; bedrijfsfuncties zijn over het algemeen stabiel, ongeacht de verandering in de organisatiestructuur.

Het bedrijfsfunctiemodel is een soort ondergrond waar vervolgens andere aspecten opgelegd worden, zoals processen, applicaties en projecten. Figuur 3.4 toont het bedrijfsfunctiemodel als spin in het web voor andere architectuurproducten.

¹ Bron: NORA 2.0



Figuur 3.4. Bedrijfsfunctiemodel als spin in het web. Bron: G. Bayens, "Bedrijfsarchitectuur, werken aan een samenhangende bedrijfsinrichting" (2009)

Bedrijfsfuncties zorgen voor een logische opdeling van activiteiten binnen een organisatie, waarbij zij zichzelf kunnen inrichten zonder daarbij afhankelijk te zijn van andere bedrijfsfuncties. Bedrijfsfuncties zijn ontkoppelbaar waardoor er flexibiliteit ontstaat in de inrichting van de organisatie. Hierbij is het belangrijk dat de verantwoordelijkheden per bedrijfsfunctie eenduidig belegd worden en 'applicaties niet over de grenzen van bedrijfsfuncties heen werken'². Bedrijfsfuncties kunnen door hun eigenschap dat ze ontkoppelbaar zijn, ook helpen bij het beantwoorden van in- en outsourcingvraagstukken.

De zuster-referentiearchitectuur van de waterschappen, WILMA, beschrijft ook nog het volgende belangrijke aspect van bedrijfsfuncties:

Door in kaart te brengen welke gegevens bedrijfsfuncties van elkaar nodig hebben, is het mogelijk om goede afspraken te maken over

² Functionaliteit moet modulair opgebouwd zijn. Overigens geldt ook hier: 'comply or explain'.

gegevensuitwisseling en wordt inzichtelijk wat kerngegevens zijn. De koppelvlakken tussen de bedrijfsfuncties geven aan welke gegevens functie overschrijdend zijn en waarover dus afspraken gemaakt moeten worden rond het delen van gegevens. Zo geeft het bedrijfsfunctiemodel focus aan de discussies over gegevensuitwisseling en kernregistraties.

Bedrijfsfuncties leggen de basis voor het maken van afspraken over gegevensuitwisseling o.a. ten behoeve van de ketens. De bedrijfsfuncties zijn verantwoordelijk voor het inzichtelijk maken van hun koppelvlakken voor zowel de eigen organisatie als andere organisaties. Via deze koppelvlakken kan de bedrijfsfunctie gestandaardiseerd gegevens uitwisselen. In toenemende mate zien we de gebiedsgerichte aanpak opkomen: de diverse ketenpartners leveren geo-gerelateerde gegevens aan omtrent een bepaald onderwerp (bv fysieke veiligheid) en hiervan wordt een gecombineerd beeld getoond. Hierdoor wordt informatie steeds minder per kolom (brandweer, GHOR) ontsloten; in toenemende mate is informatie multi-disciplinair. Hierdoor wordt het belang van afspraken over eigenaarschap van gegevens en het conformeren aan standaarden nog prominenter. Standardisatie maakt de samenwerking binnen en tussen veiligheidsregio's mogelijk. Zo draagt de VeRA bij aan één van de belangrijkste speerpunten van de veiligheidsregio's: gegevens delen.

3.3.2 Beschrijving bedrijfsfuncties van een veiligheidsregio

De bedrijfsfuncties worden in figuur 3.3 per genoemd domein gevisualiseerd in het bedrijfsfunctiemodel.

Binnen het bedrijfsfunctiemodel van de VeRA zijn de functies van de Veiligheidsketen¹ (van koud naar warm, met terugkoppeling)

opgenomen. Binnen de koude fase Risicobeheersing zijn de schakels Proactie en Preventie samengevoegd. Hiervoor is gekozen omdat het onderscheid tussen Proactie en Preventie veel meer inhoudelijk is (advies over c.q. handhaving van de brandveiligheid in de ruimtelijke ontwikkeling of van fysieke objecten) dan in de bedrijfsfunctie. Bovendien kan gesteld worden dat alle functies binnen Risicobeheersing de risico's en het minimaliseren ervan centraal stellen. Binnen de warme fase Incidentbeheersing zijn de schakels preparatie, repressie en nazorg opgenomen. De reden hiervoor is dat alle bedrijfsfuncties binnen incidentbeheersing het incident centraal stellen.

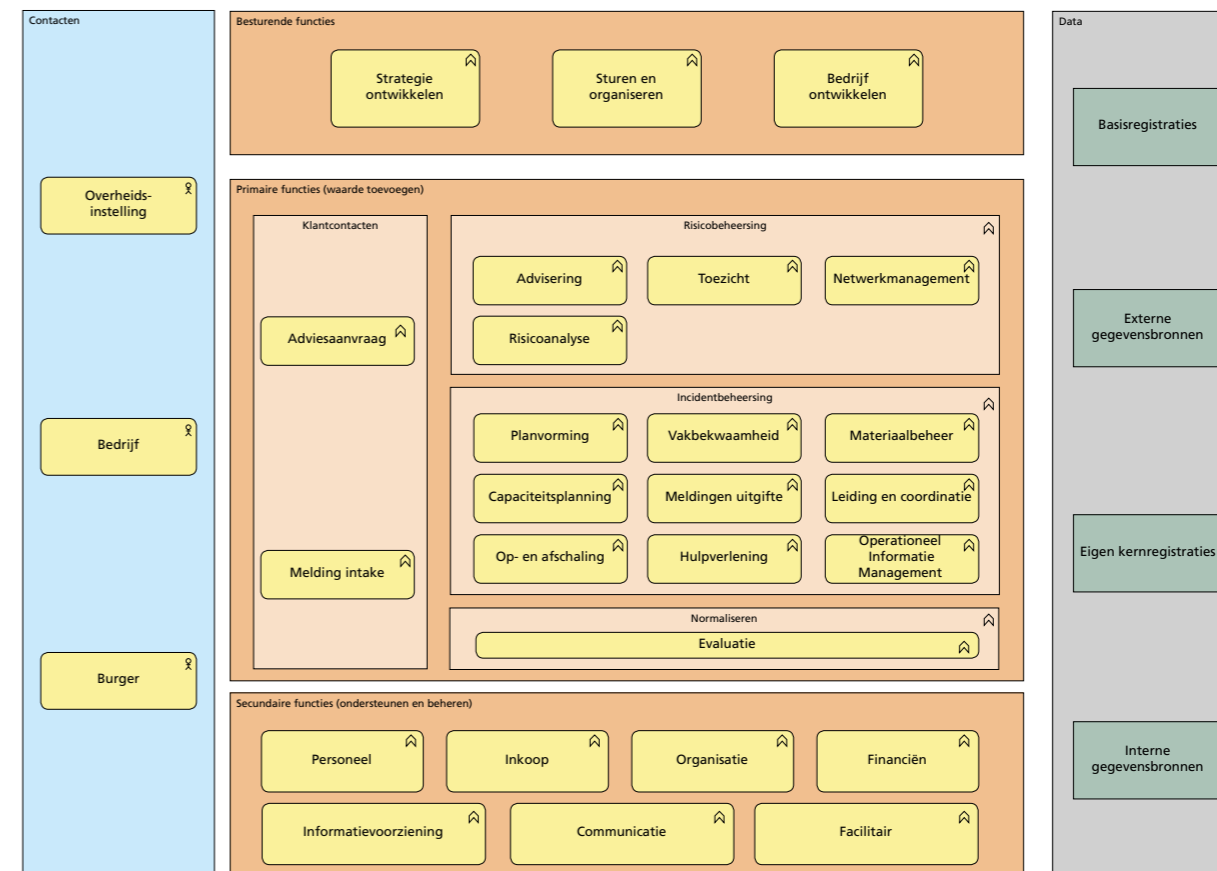
Daarnaast is er nog een aparte groepering gemaakt van bedrijfsfuncties die zich richten op de klantcontactfunctie. Uiteraard staat bij deze functies het contact met de klant centraal.

In de volgende paragrafen worden de definities gegeven van de bedrijfsfuncties. Zij staan uiteraard gegroepeerd per domein conform de Basisarchitectuur overheidsorganisaties.

3.3.3 Definitie bedrijfsfuncties

Besturende functies

Strategie ontwikkelen: Het uitwerken van de meerjarige aanpak om de visie en missie te kunnen realiseren (drie tot vijf jaar). Planmatige en doelgerichte inzet van mensen en middelen. Het vormt de basis voor het onderzoek naar de behaalde resultaten van het beleid en het bijstellen van dit beleid en omvat ook de evaluatie van het gevoerde beleid.



Figuur 3.6. Bedrijfsfunctiemodel VeRA

¹ De veiligheidsketen bestaat uit de stappen Proactie, Preventie, Preparatie, Repressie en Nazorg.

Sturen en organiseren: het verzamelen en analyseren van informatie en het formuleren van plannen als gevolg van het gemaakte meerjarenbeleid, met het oog op het ‘wat’ en het ‘wanneer’ voor de inzet van de primaire processen en de noodzakelijke ondersteuning.

Bedrijf ontwikkelen: het beoordelen van de primaire processen, de procesprestaties en de effecten hiervan. Input aanleveren voor het bijsturen van het beleid en/of primaire proces.

Primaire functies

Adviesaanvraag: een aanvraag voor advies, bijvoorbeeld in het kader van de Wet algemene bepalingen omgevingsrecht (Wabo), of over een evenement of crisisplan.

Melding intake: het aannemen, beoordelen en het verwerken van meldingen over incidenten en verzoeken tot ondersteuning (zoals medisch transport en technische ondersteuning).

Risicoanalyse: proactief inventariseren en analyseren van de risico's in het verzorgingsgebied. Dit kan het regionale risicoprofiel zijn of een risicoanalyse van objecten met bovengemiddeld risico (risicogevende en risico-ontvangende objecten).

Advisering: advisering enerzijds aan bevoegd gezag, zoals advies brandveiligheid in het kader van de Wabo, advisering vergunningen evenementen, toetsen van bouwplannen, omgevingsadvisering. En anderzijds advisering over risico's aan burgers, bedrijven en zorginstellingen over o.a. brandveilig leven.

Toezicht: het inspecteren op maatregelen genomen zoals voorgeschreven in de vergunningverlening of het controleren of taakorganisaties hun wettelijk voorgeschreven taken naar behoren uitvoeren en het geven van advies op handhaving aan het bevoegd gezag.

Netwerkmanagement: het structureel onderhouden en het uitvoeren van de regie op het waarborgen van de continuïteit van zorg door bewust, systematisch en doelgericht inzetten van netwerken van professionals. Bijvoorbeeld: convenanten met nutsbedrijven, afspraken met zorginstellingen, nazorg protocollen met de gemeenten.

Planvorming: het voorbereiden (prepareren) op hulpverlening en de beheersing van incidenten en crises door het opstellen van plannen en procedures. Bijvoorbeeld: bereikbaarheidskaarten, aanvalsplannen, regionale crisisplannen, ontruimingsplannen, calamiteitenplannen, pandemie plannen, (zorg)continuïteitsplannen.

Vakbekwaamheid: opleiden, trainen en oefenen van hulpverleners zodat ze op vakkundige wijze hulp kunnen verlenen.

Capaciteitsplanning: het inroosteren van mensen en middelen. Bijvoorbeeld: het maken van een dekingsplan of een materieelspreidingsplan, het inroosteren van piketfunctionarissen.

Materieelbeheer: alle voor hulpverlening noodzakelijk materieel en materiaal direct inzetbaar gereed houden. Hierbij valt te denken aan voertuigen, communicatiemiddelen, ademlucht, medicijnenkoffers, sigmatenten.

Melding uitgifte: het oproepen (uitgifte) van de noodzakelijke disciplines.

Toelichting

Bij de taken van een veiligheidsregio hoort het organiseren van een soepel verloop van een incidentsituatie waar weinig coördinatie benodigd is naar een situatie waarbij meer en bredere inzet en coördinatie benodigd is. In de Wvr is sprake van het ‘proces melding en opschaling’ conform door de Veiligheidsregio vast te leggen criteria³. Aangezien de processen ‘melding’ en ‘alarmering’ grotendeels⁴ onder verantwoordelijkheid van de LMO komt te liggen is het noodzakelijk om voor de architectuur zorgvuldig naar het proces of de bedrijfsfunctie ‘op- en afschaling’ te kijken. De splitsing van LMO-taken en Veiligheidsregio-taken brengt met zich mee dat er zorgvuldige afspraken over informatieoverdracht en gedeelde ketenregie worden gemaakt. Beide partijen hebben immers een belang bij een goed voorbereid⁵ gedeeld totaalbeeld en een gedeeld idee over de impact op het proces ‘leiding en coördinatie’.

Dit brengt vanuit informatiemanagement en architectuur een bijzondere verantwoordelijkheid met zich mee voor de applicatieve functies operationeel informatie management (LCMS) en melding en intake (NMS), maar ook voor aanpalende applicatieve functies, zoals de voorbereiding van evenementen (evenementenkalender) en planvorming.

Op- en afschaling: Het nemen van alle maatregelen, het maken van de afspraken en het prepareren van de informatieoverdracht voor een juist verloop van de transitieproces tijdens opschalen en afschalen bij grote evenementen, bij incident management en bij crisisbestrijding na alarmering conform afgesproken criteria. Het betreft zowel de voorbereiding en de uitvoering van deze maatregelen, afspraken en overdracht tussen verschillende afdelingen, sectoren, kolommen en ketenpartners met inbegrip van de verantwoordelijken bij de vitale infrastructuur van een regio.

Leiding en coördinatie: effectieve aansturing van alle betrokken diensten, sleutelfunctionarissen en eenheden. Bij elke inzet is sprake van leiding en coördinatie, ongeacht de omvang van de inzet of eventuele opschaling.

Hulpverlening: hulp die geboden wordt in het kader van het beheersen van incidenten in de vorm van repressie of het verlenen van acute zorg. Bijvoorbeeld: bestrijden brand, verzorgen van slachtoffers, transport van patiënten.

Operationeel informatiemanagement: het verkrijgen van alle voor de bestrijding van het incident relevante informatie over objecten, capaciteit en actoren in de regio en het actief en proportioneel beschikbaar stellen van deze informatie voor de relevante actoren. De juiste informatie moet in de juiste vorm en op het juiste moment beschikbaar zijn voor degenen die deze nodig hebben.

Evaluatie: evalueren van incidenten, educatie vanuit evaluatie, borgen van opgedane kennis in de primaire functies.

³ Zie artikel 2.2.1 Besluit Veiligheidsregio's

⁴ Alarmering kan niet plaatsvinden zonder uitvoerig overleg tussen kolom en meldkamer.

⁵ Zie ook Wet Veiligheidsregio's : artikel 48 en besluit Veiligheidsregio's, artikel 2.4.1

Secundaire functies

Personeel: beheer van alle gegevens, informatie en kennis over medewerkers, inclusief werving en selectie van nieuwe medewerkers, afvloeiings- en ontslag gerelateerde activiteiten en diverse andere activiteiten, zoals: training, carrièreplanning, beheer functiegebouw, salariering, e.d.

Inkoop: het specificeren (samen met de klant), selecteren, contracteren, bestellen en bewaken van de levering van een product of dienst waar uiteindelijk een externe factuur tegenover staat. De inkoopfunctie omvat dus meer dan alleen de inkoopafdeling en het inkoopproces. Het betreft de gehele organisatie, die zich bezighoudt met alle aspecten van het inkopen.

Organisatie: beheer van alle organisatorische gegevens, waaronder beschrijving van de bedrijfsfuncties, organisatiestructuur (organogram), functionele scope van de sectoren en afdelingen, TVB-schema's (Taken, Verantwoordelijkheden en Bevoegdheden), e.d.

Financiën: het management, het beheer, de administratie en de controle op alle financiële gegevens, processen, transacties en rapportage daarover.

Informatievoorziening: het leveren van de informatievoorzieningsdiensten -waaronder het aansluiten van de ICT-inrichting op de bedrijfsdoelstellingen- en het management en beheer van het Informatieplan en alle activiteiten die hieruit voortkomen. Het ontwerpen, beschrijven en plegen van onderhoud op bedrijfsprocessen en het bewaken van de consistentie met de administratieve organisatie en de informatiearchitectuur. Beheer van alle gegevens, informatie,

kennis, informatieresources en -middelen (bijv. telefonie, bibliotheek, automatiseringsmiddelen en -diensten) en de coördinatie, allocatie en gebruik van alle communicatiemiddelen.

Communicatie: het maken van communicatieplannen en uitvoeren van communicatie-uitingen om de gewenste boodschap over te brengen.

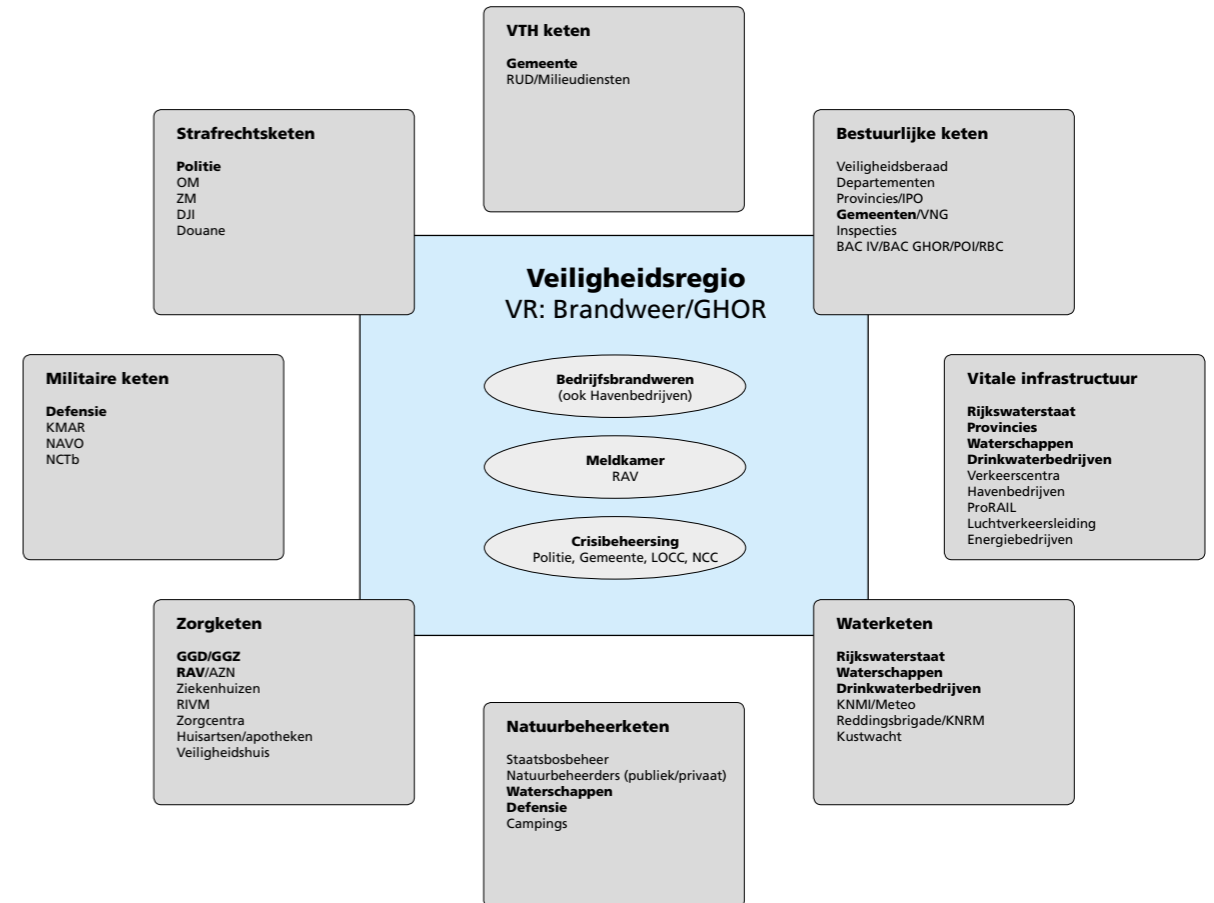
Facilitair / Huisvesting: het faciliteren van de organisatie met diensten en beheer van de huisvesting (gebouwen, terreinen), parkeerfaciliteiten, nutsvoorzieningen (gas, water, licht).

3.4 Ketensamenwerking

De Veiligheidsregio is in het eerste hoofdstuk omschreven als een organisatie die in het merendeel van de tijd preparatief in ketens en netwerken binnen en buiten de regio samenwerkt. Er wordt veelvuldig en in veel verschillende vormen samengewerkt met diverse partijen. Primair wordt samengewerkt met Politie, GGD en gemeente. Naar gelang de aard van de ramp of crisis worden hier ook andere partijen bij betrokken (waterschappen, defensie, Rijkswaterstaat, ProRail, etc.). Een andere zeer nadrukkelijke samenwerking is die met de Landelijke Meldkamer Organisatie (LMO). Specifieke ketens waarin wordt samengewerkt zijn bijvoorbeeld de VTH-keten (vergunning, toezicht en handhaving in het kader van de WABO) met organisaties als de RUD en andere toezichthouders¹.

Ketensamenwerking kenmerkt zich onder meer door het ontbreken van eenduidige regie, het ontbreken van eenduidige financiering, en

¹ Vanuit de doorontwikkeling van de NORA is een zeer leeswaardig document opgesteld over ketensamenwerking en ketensturing (zie: <http://www.noraonline.nl/wiki/Ketensturing>).



Figuur 3.7. Ketensamenwerkingen. Let op: dit overzicht heeft niet de intentie om volledig te zijn. Bovendien zal per Veiligheidsregio het belang van een ketensamenwerking verschillen

de veelheid aan probleemeigenaren. Alle betrokkenen delen eenzelfde (maatschappelijk) belang maar hebben tegelijkertijd ook hun eigen belangen.

Op organisatieniveau kan er worden samengewerkt doordat bedrijfsprocessen die bij verschillende organisaties zijn ondergebracht samen een ketenproces vormen. Op het informatieniveau is er vooral sprake van uitwisseling van gegevens. Dit kan plaatsvinden zonder dat er sprake is van samenwerking op organisatieniveau (bijvoorbeeld bij het gebruik van gegevens uit basisregistraties). Echter, bij iedere vorm van samenwerking op het organisatieniveau zal er ook sprake zijn van uitwisseling van gegevens en dit is ook mogelijk tussen organisaties. Binnen Service Gerichte Architectuur, die de NORA en de VeRA als principe hanteren, is er sprake van services (diensten) waarbij op netwerkniveau actuele gegevens (inclusief hun betekenis) opgehaald kunnen worden bij bekende en in sommige gevallen bij onbekende bronnen. In het laatste geval spreekt men van 'linked open data'.

Daarnaast kan er sprake zijn van samenwerking met ketenpartners waarbij in dezelfde applicatie wordt gewerkt. Op dat moment is er sprake van verregaande integratie op het niveau van de IT infrastructuur. Door gemeenschappelijk gebruik van een applicatie door verschillende applicatieve functies van verschillende organisaties wordt de onderlinge afhankelijkheid van de ketenpartners groot. Vanuit het concept van servicegerichte architectuur heeft dit dan ook niet de voorkeur en sluit daarmee ook niet aan op het VeRA principe S.1 (zie voor toelichting op de applicatieve functies hoofdstuk 4).

Figuur 3.7 geeft de ketenverbanden weer die voor de meeste Veiligheidsregio's relevant zijn. Het niet noemen van een keten wil dus niet zeggen dat deze niet bestaat. Het is een gecompriëerde weergave.

Figuur 3.7 schetst acht ketensamenwerkingen. Ketens waar intensief mee gewerkt wordt, staan in de tekening dicht bij de Veiligheidsregio. Ketens waar minder intensief mee gewerkt wordt, staan meer op afstand. Sommige ketenpartners komen in meerdere ketentypen voor, zoals de gemeenten, politie en de GGD.

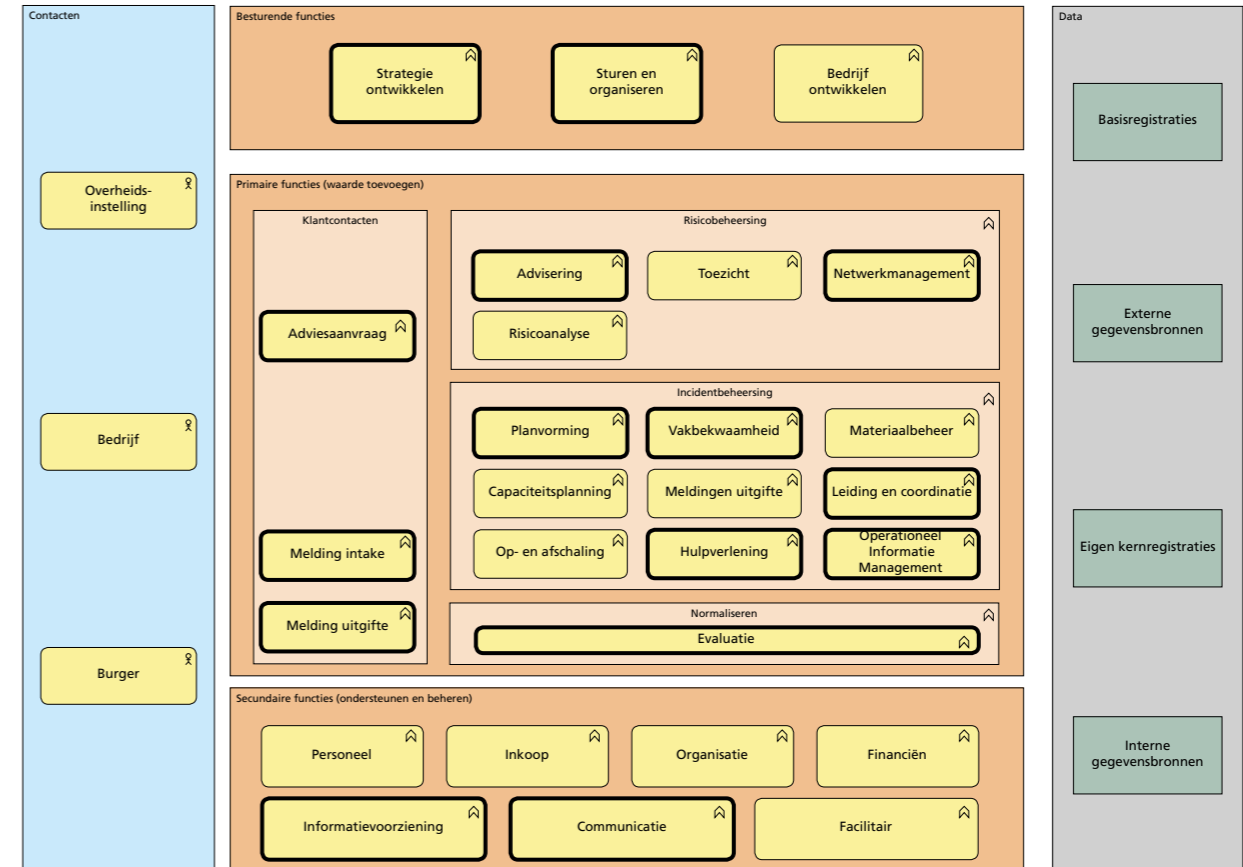
Voor de ketenpartners GGD en Politie is er een nadere analyse gedaan naar de bedrijfsfuncties waar samengewerkt wordt: zijn dit slechts enkele bedrijfsfuncties waar intensief samengewerkt wordt, of wordt er juist over de brede linie samengewerkt? Voor de gemeenten is deze analyse niet uitgevoerd; door de vele ontwikkelingen die tijdens het schrijven van het document plaats vinden bij de gemeenten, waaronder de stichting van de Regionale Uitvoerings Diensten (RUD's of Omgevingsdiensten) was het niet mogelijk om dit samen met vertegenwoordiging van de gemeenten te doen.

3.4.1 De Veiligheidsregio en de Politie

Figuur 3.8 toont de samenwerking met de Politie, waar bij zowel de besturende, de primaire, als de secundaire functies wordt samengewerkt.

Bij de besturende functies wordt vooral samengewerkt in landelijke governance overleggen zoals het Veiligheidsberaad en CIO-overleggen. Binnen de Veiligheidsregio's zelf vindt dit plaats in de Veiligheidsdirecties.

Op het gebied van klantcontacten wordt er bij alle bedrijfsfuncties samengewerkt: binnen de meldkamer wordt samengewerkt bij zowel melding intake als melding uitgifte. Bij adviesaanvragen zien we vooral samenwerking bij bijvoorbeeld de voorbereiding op grote evenementen. Deze aanvragen komen binnen bij de gemeente, die vervolgens advies kan vragen bij de Veiligheidsregio of Politie. Tevens wordt er veel samengewerkt bij het actueel houden van de evenementenkalender.



Figuur 3.8. De bedrijfsfuncties waar de Veiligheidsregio en de Politie samenwerken

Op het gebied van risicobeheersing zien we samenwerking bij advisering, dit gebeurt vaak tussen het Staf Grootchalig Bijzonder Optreden (SGBO) van de Politie en het Veiligheidsbureau. Gegevens die worden uitgewisseld hebben voornamelijk betrekking op de locatie/route van het evenement, de afzettingen en tijdelijke parkeerplaatsen. Bij samenwerking op het gebied van netwerkmanagement kan gedacht worden aan het gezamenlijk afsluiten van convenanten.

Bij incidentbeheersing zien we vooral samenwerking in geval van een opgeschaalde situatie (GRIP) en de gezamenlijke voorbereiding hierop. Er worden vaak gezamenlijk multidisciplinaire oefeningen uitgevoerd, zoals CoPI- en ROT-trainingen, waar bijvoorbeeld de netcentrische werkwijze beoefend wordt. Informatie die vergaard wordt in de bedrijfsfunctie 'planvorming' van de Veiligheidsregio, kan tijdens een incident opgehaald worden door alle crisispartners zoals benoemd in het regionaal crisisplan (brandweer, GHOR, politie, gemeente, defensie). De Politie wisselt tijdens opgeschaalde incidenten ook de informatie uit die zij binnen hun 'gedeeld veiligheidsbeeld' vergaard hebben en die van belang kan zijn voor andere crisispartners.

Met betrekking tot de secundaire functies wordt er vooral samengewerkt tussen de Veiligheidsregio en de politie op het gebied van informatiemanagement. De Veiligheidsregio en de Politie werken vooral samen op het gebied van het beheren van gemeenschappelijke voorzieningen zoals de WAS-sirenes en C2000 infrastructuur en gemeenschappelijke applicaties zoals het GMS.

Met betrekking tot gegevens is geconstateerd dat er definitieverschillen bestaan tussen de kolommen in de Veiligheidsregio en de politie voor bepaalde kernregistraties. Bijvoorbeeld bij de kernregistratie personen, gebruiken de GHOR en GGD het Elektronisch Patiënten Dossier (EPD)

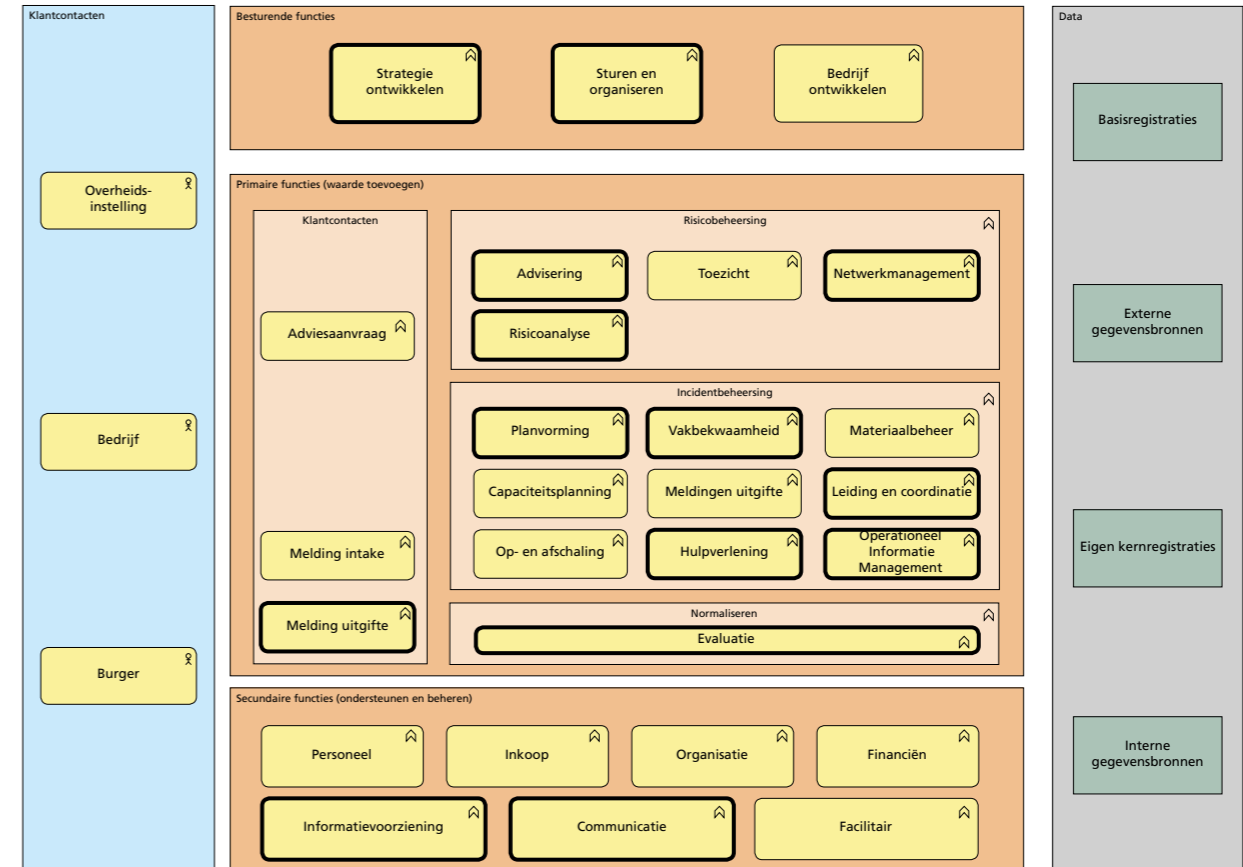
en de Politie heeft een verdachtenregistratie. De brandweer stuurt nauwelijks op een kernregistratie personen, maar is vooral object-georiënteerd. De basisregistratie voor deze objecten, de Basisregistratie Adressen en Gebouwen (BAG) bevat alleen adresseerbare objecten. De brandweer heeft ook behoefte aan niet-adresseerbare objecten zoals terreinen. De Politie hanteert een bredere definitie van objecten: auto's kunnen ook objecten zijn. Hieruit blijkt dat het belangrijk is om op dataniveau afspraken te maken om te komen tot een gemeenschappelijke vocabulaire.

3.4.2 De Veiligheidsregio en de GGD

Figuur 3.9 toont de samenwerking met de GGD, waar bij zowel de besturende, de primaire, als de secundaire functies wordt samengewerkt.

De GHOR en de GGD werken in toenemende mate samen. Het gezamenlijk sturen van de GHOR en GGD begint met de aanstelling van één directeur Publieke Gezondheidszorg (DPG) per veiligheidsregio. Deze stuurt op geneeskundige hulpverlening in zowel de preparatieve als repressieve fase. De DPG heeft vaak zitting in de Veiligheidsdirecties. Bij de besturende functies wordt ook veel samengewerkt in landelijke governance overleggen zoals het Veiligheidsberaad en CIO overleggen. De GHOR en de GGD stellen samen ook vaak strategische plannen op.

De GHOR en de GGD werken bij een groot aantal primaire bedrijfsfuncties samen. In de risicobeheersing levert de GGD bijvoorbeeld de risico's met betrekking tot Medische Milieukunde en Infectieziektebestrijding aan, die door de Veiligheidsregio verwerkt worden in het regionaal risicoprofiel. Ook wordt bij de advisering van evenementen samengewerkt tussen de GGD en de GHOR.



Figuur 3.9. De bedrijfsfuncties waar de Veiligheidsregio en de GGD samenwerken

Op het gebied van incidentbeheersing wordt vooral samengewerkt in geval van een opgeschaalde situatie (GRIP) en bij de gezamenlijke voorbereiding hierop. De opschaling van de GGD (GGD rampen opvangplan) sluit aan bij de GRIP-structuur van de Veiligheidsregio's. De preparatieve gegevens zoals vergaard binnen de Veiligheidsregio's worden tijdens een incident gedeeld met de GGD door de backoffice GHOR. De GGD maakt planvorming ten aanzien van bijvoorbeeld infectieziektebestrijding en deelt dit weer met de Veiligheidsregio. Tijdens de hulpverlening wordt informatie vaak mondeling uitgewisseld.

Met betrekking tot de secundaire functies wordt er vooral samengewerkt tussen de Veiligheidsregio en de GGD op het gebied van informatiemanagement. We zien regelmatig dat de ICT-technische infrastructuur gedeeld wordt, of dat één van de twee partijen de kantoorautomatisering voor de andere partij beheert.

3.4.3 Impact van de brede samenwerking met Politie en GGD op de informatie uitwisseling

In de vorige paragrafen is beschreven dat de Veiligheidsregio een brede samenwerking heeft met de Politie en de GGD, waarbij er op meerdere bedrijfsfuncties samengewerkt wordt. Om goed samen te kunnen werken, maar ook om de eigen organisatie te kunnen blijven ontwikkelen, is het belangrijk dat er op modulaire wijze samengewerkt wordt: hierdoor zal een wijziging in een bepaald gebied niet direct leiden tot een 'domino-effect' aan wijzigingen in andere bedrijfsfuncties. Het creëren van één 'supercloud' waarin alle functionaliteit aanwezig is waardoor Veiligheidsregio's kunnen samenwerken met alle ketens, lijkt hierdoor onmogelijk. Samenwerking dient vooral te geschieden door het uitwisselen van gegevens; het delen van applicatieve functies heeft niet de voorkeur.

Voor het opzetten van samenwerkingsverbanden met de in fig. 3.7 genoemde ketenpartners t.b.v. het uitwisselen van gegevens voor een gezamenlijk maatschappelijk doel ("keteninformatisering"), is het verstandig om gelijk in te zetten op een cyclisch proces voor opzet en continue verbetering:

1. Ketenanalyse, zowel qua doel ("dominant ketenprobleem"), als bedrijfsprocessen, als gegevensstromen tussen de betrokken partijen.
2. Keten-ontwerp;
3. Keten casus opvolging, het toetsen in de praktijk waarbij een casus of een dienst als onderdeel van het bedrijfsproces geanalyseerd wordt om te onderzoeken of de informatieoverdracht goed verlopen is;
4. Ketenherontwerp.

De strategie van Veiligheidsregio's is dat we:

1. hier aan willen haken bij de wettelijk verplichte 'terugmelding' van gegevens waar 'gerede twijfel' bestaat over de juistheid ervan;
2. dit in samenwerking willen doen met onze ketenpartners;
3. dat we dit doen op de 'zogenaamde pluslagen' van de basisregistraties. Dit zijn sectorspecifieke aanvullingen op de set van basisregistraties.



4 Informatiearchitectuur

4.1 Inleiding tot informatiearchitectuur

Het definiëren van applicatieve functies is één van de eerste stappen bij het opstellen van een informatiearchitectuur.

Een applicatieve functie is een zelfstandige eenheid functionaliteit. Het modulaire karakter is belangrijk: een applicatieve functie is een afgebakend geheel aan functionaliteiten, dat als zodanig vervangen kan worden. De kracht van applicatieve functies is dat specifieke en generieke functionaliteiten apart benoemd worden. De meeste software biedt specifieke en generieke functionaliteit in één pakket aan (bijvoorbeeld workflow- en documentmanagement in één pakket voor het afhandelen van verguningsaanvragen). Het risico is dat bij de aanschaf van dergelijke software overlap in functionaliteit in de organisatie ontstaat. Ook bestaat de kans dat een en hetzelfde gegeven op meerdere plekken ingevoerd en beheerd moet worden. Het definiëren van applicatieve functies is een eerste stap in het ontwarren van de 'spaghetti' aan applicaties in een organisatie.

Het bedrijfsfunctiemodel is het beginpunt geweest voor een analyse van de applicatieve functies van veiligheidsregio's. Dit heeft een applicatielandschap opgeleverd dat veiligheidsregio's kunnen vergelijken met hun eigen landschap. Blijkt daar dat meerdere applicaties één applicatieve functie afdekken, dan is applicatiesanering een optie. Zijn er gaten zichtbaar, dan is er mogelijk een (latente) behoefte van de organisatie niet ingevuld.

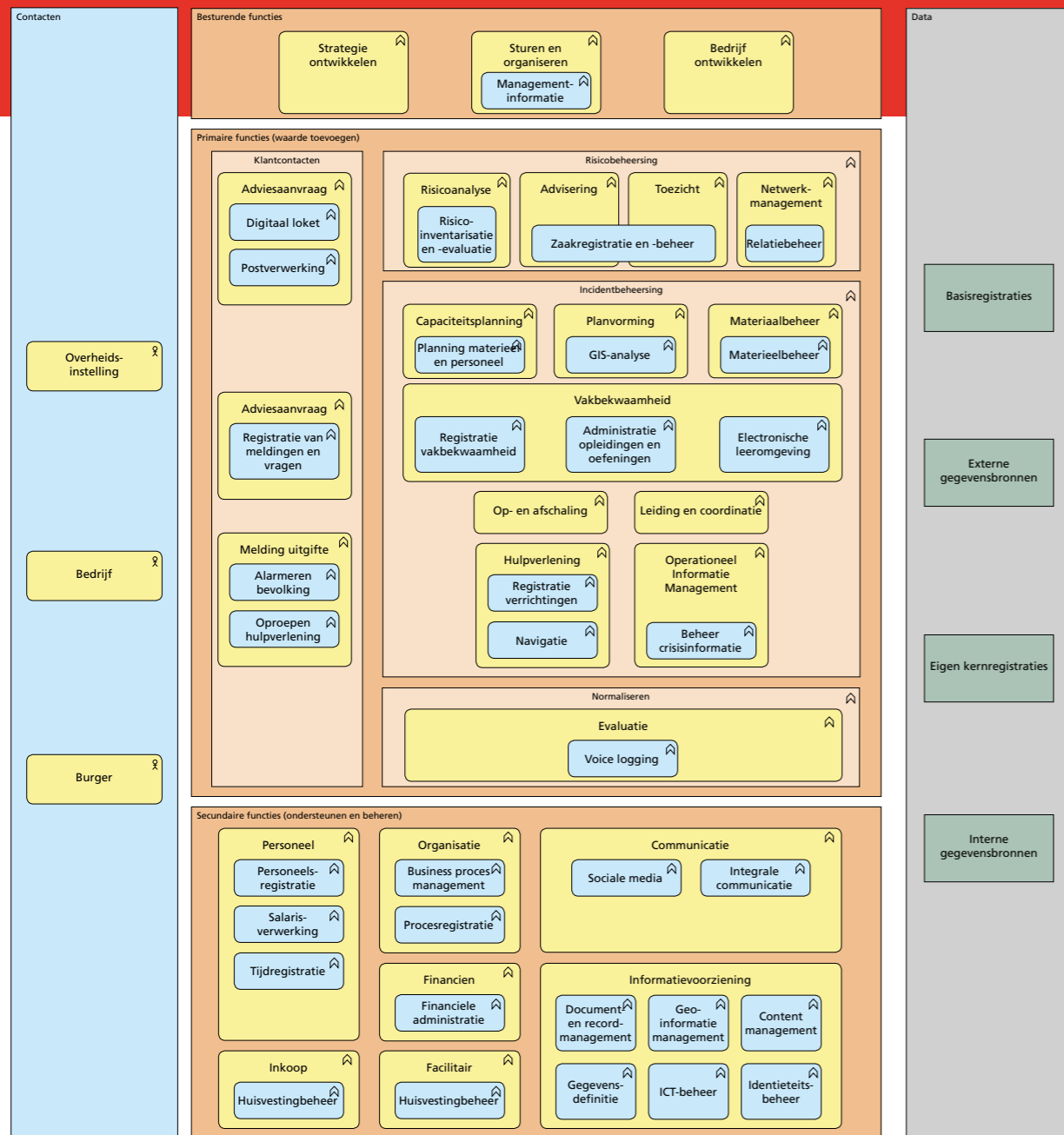
De applicatieve functies geven ook (ont)koppelpunten van applicaties aan, ze maken zichtbaar waar koppelvlakken liggen.

De meeste veiligheidsregio's hebben nu een applicatielandschap met een zogenaamde 'spaghettistructuur'. Op organische wijze zijn er steeds meer applicaties in gebruik genomen zonder dat is gekeken naar een logisch verband met het gebruik ervan binnen een specifiek toepassingsgebied overeenkomstig een bedrijfsfunctie. Hierdoor ontstaan er dubbelingen in functionaliteit omdat individuele korpsen ieder hun eigen systemen hebben waarmee een applicatieve functie wordt ingevuld. Bovendien is er in dit proces vaak slechts beperkt gekeken naar hergebruik van functionaliteit en het generiek ter beschikking stellen van gegevens.

De kracht van het benoemen van applicatieve functies ligt in de ontvlechting van de verschillende bedrijfsfuncties en is daarmee de basis voor eenduidig gebruik van functionaliteit, één van de inrichtingsprincipes van de NORA. Ook ligt dit aan de basis van een ander inrichtingsprincipe van zowel de NORA als het IBV, namelijk het hergebruik van gegevens.

Functioneel applicatielandschap

Een functioneel applicatielandschap geeft aan op welke wijze een applicatieve functie wordt ingevuld en welke relaties er tussen applicatieve functies zijn. Een applicatieve functie verbeeldt een samenhangende set functionaliteit die geleverd dient te worden. Een informatiesysteem (softwarepakket / applicatie) bevat uiteindelijk één of meerdere applicatieve functies. Iedere Veiligheidsregio kan eigen informatiesystemen aanschaffen (zelf ontwikkelen of aankopen) om invulling te geven aan deze applicatieve functies. Applicatieve functies zeggen niet welke informatiesystemen een Veiligheidsregio moet aanschaffen, maar wel welke functionaliteit via (delen van) informatiesystemen aanwezig moet zijn. Doordat op deze manier het applicatielandschap wordt ingericht, is het eenvoudiger om per bedrijfsfunctie de gebruikte informatiesystemen



Figuur 4.1. De applicatieve functies van een veiligheidsregio

te vervangen of uit te besteden overeenkomstig het gekozen groeipad binnen de bedrijfsfunctie.

Het verbinden van bedrijfsfuncties gebeurt door het beschrijven van processen. Op dezelfde manier worden applicatieve functies aan elkaar verbonden met informatiestromen (gegevensuitwisseling). Zowel de processen als de gegevensuitwisseling komen uitgebreid aan bod in een volgende versie van de VeRA.

4.2 Applicatieve functies

In figuur 4.1 zijn de applicatieve functies van veiligheidsregio's getekend in relatie tot de bedrijfsfuncties (zie hoofdstuk 3) en daarmee in relatie tot de domeinen van de basisarchitectuur voor overheidsorganisaties. In de tekst wordt per functie een definitie gegeven.

4.2.1 Besturende applicatieve functies

Besturende functies geven weer hoe de organisatie zichzelf richting geeft, bijstuurt en ontwikkelt. Binnen de besturende laag is er één applicatieve functie geïdentificeerd, namelijk management-informatie:

Managementinformatie

Managementinformatie is een functionaliteit waarmee gegevens worden geanalyseerd en de resultaten worden gepresenteerd in een zodanige vorm dat het management ondersteund wordt bij de besturing van de organisatie en bij het afleggen van verantwoording over haar functioneren. Het gaat dus om het genereren van stuur- en verantwoordingsinformatie ter ondersteuning van het besluitvormingsproces van het management of ten behoeve van landelijke statistieken (bijvoorbeeld CBS). De term Business Intelligence wordt ook vaak gebruikt voor deze applicatieve functie.

Een metafoer

Een stad bestaat uit wijken, in deze wijken staan vervolgens weer bouwwerken. De manier waarop een stad wordt ingedeeld gebeurt zeer doordacht via streekplannen en bestemmingsplannen. Afstanden tussen industriële bebouwing en woonwijken zijn juridisch vastgelegd en moeten gerespecteerd worden. Wie wil er nu ook in zijn tuin zitten terwijl er veertig meter verderop een fabriek staat te ronken? De mogelijkheden (functionaliteit) die een gebiedsfunctie biedt aan de stad wordt dus ingevuld door het type bouwwerk. Een fabriek, huis of recreatiegebied bieden immers elk andere mogelijkheden aan de inwoners van de stad. Allerlei verschillende soorten bouwwerken die een woonfunctie hebben, laten complete woonwijken ontstaan. Daar tegenover staan de industrieterreinen waar zich grote productiebedrijven en allerlei groothandels bevinden. Ook de inwoner van Nederland die van rust, schoonheid, ontspanning en natuur houdt wordt niet vergeten. Er bestaan mooie recreatiegebieden waar voor iedereen wat wils is. De wandelaar, kampeerder, visser en watersporter, ze komen allemaal aan hun trekken.

De functionaliteit die een applicatieve functie biedt kan vergeleken worden met een gebiedsfunctie: iedere applicatieve functie biedt de medewerker een set functionaliteiten zodat specifieke bedrijfsmatige werkzaamheden uitgevoerd kunnen worden. Net zoals gebiedsfuncties staan ook applicatieve functies niet op zichzelf. Verschillende functies werken samen of zijn afhankelijk van elkaar. De mobiliteit tussen gebiedsfuncties wordt ingevuld door een vervoersplan. Samenwerking tussen applicatieve functies gebeurt door uitwisseling van informatie.

4.2.2 Primaire applicatieve functies

Primaire functies hebben betrekking op het feitelijke werk van de organisatie. Deze functies leveren een directe bijdrage aan de producten en diensten van een organisatie. Met andere woorden, deze functies leveren primair de toegevoegde waarde van de organisatie. Primaire applicatieve functies zijn bijvoorbeeld:

Digitaal loket

Functionaliteit voor het digitaal indienen van verzoeken en aanvragen zoals bijvoorbeeld een advies brandveiligheid voor een bouwvergunning.

Postverwerking

Functionaliteit waarmee inkomende en uitgaande informatie geautomatiseerd naar het gewenste formaat, medium en vorm gebracht kan worden.

Registratie van meldingen en vragen

Functionaliteit voor het vastleggen van (meestal telefonische) meldingen (waaronder 112 en OMS) en vragen. Mede door de urgentie van meldingen bij incidenten (brand, ongeval, etc.) is standaard callcenterfunctionaliteit niet toereikend.

Alarmeren bevolking

Functionaliteit waarmee de bevolking gewaarschuwd kan worden voor situaties die de volksgezondheid bedreigen. Een voorbeeld van een systeem waarmee landelijk dergelijke functionaliteit wordt geboden is NL Alert.

Oproepen hulpverlening

Functionaliteit voor de uitgifte van een melding gericht op het oproepen van de juiste hulpverlening. Voorbeelden van systemen waarin dergelijke functionaliteit wordt geboden zijn P2000 en C2000.

Risico-inventarisatie en –evaluatie

Functionaliteit waarmee geïdentificeerde risico's van objecten, evenementen, etc. kunnen worden geregistreerd en geëvalueerd.

Zaakregistratie en –beheer

Functionaliteit waarmee gegevens over een zaak zelf worden vastgelegd, georkestreerd en beheerd. Een zaak wordt in het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ, onderdeel van de GEMMA) gedefinieerd als "een samenhangende hoeveelheid werk met een gedefinieerde aanleiding en een gedefinieerd resultaat, waarvan kwaliteit en doorlooptijd bewaakt moeten worden". De zaken worden aangemeld via het digitaal loket en afgehandeld met behulp van de hier genoemde functionaliteit. Belangrijk hierbij is dat via het digitaal loket altijd inzage is in de status van een zaak voor de communicatie naar de aanvrager.

Relatiebeheer

Functionaliteit om relaties te registreren en te beheren.

Planning materieel en personeel

Functionaliteit voor het plannen (roosteren) van de beschikbaarheid van hulpverleners en van het benodigde materieel. Belangrijke aspecten ten aanzien van het materieel zijn voorraadbeheer, eigenschappen van de middelen, inzet- en onderhoudsplanning.

GIS-analyse

Functionaliteit voor het genereren en beheren van kaartgerichte analyses met behulp van geo-gerefererde gegevens (wat bijvoorbeeld resulteert in een dekkingsplan).

Materieelbeheer

Functionaliteit voor het beheren van het materieel (voertuigen, hulpmiddelen, etc.) dat wordt ingezet bij de hulpverlening.

Registratie vakbekwaamheid

Functionaliteit voor het registreren van de vakbekwaamheid van (operationele) medewerkers.

Administratie opleidingen en oefeningen

Functionaliteit om de opleidingen en oefeningen te administreren. Deze administratie betreft zowel de inhoud (leerdoelen, etc.) als de logistiek (planning, inschrijving, etc.) van opleidingen en oefeningen.

Elektronische leeromgeving

Functionaliteit om educatieve inhoud via e-learning aan te bieden. Het faciliteert het proces van leren en de communicatie die nodig is voor dat leren.

Registratie verrichtingen

Functionaliteit voor het vastleggen van daadwerkelijk gerealiseerde verrichtingen zoals bijvoorbeeld een uitruk.

Navigatie

Functionaliteit voor het navigeren naar een incidentlocatie in een hulpverleningsvoertuig.

Beheer crisisinformatie

Functionaliteit voor het ondersteunen van de crisisbeheersing en de rampenbestrijding door het registreren, beheren en uitwisselen van relevante informatie t.a.v. een crisis of ramp.

Voice logging

Functionaliteit waarmee (telefonische) gesprekken worden geregistreerd en opgeslagen.

4.2.3 Secundaire applicatieve functies

Secundaire functies zijn de zogenaamde PIOFACH-functies. Deze functies ondersteunen de overige functies en kunnen worden gezien als generieke functies die in elke willekeurige organisatie zijn te herkennen. Secundaire applicatieve functies zijn:

Personeelsregistratie

Functionaliteit voor de registratie van personeelsgegevens.

Salarisverwerking

Functionaliteit voor de verwerking van salaris en vergoedingen. Centraal hierin staan de geldende arbeidsvoorwaarden en CAO-bepalingen.

Tijdregistratie

Functionaliteit om de tijdsbesteding van medewerkers te registreren.

Inkoop- en contractmanagement

Functionaliteit voor de registratie van inkooporders, gereed melding van orders en vastlegging van contractuele afspraken.

Business proces management

Generieke functionaliteit om zowel binnen één bedrijfsfunctie één of meerdere werkprocessen, maar ook bedrijfsfunctie overstijgend één of meerdere bedrijfsprocessen, eenduidig te ondersteunen. Deze functionaliteit richt zich op het op eenvoudige en eenduidige wijze beschrijven, modelleren én te publiceren van processen.

Procesregistratie

Functionaliteit om de (werk)processen binnen de organisatie te kunnen beschrijven, om zo te voldoen aan de eisen aan de administratieve organisatie.

Financiële administratie

Functionaliteit waarmee budgetten, inkomsten, uitgaven en verplichtingen worden geregistreerd en beheerd.

Huisvestingbeheer

Functionaliteit waarmee huisvesting beheerd kan worden. Hierbij valt te denken aan operationele taken, groot en klein onderhoud, reserveringen, schoonmaak, meerjarenplanning, reparaties, etc..

Sociale media en samenwerkingsplatformen

Een verzamelaar voor alle functionaliteit waarmee het mogelijk is om informatie met elkaar te delen, te verbinden en te becommentariëren. Het betreft niet alleen informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via sociale media. Deze functionaliteit kan zowel intern als extern (bijvoorbeeld met burgers tijdens een incident, ramp of crisis) worden ingezet.

Integrale communicatie¹

Functionaliteit waarmee verschillende vormen van communicatie integraal kunnen worden gebruikt zoals instant messaging (chat), aanwezigheidsinformatie, telefonie (inclusief IP telefonie), video-conferencing, datasharing, call control en spraakherkenning (allen realtime) met functionaliteiten zoals voicemail, e-mail, SMS en fax (niet realtime). Deze functionaliteit biedt gebruikers de mogelijkheid om een bericht te versturen via één medium en hetzelfde bericht via een ander medium te ontvangen. Iemand kan bijvoorbeeld een voicemail ontvangen en kiezen om dit bericht te lezen via e-mail. Deze functionaliteit kan zowel intern als extern (bijvoorbeeld met ketenpartners tijdens opschaling) worden ingezet.

¹ Integrale communicatie wordt ook wel unified communications genoemd

Document- en recordmanagement

Functionaliteit waarmee documenten en archieven (records) elektronisch kunnen worden opgeslagen conform vastgestelde metadata, beheerd (vooral versiebeheer is belangrijk) en geraadpleegd. Dit is tevens functionaliteit waarmee documenten (brieven, e-mails) conform een vastgestelde huisstijl kunnen worden gegenereerd.

❖ Geo-informatiemanagement

Functionaliteit om geo-gerefererde gegevens en kaarten te maken, te beheren en te gebruiken. Het meest bekende voorbeeld is de Digitale bereikbaarheidskaart.

❖ Contentbeheer

Functionaliteit die het mogelijk maakt dat eenvoudig teksten en media (geluid, afbeelding, video) oftewel 'content' binnen en buiten de organisatie digitaal kunnen worden gepresenteerd.

❖ Gegevensdefinitie

Functionaliteit om gegevens eenduidig te definiëren (metadatamanagement).

❖ ICT-beheer

Functionaliteit voor het ondersteunen van de ICT-dienstverlening. Deze functionaliteit omvat diverse aspecten van het beheer van de ICT-diensten zoals werkplekbeheer, het beheersen van meldingen en vragen, beheersen van wijzigingsverzoeken en registratie van de verschillende onderdelen van de ICT-dienstverlening.

Identiteitsbeheer

Generieke functionaliteit voor het vastleggen van profielen en bijbehorende autorisaties, in relatie tot personen (medewerkers en externen).

4.3 Gegevens

In het volgende deel van het applicatielandschap worden gegevensgroepen van veiligheidsregio's benoemd, onderverdeeld naar basisregistraties, externe gegevensbronnen, eigen kernregistraties en interne gegevensbronnen.

De gegevens in basisregistraties worden eenmalig ingevoerd. Daarna worden deze gegevens door de gehele overheid gebruikt. Externe gegevens die niet vervat zijn in het Stelsel van Basisregistraties worden aangeduid met externe gegevensbronnen. De gegevens in een kernregistratie worden ook eenmalig ingevoerd maar daarna worden deze gegevens door de gehele Veiligheidsregio gebruikt. De gegevens van een interne gegevensbronnen worden alleen door één organisatie- eenheid gebruikt.

4.3.1 Basisregistraties

Om haar werk te doen heeft de overheid gegevens nodig die zijn vastgelegd in ongeveer 30.000 verschillende registraties. Basisregistraties zorgen ervoor dat gegevens minder versnipperd en eenvoudiger beschikbaar zijn. Steeds alle gegevens die bij elkaar horen op één plek verzamelen; dat is in essentie een basisregistratie. Uiteindelijk zullen losse basisregistraties gaan functioneren als één logisch, samenhangend geheel: het Stelsel van Basisregistraties. Dit stelsel zorgt dat bij het beantwoorden van een vraag of het oplossen van een probleem direct alle relevante gegevens uit verschillende registraties bij elkaar kunnen komen. Basisregistraties zijn bij wet vastgelegd en overheidsorganisaties zijn of worden verplicht ze te gebruiken, afhankelijk van het ontwikkelstadium van de basisregistratie.

Er zijn dertien basisregistraties:

- GBA – Gemeentelijke Basisadministratie persoonsgegevens (wordt BRP) (Gemeenten)
- NHR – Nieuwe Handelsregister (Kamer van Koophandel NL)
- BAG – Basisregistratie Adressen en Gebouwen (Gemeenten, Kadaster)
- BRT – Basisregistratie Topografie, met de Top10NL topografie (Kadaster)
- BRK – Basisregistratie Kadaster (percelen, eigendom) (Kadaster)
- BRV – Basisregistratie Voertuigen (kentekenregistratie) (RDW)
- BLAU – Basisregistratie Lonen, arbeids- en uitkeringsverhoudingen (SZW)
- BRI – Basisregistratie Inkomens (SZW)
- WOZ – Basisregistratie Onroerende Zaken (waardebepaling) (Gemeenten)
- RNI – Registratie Niet-Ingezetenen (wordt BRP) (Gemeenten)
- BGT – Basisregistratie Grootchalige Topografie (vh. GBKN) (400+ bronhouders)
- BRO – Basisregistratie Ondergrond (voorheen ook wel DINO) (TNO)

Niet alle basisregistraties zijn voor alle VeRA bedrijfsfuncties van even groot belang. Aangezien het werk zich vaak concentreert rond de vraag "Waar is het en wat is daar?" zijn vooral de locatiegebaseerde basisregistraties van belang. Dat betreft: de BAG, de BRT, de BRO, de WOZ en de BGT (in ontwikkeling). Verder wordt ook het Nieuwe Handelsregister (NHR) steeds belangrijker om de juiste instelling/organisatie op de kaart te kunnen vinden.

Locatiegebaseerde basisregistraties zijn in het algemeen beschikbaar via de Publieke Dienstverlening op de Kaart¹ en te vinden in het bijbehorende Nationaal Georegister². Enkele basisregistraties bieden ruimte voor zgn. sectorale 'plus-lagen', dus ook voor de OOV. Dit biedt ruimte om OOV-specifieke kenmerken in een basisregistratie geborgd te krijgen. Een voorbeeld vormen de complexe ondergrondse objecten (tunnels, treintunnels) die niet standaard in de BGT zitten, maar wel in de BGT OOV+ laag. Op landelijk niveau is de OOV-sector vertegenwoordigd in het BGT gebruikerspanel.

4.3.2 Externe gegevensbronnen

Hier gaat het om externe gegevens die niet vervat zijn in het Stelsel van Basisregistraties. Hieronder vallen (niet volledig):

- Luchtfoto's loodrecht (uit de Landelijke Aanbesteding Beeldmateriaal);
- 3D-foto's (uit de Landelijke Aanbesteding Beeldmateriaal);
- Wegen, hetzij uit het NWB (RWS) of externe bronnen zoals OpenStreetMap *;
- Actuele Hoogtekaart Nederland (thans AHN2, 0,5x0,5m) (RWS/Waterschappen) *;
- De risicokaart (IPO/Bij12) **;
- Locaties Bluswaterwinpunten, w.o. Brandkranen (Vewin en haar leden);
- De Natura2000 gebieden *;
- De WAS sirenepalen (LFR/Siemens);
- Het Antenneregister (Telecommasten) (Dienst Antenneregister) *;
- De Hydrografie (vaarwegen, dieptelijnen, betonning) (RWS/Defensie) ***;

- ProRail spoorelementen (ProRail);
- CBS Wijken, buurten en demografische gegevens (CBS) *;
- Postcodegebieden (PostNL);
- Locaties Cultureel Erfgoed (Rijksdienst voor het Cultureel Erfgoed) *;
- De Bewegwijzering, m.n. de ANWB Paddenstoelen (RWS Bewegwijzeringdienst) *;
- Landelijk Register locaties Kinderopvang en Gastoudergezinnen *.

In de verdere ontwikkeling van de VeRA zal gekeken worden naar welke externe gegevensbronnen noodzakelijk zijn voor welke bedrijfsfuncties. Van belang daarbij is dat niet alle externe gegevensbronnen 'zomaar' beschikbaar zijn, d.w.z. niet alles is 'open data'. Bij bronnen die ten tijde van de publicatie van VeRA2 wél open data zijn, is dat aangegeven met één sterretje *. Deze bronnen worden landelijk ter beschikking gesteld via het Programma Geo van het Veiligheidsberaad. Voor de bronnen met meer sterretjes geldt:

** De publieke versie van de Risicokaart is open data, maar de professionele versie niet. De professionele versie is voor de hulpdiensten kosteloos beschikbaar.

*** Vaarwegen en betonning (RWS) zijn open data, maar de bathymetrie (iso-dieptelijnen van de Dienst Hydrografie van Defensie) niet.

Voor datasets die niet open data zijn, zullen convenanten moeten worden afgesloten met de eigenaar/beheerder van de registratie. Dit wordt zoveel mogelijk op landelijk niveau (Veiligheidsberaad/IFV) gedaan. Elke veiligheidsregio kan nog steeds de data regionaal verkrijgen, verrijken en gebruiken, maar het convenant hoeft maar één keer afgesloten en beheerd te worden. Binnen het Veiligheidsberaad start vanaf 2015 een landelijk programma Geo dat onder andere dergelijke convenanten zal organiseren en beheren.

4.3.3 Eigen kernregistraties

Kernregistraties zijn interne gegevensverzamelingen die voor meervoudig gebruik in aanmerking komen. Deze gegevens worden gebruikt in verschillende applicatieve functies. Door verwijzing naar een gegeven uit een kernregistratie kunnen verschillende applicatieve functies aan elkaar gerelateerd worden. Binnen de veiligheidsregio's kunnen de volgende kernregistraties worden geïdentificeerd:

- Incidenten: betreft de set aan basiskennmerken van een incidentmelding;
- Personeel: betreft de set aan basiskennmerken van een medewerker, zowel vast als tijdelijk en extern (inhuur);
- Materieel: betreft de set aan basiskennmerken van materieel die gebruikt wordt voor de hulpverlening;
- Objecten: betreft de set aan basiskennmerken van objecten in de openbare ruimte waarop verschillende werkzaamheden betrekking kunnen hebben (zoals bereikbaarheidskaarten, vergunningen, incidenten, etc.);
- Eigen locaties: betreft de set aan basiskennmerken over de vestigingslocaties van brandweerkazernes, ambulanceposten, meldkamers, alsmede de locaties van directe ketenpartners zoals politie, gemeenten, Defensie, KNRM, Reddingsbrigade, Justitie (Rechtbanken en penitentiaire locaties), waterschappen e.d.;
- Zorgcontinuïteit: betreft de set aan basiskennmerken over de zorgaanbieders en zorginstellingen (verminderd zelfredzame personen). Deze OOV kernregistratie staat in de praktijk bekend als "De Witte Kaart" en wordt beheerd door GGD/GHOR Nederland;
- Natuurbrandrisico: betreft de set aan basiskennmerken van natuurgebieden in termen van vatbaarheid voor natuurbrand;
- Budgetten: betreft de set aan basiskennmerken voor de financiële vastlegging van de werkzaamheden;

- Documenten: betreft een set aan basiskennmerken van een document plus het document zelf. Een document is een verzameling gegevens vastgelegd op een gegevensdrager zoals bijvoorbeeld papier of digitaal bestand;
- Relatie: betreft een set aan basiskennmerken van een persoon of organisatie waarmee de Veiligheidsregio een zakelijke relatie heeft. Relaties kunnen gekoppeld zijn aan GBA en aan NHR;
- Organisatie-eenheid: betreft een set aan basiskennmerken van een organisatie-eenheid (groep binnen een organisatie die een gezamenlijk doel nastreeft);
- Zaak: betreft een set aan basiskennmerken van een zaak. Een zaak is een samenhangende hoeveelheid werk met een gedefinieerde aanleiding en gedefinieerd resultaat, waarvan kwaliteit en doorlooptijd bewaakt moeten worden;
- Inzet: betreft een set aan basiskennmerken van een gerealiseerde inzet van hulpverleners en sleutelfunctionarissen (in verband met uitbataling, vakbekwaamheid).

Eigen kernregistraties worden dus door de veiligheidsregio's zelf beheerd. Ook dit gebeurt bij voorkeur op landelijk niveau, onder het motto: landelijk wat kan, regionaal waar het moet.

4.3.4 Interne gegevensbronnen

Bij interne gegevensbronnen gaat het om de data die vastgelegd worden in de processystemen. Bij deze gegevens wordt meervoudig gebruik niet ondersteund. De vastgelegde data zijn dus zeer specifiek voor een bepaalde bedrijfsfunctie.

4.3.5 Geografische informatie

Strikt genomen behoort 'geografische informatie' geen eigen paragraaf te hebben, omdat geografische informatie al verweven zit in de typen

¹ PDOK, www.pdok.nl
² Zie www.nationaalgeoregister.nl. Voor het zien van de data is een GIS viewer vereist.

gegevensbronnen zoals hierboven beschreven. Echter, gezien (a) het belang van 'de kaart' in het OOV werk en (b) de oogst van de VeRA Geo workshops uit 2013, wordt hier toch enige ruimte besteed aan geografische informatie, in termen van principes en uitgangspunten.

1. Er is geen strak onderscheid tussen 'geografische informatie' en 'niet geografische informatie'. Geografische informatie kan gedefinieerd worden als alle gegevens die wenselijk zijn om een kaartbeeld betekenisvol te maken. Dat verschilt per bedrijfsfunctie. Voorbeeld: voor de GHOR in de bedrijfsfunctie "netwerkmanagement" is De Witte Kaart administratieve informatie; in de bedrijfsfunctie 'op- en afschaling' wordt diezelfde Witte Kaart (via LCMS) ineens geografische informatie. Dezelfde gegevens worden in die bedrijfsfunctie op een kaartbeeld getoond.
2. Enkele van de locatiegebaseerde basisregistraties kennen sectorale 'plus-lagen', zo ook voor de OOV sector. Het bekendste voorbeeld is de BGT, waar vele sectoren hun wensen hebben aangedragen voor hun sectorale 'plus-laag'. Dergelijke sectorale inbreng wordt landelijk georganiseerd, via de landelijke Vakgroep Geo & Basisregistraties.
3. Het terugmelden van fouten ("bij gereede twijfel aan de juistheid") geldt voor alle typen registraties. De hiervoor benodigde functionaliteit is echter veelal nog niet beschikbaar. Dit is belangrijk voor het behalen van het gewenste kwaliteitsniveau van de registraties en motivatie om de basisregistraties en kernregistraties te blijven gebruiken. Ook hieraan dient op landelijk niveau prioriteit te worden gegeven.
4. Geografische gegevens worden bij voorkeur zoveel mogelijk direct bij landelijke bronnen (PDOK, Geo4OOV) betrokken, tenzij beschikbaarheid/performance/storage/security redenen een regionale of lokale opslag vereisen. Dit fungeert dan als 'cache' van de bron.

5. Per bedrijfsfunctie kan geografische informatie worden bekeken, geanalyseerd en bewerkt (naast algemene functies zoals maken, beheren, delen, printen, en exporteren). In 2013 is in twee speciale Geo-workshops in kaart gebracht welke bedrijfsfuncties op welke wijze gebruik maken van Geo. Hieruit bleek dat bijvoorbeeld dat veel geo-analyses input vormen voor een volgend bedrijfsproces.
6. GIS vormt in technische zin een geheel van ICT (software en hardware), gegevens en methoden (workflow ondersteuning). In menselijke zin hoort daar ook nog de organisatie en de kennis en creativiteit bij. De VeRA stelt geen eisen aan GIS anders dan het algemene uitgangspunt dat open data en de facto open standaarden zoveel mogelijk worden ondersteund. De term de facto betekent 'uit de praktijk'. Shapefiles bijvoorbeeld zijn strikt genomen geen open standaard, maar zijn in de praktijk wel een open standaard geworden en zijn dus toegestaan. Voorbeelden van andere toegestane formaten zijn: PostGIS, GeoJSON, SpatialLite, CSV, Excel, FGDB, KML, GeoTIFF, IMG, XYZ, en wat webservices betreft: WMS, WMTS, WFS, WCS, WMC, WPS. De actuele lijst met toegestane de facto standaarden wordt in een apart document gepubliceerd.
7. Op basis van de 'bodemplaat' wordt op landelijk niveau een koppeling gelegd tussen kaartlagen en het gegevensboek, zodat het opvragen van kaartlagen gebeurt met een term die onder beheer valt en zodat er een begrijpelijke legenda bij de gegevens gevoegd kan worden.
8. Iconen (pictogrammen) volgen de NEN 1414-plus standaard, voor zover mogelijk en relevant. Deze standaard is in beheer bij de landelijke NEN standaardisatiecommissie.

4.4 Gegevensuitwisseling

4.4.1 Typen gegevens uitwisseling

Koppelingen tussen applicaties kunnen heel divers zijn. Niet alleen in de functionaliteit of gegevens die worden uitgewisseld, maar vooral in de manier waarop die uitwisseling plaatsvindt. In deze diversiteit zijn wel standaardpatronen te herkennen. Dit worden ook wel integratiestijlen genoemd.

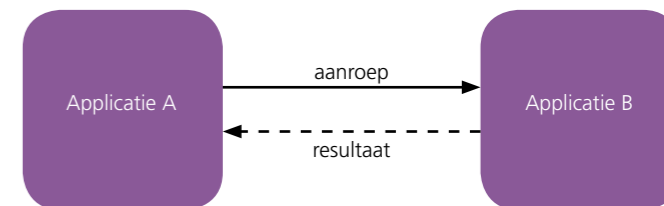
Om te voorkomen dat de complexiteit van koppelingen te groot wordt, is het noodzakelijk om te streven naar een beperkt aantal integratiestijlen, en een aantal afspraken te maken over de manier waarop die worden ondersteund. Zo kan de complexiteit worden vermindert en het beheer worden vereenvoudigd. De gewenste integratiestijlen zijn:

- Service of functieaanroep;
- Berichtuitwisseling;
- Bulkuitwisseling (minst gewenst).

Elk van deze integratiestijlen heeft bepaalde kenmerken en daarmee een bepaald toepassingsgebied waarvoor het bij uitstek geschikt is. Bulkuitwisseling is ten opzichte van de andere twee integratiestijlen minder gewenst. De actualiteit van de gegevensuitwisseling ligt lager en er wordt meer informatie uitgewisseld dan nodig is. De andere integratiestijlen vragen wel een modernere omgeving, waardoor bulkuitwisseling toch vaak als een 'second-best' oplossing wordt toegepast. Er zijn wel situaties, zoals de uitwisseling met een datawarehouse, waarvoor bulkuitwisseling wel geschikt is.

Service- of functieaanroep

Deze integratiestijl houdt in dat een applicatie direct een service (of functie) van een andere applicatie aanroept.



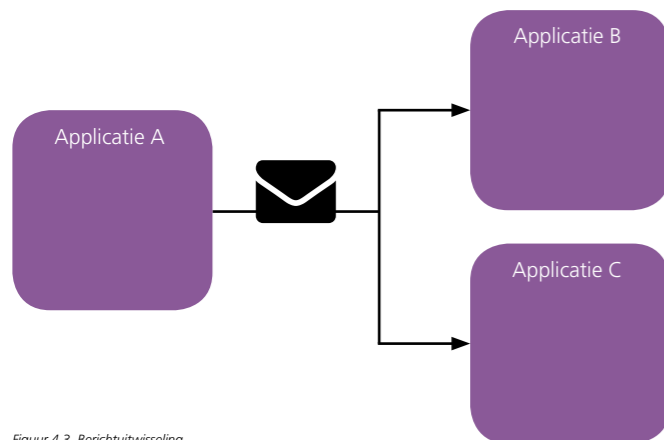
Figuur 4.2. De service- of functieaanroep

Dit type koppeling is over het algemeen synchroon, wat betekent dat de applicatie afhankelijk is van de beschikbaarheid van applicatie B, en wacht op het resultaat van de service- of functieaanroep.

Voor dit type koppelingen is het concept van services het uitgangspunt, wat betekent dat applicaties bepaalde functies beschikbaar stellen als services. Technisch gezien kunnen deze services op verschillende manieren worden geïmplementeerd. De keuze is om hiervoor te standaardiseren op web services. Bij deze integratiestijl is het belangrijk om te allen tijde betrouwbare verbindingen te hebben.

Berichtuitwisseling

Deze integratiestijl houdt in dat een applicatie een bericht stuurt naar één of meerdere andere applicaties.



Figuur 4.3. Berichtuitwisseling

Deze integratiestijl is doorgaans asynchroon, wat betekent dat applicatie A het bericht verstuurt zonder op een antwoord te wachten. Vaak heeft het bericht de betekenis van het verzenden van een gebeurtenis (een event), waarop één of meerdere andere applicaties moeten reageren. Voor applicatie A is het alleen maar van belang dat het bericht correct verstuurd en ontvangen is. Wat de andere applicatie(s) ermee doen is voor applicatie A niet van belang.

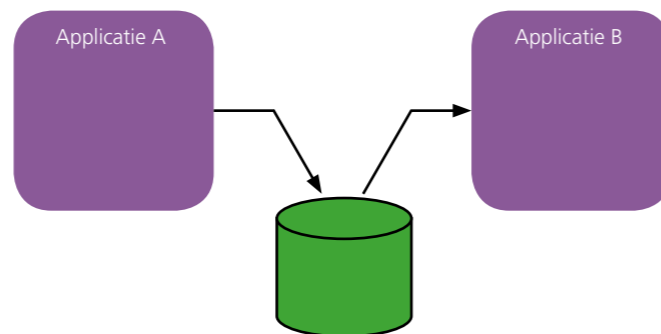
Het belangrijkste is hier, dat er standaardisatie van berichtstructuren mogelijk wordt door alle berichten als XML-berichten te definiëren.

Bulkuitwisseling

Deze integratiestijl houdt in dat een verzameling gegevens, vaak periodiek, wordt uitgewisseld met een andere applicatie.

Deze integratiestijl heeft het karakter van een export door applicatie A, gevolgd door een import door applicatie B. Het enige wat beide van elkaar nodig hebben is een gedeelde voorziening voor gegevensopslag waar beide gebruik van kunnen maken.

Net als bij de berichtuitwisseling wordt gestandaardiseerd op XML, met de mogelijkheid om de berichtstructuren met behulp van XSD-specificaties te standaardiseren.

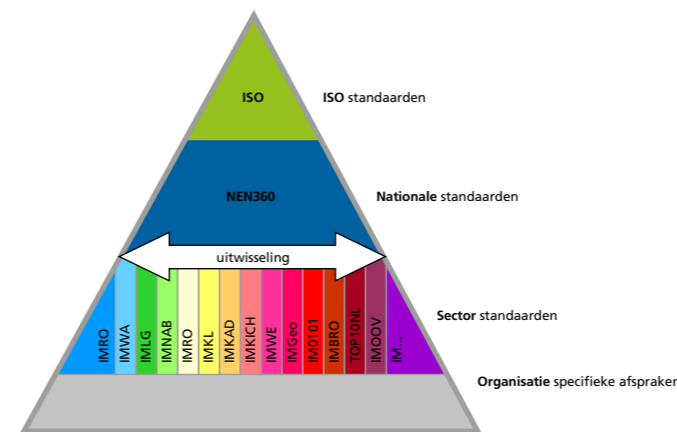


Figuur 4.4. Bulkuitwisseling

4.4.2 Standaarden voor gegevens uitwisseling

Geografische gegevensuitwisseling

Er is door de geografische specialisten van de Veiligheidsregio's gekozen voor het raamwerk van geografische standaarden dat valt onder de NEN 3610 dat in beheer is bij Geonovum. Onder deze familie van standaarden valt het overkoepelend informatiemodel IMGEO2 en de internationale standaard CityGML.



Figuur 4.5. Algemeen Basismodel geo-informatie (NEN3610)

In figuur 4.5 wordt voor de sector openbare orde en veiligheid de sectorstandaard IMOOV vermeld. Deze sectorstandaard wordt binnen de VeRA voor geografie vervangen door IMGEO2. Binnen de VeRA kiezen we voor het IMGEO informatiemodel. De nieuwe versie van I-DBK voor de digitale bereikbaarheidskaart voldoet aan deze standaard. De DBK wordt daarmee onderdeel van de gehele objectenorganisatie van een regio. Een object bevat attributen met verschillende gebruikdoeleinden en mate van detail. Onderdelen van dit stelsel zijn de uitwisselformaten WMS, WFS, WMC en WPS. Bij de vastlegging van de gegevens over objecten hebben BGT-plichtige bronbeheerders van de gehele infrastructuur (basisregistratie grootschalige topografie) vanaf 2016 de verplichting en de keuze om hun gegevens vast te leggen volgens het informatiemodel van de BGT standaard of conform IMGEO2. De Veiligheidsregio's dienen er op aan te dringen dat men IMGEO2 hanteert met een grotere detaillering voor de relevante attributen van het object, zoals ventilatieopeningen van een tunnel.

Semantiek

Semantiek betreft de manier om gegevens en kennis van labels (bv. trefwoorden, registers, nummers) te voorzien, zodat stukjes informatie koppelbaar en vindbaar worden. De belangrijkste bijdrage van semantiek is dat dit milde harmonisatie oplevert in plaats van brute standaardisatie. Moderne trefwoordkunde maakt gebruik van flexibele termenlijsten (taxonomieën en ontologieën) die variatie toelaten tussen kolommen of zelfs in zekere mate tussen Veiligheidsregio's. Dit houdt in dat niet iedereen hetzelfde woord of symbool hoeft te gebruiken, maar voor de gebruiker ziet het er wel hetzelfde uit. Dit maakt semantiek bij uitstek het nieuwe ontwikkelgebied voor crisisbeheersing en voor de relatie tussen alle sectoren en ketenpartners.

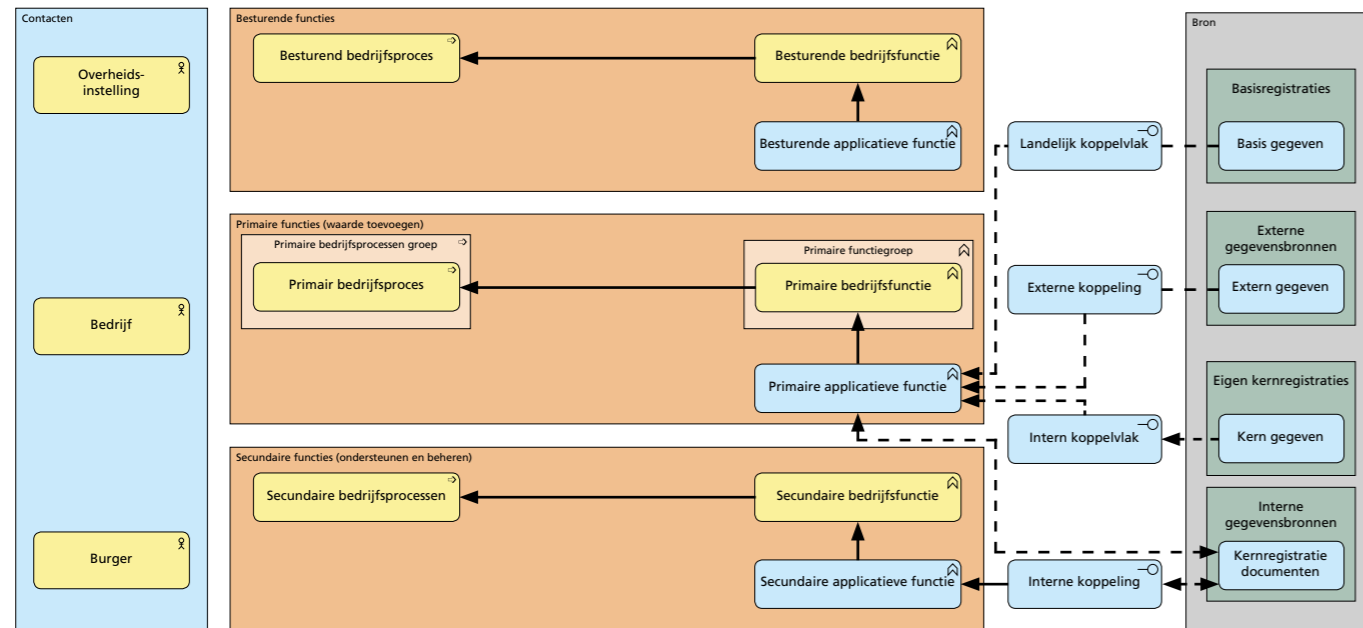
Er wordt aangesloten bij een landelijk en een internationaal stelsel. Dit betreft enerzijds de aansluiting bij de intentie van de Nederlandse overheid om te bewegen naar een zo groot mogelijk aanbod van gegevens in het kader van 'Open Linked Data'. Anderzijds betreft het de nauwkeurige omschrijving van begrippen, symbolen en de dilemma's bij de definitie van deze begrippen dat dit alleen gefaciliteerd kan worden in een flexibel stelsel van naar elkaar verwijzende en goed onderhouden bibliotheken met gecontroleerde termen.

De standaarden voor Semantiek en Geografie worden aangegeven door het W3C, de NEN en Europese programma's als INSPIRE. De veiligheidsregio's hanteren hierbij RDF als standaard voor de uitwisselbaarheid van bibliotheken met gecontroleerde termen en symbolen. Deze standaard biedt de mogelijkheid voor het verbinden van termen aan URI's (Unique resource identifier). Hiermee wordt een stelsel van onderlinge, flexibele en onderhoudbare termen mogelijk gemaakt. Hierbij is SKOS-XL (simple knowledge organization system - extended) de standaard voor het beheer en het redeneren met concepten.

4.5 Samenhang bedrijfsarchitectuur en informatie architectuur

In de voorgaande paragrafen zijn de applicatieve functies en de bijbehorende gegevens benoemd, en is beschreven op welke wijze gegevens uitgewisseld kunnen worden. Deze componenten van de referentiearchitectuur staan niet los van elkaar, er zijn verbanden te benoemen. Deze componenten van de informatie architectuur staan ook weer in verband met de eerder beschreven bedrijfsarchitectuur. In deze paragraaf wordt dit nader toegelicht.

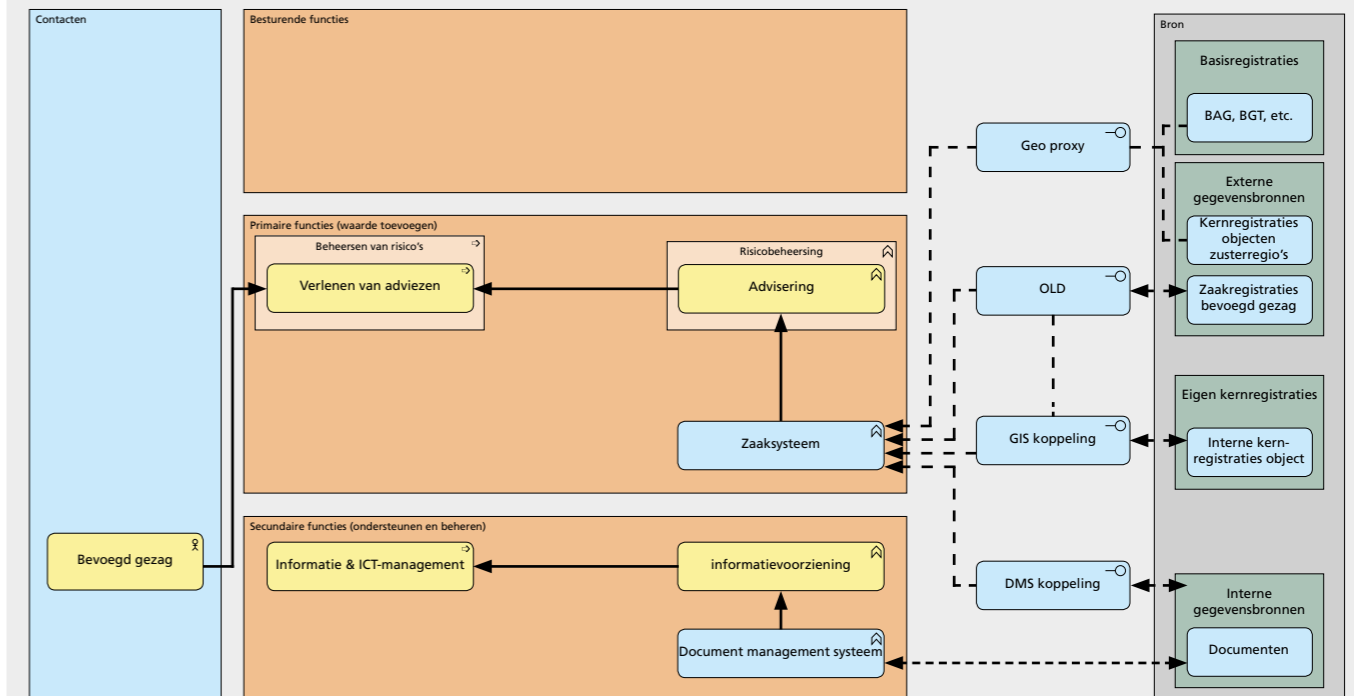
In figuur 4.6 wordt het verband tussen de processen, de bedrijfsfuncties en de gegevens weergegeven. Binnen een proces worden er één of meerdere bedrijfsfunctie aangeroepen. Deze bedrijfsfuncties worden op hun buurt ondersteund door applicatieve functies. Deze kunnen generiek zijn, oftewel gebruikt worden door meerdere bedrijfsfuncties, of specifiek voor de bedrijfsfunctie. De data voor deze applicatieve functie worden geleverd binnen de applicatieve functie zelf (interne gegevensbron) of wordt middels een koppeling opgehaald uit externe databronnen.



Figuur 4.6. Verband tussen processen, bedrijfsfuncties en gegevens

Toelichting

Dit concept is in figuur 4.7 uitgewerkt voor het proces 'verlenen van adviezen'. Eén van de bedrijfsfuncties die hiervoor aangeroepen wordt is 'advisering'. De bedrijfsfunctie advisering maakt gebruik van de generieke applicatieve functie 'zaaksysteem'. Dit zaaksysteem maakt gebruik van interne en externe koppelingen om data op te halen vanuit het bevoegd gezag (OLO), vanuit interne gegevensbronnen (DMS koppelingen) en haalt via een geo proxy server GIS informatie op vanuit de basisregistraties en andere externe gegevensbronnen.



Figuur 4.7. Voorbeeld: 'verlenen van adviezen'



5 Beheer

5.1 Waarom beheer

Applicaties worden ingezet om de bedrijfsprocessen binnen de veiligheidsregio te ondersteunen. Vaak worden projecten gestart om de aanschaf en implementatie van een dergelijk systeem te begeleiden. Met een feestelijke kick-off wordt het gebruik ervan ingeluid. Echter, met de aanschaf en implementatie van een applicatie ben je er nog niet. De omgeving wijzigt continu. Voortdurend moet worden gezorgd dat het informatiesysteem blijft voldoen aan de eisen en wensen van haar gebruikers en het proces dat zij ondersteunt. Om dit te borgen is het noodzakelijk om beheer van de applicatie en de daarbij behorende informatievoorziening in zijn geheel te organiseren. Vaak krijgt beheer binnen de veiligheidsregio's weinig aandacht. Daarom is besloten om in de VeRA een hoofdstuk te wijden aan beheer met als doel aandacht te vragen voor met name functioneel beheer en de inrichting van informatiemanagement binnen de regio.

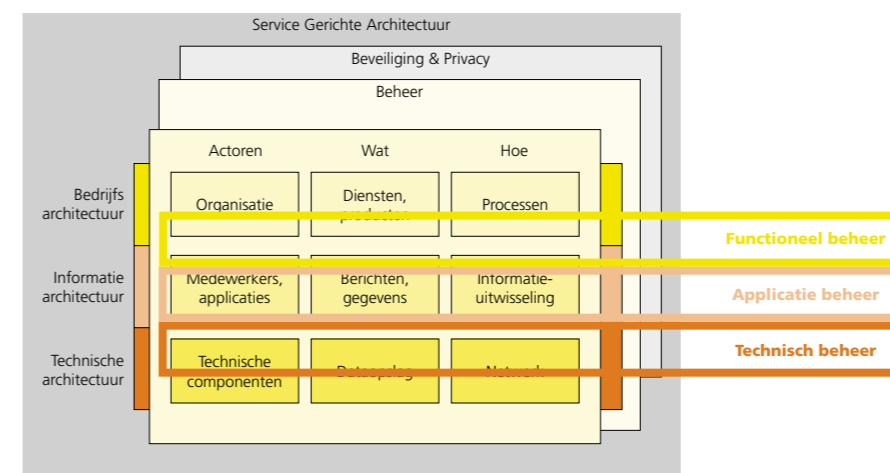
5.2 Wat is beheer?

Figuur 5.1 geeft een overzicht van typen beheer.

Om de totale informatievoorziening te beheren zijn de volgende soorten beheer te onderscheiden:

- 1 Gegevensbeheer. Hier is in Hoofdstuk 4 al het nodige over geschreven.

- 2 Functioneel beheer (standaard BSL)
Functioneel beheer houdt zich bezig met het beheren van de informatievoorziening binnen een Veiligheidsregio. De applicaties worden gebruikt door de gebruikersorganisatie en moeten eventueel door veranderende eisen: 1) anders worden ingericht door de functioneel beheerder of 2) worden aangepast door de applicatiebeheerder. Het beschrijven van deze wijzigingen, het (laten) doorvoeren van de voorgestelde wijzigingen en het controleren van de wijzigingen behoort tot het takenpakket van Functioneel Beheer. De functioneel beheerder stuurt de applicatiebeheerder aan.
- 3 Applicatiebeheer (standaard ITIL en ASL)
Applicatiebeheer houdt zich bezig met de creatie, beheer en wijzigen van applicaties naar aanleiding van geconstateerde fouten of veranderende technische of functionele eisen. Dit zal veelal bij de leverancier van de desbetreffende applicatie belegd zijn. Over deze dienstverlening dienen dan ook afspraken gemaakt te worden bij de aanschaf of ontwikkeling van de applicatie.
- 4 Technisch beheer (standaard ITIL)
Dit beheer richt zich op het instandhouden, beheren en onderhoud van de IT-infrastructuur en heeft ITIL als standaard. De IT-infrastructuur is de basis waarop applicaties kunnen draaien en bestaat uit het netwerk, de computers en operating systems en overige randapparatuur.



Figuur 5.1. Soorten beheer van applicatieve functionaliteit (Bron: NORA2).

5.3 Functioneel beheer

Functioneel beheer beslaat drie niveaus: strategisch, tactisch en operationeel. Op het strategische niveau wordt de bedrijfsarchitectuur als afgeleide van de sectorale referentiearchitectuur (VeRA) ontwikkeld en beheerd. Op tactisch niveau worden project start architecturen ontwikkeld welke passen binnen de bedrijfsarchitectuur. Operationeel functioneel beheer betreft het onderhouden van de informatievoorziening. Om dit goed te beleggen bij een Veiligheidsregio gelden de volgende richtlijnen:

1 Beleg het functioneel beheer binnen de Veiligheidsregio zelf en nooit extern

Functioneel beheer is een spijlfunctie. De functioneel beheerder zorgt er immers voor dat de informatievoorziening optimaal blijft aansluiten bij de gebruikersorganisatie (bedrijfsarchitectuur). Dit is iets waarop een Veiligheidsregio altijd zelf regie over wil blijven voeren.

2 Beleg het functioneel beheer niet kwetsbaar

Dit wil zeggen dat er altijd meerdere personen binnen een Veiligheidsregio aanwezig moeten zijn die het operationeel functioneel beheer kunnen voeren over een applicatie. Bij vakantie of ziekte is de continuïteit dan de applicatie dan geborgd.

3 Functioneel beheer is een vak apart

Beleg het operationeel functioneel beheer niet bij een 'superuser' van de applicatie. De benodigde vaardigheden en competenties van een functioneel beheerder zijn wezenlijk anders dan die van een vakinhoudelijk medewerker. De praktijk leert tevens dat de prioriteit van een vakinhoudelijk medewerker altijd bij de afhandeling van het bedrijfsproces zal liggen en niet bij de continuïteit of doorontwikkeling van de applicatie.

4 Wijs verantwoordelijken aan als eigenaar van een informatiesysteem

Er is een grijs gebied tussen functioneel beheer en het beheer van de content in applicaties. Het beheer van de content is nadrukkelijk de taak van business. Dit wordt lastiger bij ketens en kernregistraties die afdeling overstijgend zijn. De functioneel beheerder kan vanuit zijn expertise de business adviseren bij het in beeld brengen van de keten en het inrichten van ketenregie op de informatie.

5 Gebruik BISL als leidraad om functioneel beheer en informatiemanagement in te richten

De VeRA adopteert BISL als raamwerk om functionele gebruikersbehoefte te vertalen naar functionele specificaties. BISL zijn best practices om functioneel beheer en informatiemanagement in te richten.

5.4 BISL

De toepassing van BISL (Business Information Services Library) zorgt ervoor dat de informatiebehoefte vanuit verschillende bedrijfsprocessen van een organisatie worden vertaald. Dit wordt samengevat onder de term 'informatiemanagement'¹. In de praktijk wordt de term 'informatiemanagement' alleen gebruikt voor de strategische en tactisch activiteiten. Voor operationele (dagelijkse) activiteiten wordt meestal de term functioneel beheer gebruikt.

De VeRA erkent de toepassing van BISL voor het uitvoeren van functioneel beheer en informatiemanagement. Het is een raamwerk dat zich met name richt op de gebruikersorganisatie (vraagzijde) en niet op de ICT-organisatie (aanbodzijde). In dit raamwerk staat beschreven hoe de gebruikerswensen vertaald worden naar functionele specificaties (functioneel beheer) en hoe de toekomst bepaald wordt van de informatiesystemen binnen de veiligheidsregio (informatiemanagement).

BISL biedt handvatten op richtinggevend, sturend en uitvoerend niveau en sluit aan op andere raamwerken zoals ASL voor applicatiebeheer (Application Services Library: processen van het beheer, onderhoud en vernieuwing van informatiesystemen en applicaties) en ITIL voor technisch beheer (Information Technology Infrastructure Library: beheerprocessen binnen de ICT organisatie).

¹ Informatiemanagement moet niet verward worden met Operationeel Informatiemanagement tijdens de warme fase.



6 Actuele en toekomstige ontwikkelingen

Semantiek

In VeRA 1.0 werd door het kernteam aangegeven dat semantiek een onderwerp van de toekomst zou worden. Dat is natuurlijk nog steeds zo. De OOV-sector heeft met de bouw van het gegevensboek, de Firebrary en het iNowit platform zeker stappen gezet. Semantiek is nu een aanvaard kernbezit van een sector aan het worden, omdat in de digitale wereld de goed gedefinieerde vaktermen letterlijk het vakmanschap beschikbaar en uitwisselbaar maakt. Na de vaststelling van de LMC (Landelijke meldingsclassificatie) wordt door onze experts de definitie van andere reeksen termen (vakbekwaamheid, duiken, dekking en risico, enzovoorts) nu voortvarend aangepakt, inclusief het beheer van de termen en gegevensdefinities.

Landelijke Meldkamer Organisatie (LMO)

De meest evidente nieuwe ontwikkeling is de relatie met de Landelijke Meldkamerorganisatie, de LMO. VERA 2.0 is nadrukkelijk geschreven met deze centralisatie in het achterhoofd, omdat juist dan de ketensamenwerking - vanuit het veld naar de meldkamer en terug - relevant wordt. Die samenwerking gebeurt niet vanzelf en vergt een gezamenlijke investering in 'koud multi'. Een gebiedsgerichte aanpak maakt duidelijk dat het voor alle betrokken partijen relevant is om informatie te hebben over objecten, gebouwen, personen in dat gebouw en de aanwezige vitale infrastructuur. Het delen van die informatie is voor de meeste overheidspartijen een vanzelfsprekendheid aan het worden.

Zelfredzaamheid

Bij GHOR en GGD is het klantbewustzijn sterk aanwezig en er valt in dat kader veel te leren over nieuwe concepten als resilience of weerbaarheid, zelfredzaamheid en samenwerking met onze burgers. De nieuwe media worden hierbij al toegepast en mengvormen tussen interne robuuste systemen en crowd-systemen in de buitenwereld zullen zich meer en meer voordoen. Er ontstaan steeds meer open ontwikkelplatform voor het bevorderen van de veiligheid van bijvoorbeeld de ouderen in de samenleving. Deze informatietechnologie brengt ook nieuw werk voor de Veiligheidsregio met zich mee. Kennisontwikkeling op dit gebied wordt belangrijker.

Basisregistraties en kernregistraties

De invoering van de BGT (basisregistratie grootschalige topografie) vanaf 2016 versterkt de invoering en het gebruik van basisregistraties en kernregistraties. Dit geldt daarnaast voor PDOK (publieke dienstverlening op de kaart) en de bouw van sectorale geo-knooppunten. We kunnen meer en meer met elkaar uitwisselen en de gedachte van die ene super database voor alle gebruikers is definitief over. De DBK migreert naar een kernregistratie van objecten in overeenstemming met de WvR, artikel 2.3.1.

Workflow en zaakgericht werken

In het administratieve front wordt hard gewerkt aan nieuwe modellen voor de workflow vanuit kernregistraties in de eHRM en eFIN systemen naar voor ons werk belangrijke instrumenten zoals de applicatieve functie 'roosteren' en de bedrijfsfunctie 'opleiden'. Tegelijkertijd ontstaat een bottom-up benadering voor het roosteren vanuit de individuele mobiele telefoon. Documenten, dossiers en webpagina's groeien naar elkaar toe in generieke document- en zaakplatforms voor alle teksten met goede metadata en steeds minder email. Dit leidt tot systemen die voldoen aan de archiefwet.

Methodologie

Een van de nieuwe ontwikkelingen die binnen het toekomstig IFV lectoraat informatievoorziening opgepakt zal worden, is het meetbaar maken van de informatiepositie. Bij de professionalisering van ons vak hoort dat we wetenschappelijke methoden ontwikkelen om te weten of hoe goed we het doen en wanneer het goed genoeg is.

Ketensamenwerking

Een tweede punt dat duidelijk wordt is onze rol in het economisch verkeer van het logistiek knooppunt Nederland ten opzichte van Europa. Een ongeluk in een van onze vele transportaders levert meteen een infarct op waar half Europa last van kan hebben. De samenwerking op het gebied van informatie-uitwisseling, bijvoorbeeld over vracht en lading met Spoor, Haven en Wegverkeer wordt hierdoor steeds belangrijker.

Social media

Er bestaat een natuurlijk spanningsveld tussen Architectuur en dat wat men 'Social Media' zoals Crowd-control¹, CrowSourcing² en Mobiele apps³ is gaan noemen. Social media beweegt zich op het vlak van grote aantallen personen die met elkaar communiceren met behulp van beeld, geluid en tekst. De podia wisselen snel, zoals bijvoorbeeld de geschiedenis van Hyves en FaceBook aantoont. Men stapt nu weer massaal over naar mobile apps zoals 'instagram'⁴. Die podia kenmerken zich door één commerciële aanbieder, die in een hoog tempo massale aantallen gebruikers moet bedienen. De keuze voor de podia wordt vaak bepaald door de gebruiksvriendelijkheid. Architectuur

¹ Applicaties als twitcident ondersteunen het aansturen van menigten bij evenementen. De monitoring van Twitter berichten geeft een beeld van de sfeer in de crowd.

² Applicaties als Google Crisis Response maken gebruik van crowdsourcing voor het ontvangen van informatie van burgers, die niet kunnen inloggen op LCMS.

³ Een applicatie (app) die speciaal is ontwikkeld voor een mobiele device.

⁴ Rapport: <http://blog.globalwebindex.net/facebook-teens-decline>

heeft met name als missie om in de complexe wereld van software en hardware enige standaardisatie, structuur en continuïteit te brengen⁵. Traditioneel is het perspectief gericht op software aangeboden door meerdere aanbieders, waarbij meerdere applicaties gedurende langere tijd met elkaar moeten kunnen 'praten'. Wat kan architectuur voor de veiligheidsregio's betekenen in deze context?

De kracht van de Social Media is tegelijkertijd de zwakte. Het is een front-end applicatie interface en geeft een goed beeld van de gebruikerswensen. Integratie van gegevens of processen aan de achterkant is bijna onmogelijk.

Samenvattend kan voor Social Media gesteld worden dat er een aantal applicatieve functies en bedrijfsfuncties mee gediend is. Bestuursfuncties als risicoanalyses, communicatieve functies en loketfuncties worden bijvoorbeeld gemakkelijker en gebruiksvriendelijker. De uitdaging is om deze applicaties en podia te verbinden met systemen die robuust en betrouwbaar moeten zijn. Daar waar ze niet verbonden behoeven te worden zijn issues als privacy, beveiliging en verwachtingsmanagement punten van aandacht.

Open Linked Data

Sinds enige tijd wordt bij regio's zoals Amsterdam-Amstelland of Hollands Midden geëxperimenteerd met het verzamelen, het analyseren en het slim toepassen van zogenaamde 'Open data'. Doordat men grote hoeveelheden gegevens vergaart, kan men trachten om voorspellende uitspraken te doen over risico's, dekking en locaties van kazernes.

In een aantal gevallen is sprake van real time data, zoals het tot stand brengen van een real-time kaart over de toestand van een gebouw of een real time bereikbaarheidskaart, die on the fly samengesteld wordt uit meldkamerkladblok, open data en business rules.

⁵ Proefschrift Jan Truijens, oud-voorzitter architectuurvereniging en ex-CIO Rabobank

'Open Linked data' is de VERA versie van 'Open data', waarbij de gegevens gekoppeld worden aan betekenis en termen die onderhoudbaar zijn in trefwoordenregisters als het Brandweer gegevensboek. Dit maakt geautomatiseerde complexe analyses en scenario-uitwerkingen mogelijk. Dit gebeurt in lijn met de W3C standaarden van semantic web. Daarmee worden de gegevens overdraagbaar en reproduceerbaar.

Privacy

De Veiligheidsregio heeft voor een aantal processen en functies te maken met privacy. Dit geldt bijvoorbeeld voor de meldkamer, voor die regio's met een GGD en voor bedrijfsgevoelige gegevens bij het handhaving- en vergunningsdossier. Voor privacy geldt in eerste instantie dat de regio zich houdt aan de regels van de wet en het college bescherming persoonsgegevens. Dit houdt in dat men zonder verkregen toestemming gegevens over bedrijven en personen niet langer vasthoudt dan strikt noodzakelijk is, dat men deze gegevens bewust vernietigt en dat wanneer er inbreuk gedaan wordt op de privacy, dat dit gebeurt met de expliciete opdracht van een leidinggevende en dat men verantwoording kan afleggen over de handelswijze. Het argument voor inbreuk is 'gerede twijfel'. Iedere veiligheidsregio dient daartoe een set van voorbeeldscenario's op te stellen waarbij gegevensuitwisseling noodzakelijk geacht wordt. Hier kan naar verwezen worden bij de verantwoording, omdat er dan geprotocolleerd gehandeld wordt conform de wet.

Daarnaast heeft de regio te maken met de wet politiegegevens⁶. Deze wet legt nog strengere normen op ten aanzien van de opslag, vernietiging en het expliciet en van te voren protocolleren dan de 'normale wet'. Veiligheidsregio's met een 'multi-intake' en gecoloeerde medewerkers, dienen er op toe te zien dat deze protocollen onderhouden worden.

⁶ http://wetten.overheid.nl/BWBR00224631geldigheidsdatum_19-03-2014

Beveiliging en Architectuur

In dit deel van de VERA wordt niet gedetailleerd ingegaan op de ICT architectuur van beveiliging. Daar waar veiligheidsregio's samenwerken met derden is het van belang om extra aandacht te besteden aan dit onderwerp, omdat 'wij' dan immers met de gegevens van een andere partner werken. In de discussie rond het koppelvlak met de NMS (applicatieve functie nieuwe landelijke meldkamer) is er voor gekozen om te werken met een 'role based access in combinatie met een 'trigger-architectuur'.

Het is te complex om role based access tot op elk attribuut van een object te definiëren. Het is bijvoorbeeld onmogelijk en niet onderhoudbaar om alleen een TAS-bevelvoerder toegang te geven tot de eigenschap van een pand die luidt: 'vuurgevaarlijk'. Het is wel mogelijk om met de LMO en andere sectoren af te spreken dat bij een bijzonderheid van een object alle betrokken geïnformeerd worden over het feit dat er iets bijzonders aan de hand is – op het moment dat dit object onderdeel wordt van het opgevraagde kaartbeeld. Ten aanzien van objectregistratie delen Veiligheidsregio's informatie volgens het principe van "Ja, tenzij...". Ten aanzien van persoonsinformatie geldt dat Veiligheidsregio's informatie delen onder het regime "Nee, tenzij...".

Big Data

In technologiekringen steekt steeds vaker de term Big Data de kop op. Door steeds geavanceerder hard- en software is het mogelijk meer data te verzamelen, te bewerken en te bewaren. Door steeds krachtiger algoritmes is het mogelijk geworden vanuit deze data patronen en verbanden te ontdekken die het menselijk denkvermogen te boven gaan. Toepassing van deze ontwikkeling vinden we terug in het voorspellende karakter van sommige softwarepakketten. Zowel binnen

de brandweer- als ambulancebranche wordt al voorzichtig gewerkt met het voorspellen van het volgende incident of brand waarbij zelfs voertuigen op basis van deze voorspellingen op de juiste plek worden gepositioneerd.

Koppelen en relateren van de VeRA en de PURA

Voor de Publieke Gezondheid (GGD) is net als voor de veiligheidsregio's een referentiearchitectuur opgesteld. De PURA-versie 1.0 is breed omarmd en daarmee door de DPG'en vastgesteld als gezamenlijke publicatie. Dit betekent dat GGD'en PURA toepassen daar waar nodig. De PURA is opgesteld op basis van het gedachtengoed van de VeRA. De GGD'en werken nauw samen met de veiligheidsregio's en in een aantal gevallen zijn ze zelfs in één organisatie. Eén van de volgende ontwikkelstappen van beide referentiearchitecturen zal zijn om deze aan elkaar te gaan relateren, omdat de onderlinge afstemming vanwege de aanwezige ketenrelaties van belang is en om de samenwerking en kennisdeling verder te bevorderen.



Bijlage A:

wettelijke taken en bevoegdheden veiligheidsregio's

Wettekst van wet van 11 februari 2010, Wet veiligheidsregio's (Wvr), artikel 10

Bij de regeling, bedoeld in artikel 9, worden aan het bestuur van de veiligheidsregio de volgende taken en bevoegdheden overgedragen:

- a) Het inventariseren van risico's van branden, rampen en crises;
- b) Het adviseren van het bevoegd gezag over risico's van branden, rampen en crises in de bij of krachtens de wet aangewezen gevallen alsmede in de gevallen die in het beleidsplan zijn bepaald;
- c) Het adviseren van het college van burgemeester en wethouders over de taak, bedoeld in artikel 3, eerste lid;
- d) Het voorbereiden op de bestrijding van branden en het organiseren van de rampenbestrijding en de crisisbeheersing;
- e) Het instellen en in stand houden van een brandweer;
- f) Het instellen en in stand houden van een GHOR;
- g) Het voorzien in de meldkamerfunctie;
- h) Het aanschaffen en beheren van gemeenschappelijk materieel;
- i) Het inrichten en in stand houden van de informatievoorziening binnen de diensten van de veiligheidsregio en tussen deze diensten en de andere diensten en organisaties die betrokken zijn bij de onder d, e, f, en g genoemde taken.

Wettekst van wet van 11 februari 2010, Wet veiligheidsregio's (Wvr), artikel 22

De besturen van de veiligheidsregio's dragen gemeenschappelijk zorg voor de inrichting van een uniforme informatie- en communicatievoorziening, daaronder begrepen het vaststellen van de informatiebehoefte en het vaststellen van kaders, standaarden en kwaliteitseisen met het oog op de informatie-uitwisseling binnen en tussen de in artikel 10, onder i, bedoelde organisaties.

Besluit Veiligheidsregio's 2010, § 4 Informatiemanagement Artikel 2.4.1

1. Het bestuur van de veiligheidsregio draagt er zorg voor dat binnen de hoofdstructuur van de rampenbestrijding en crisisbeheersing tijdens een ramp of crisis een totaalbeeld wordt bijgehouden;
2. Het totaalbeeld is opgebouwd uit de beschikbare gegevens over:
 - a. het incident, waaronder wordt begrepen:
 - 1° de aard van het incident en de betrokken objecten,
 - 2° de actuele situatie met betrekking tot het incident, en
 - 3° de risico's en de effecten van het incidenttype en de bestrijdingsmogelijkheden;
 - b. de hulpverlening, waaronder wordt begrepen:
 - 1° de bestrijdingsmogelijkheden,
 - 2° de bereikbaarheid voor de hulpverlening, en
 - 3° de risico's voor de hulpverleners en de daarmee samenhangende veiligheidsmaatregelen;

- c. de prognose en de aanpak, waaronder wordt begrepen:
- 1° de verwachting met betrekking tot de ontwikkeling van het incident, de risico's en de effecten ervan ende bestrijdingsmogelijkheden,
 - 2° het slachtofferbeeld, de verwachte ontwikkeling ervan, de noodzakelijke maatregelen en de benodigde hulpverleners en middelen,
 - 3° de risico's voor de bevolking, de verwachte ontwikkeling van deze risico's en de benodigde hulpverleners en middelen,
 - 4° het beeld bij de bevolking van het incident en de risico's, het gedrag van de bevolking, de informatie die aan de bevolking is verstrekt en maatregelen die zijn of worden getroffen, en
 - 5° overige bedreigingen zoals die voor de vitale belangen, het milieu of de economie, de verwachte ontwikkeling ervan en de benodigde hulpverleners en middelen;
- d. de getroffen maatregelen en de resultaten ervan, waaronder wordt begrepen:
- 1° de actuele bestrijdingsorganisatie,
 - 2° de voorstellen en besluiten over de bestrijdingsstrategie, de inzetplannen en de benodigde hulpverleners en middelen,
 - 3° de feitelijke inzet en uitvoering van de bestrijding, en
 - 4° de voortgang van de inzet en de uitvoering, de bijstelling van besluiten of de uitvoering ervan en de bereikte resultaten;
3. Het totaalbeeld wordt langs geautomatiseerde weg zo spoedig mogelijk en voor zover dat redelijkerwijs mogelijk is geverifieerd, beschikbaar gesteld aan:
- a. de onderdelen van de hoofdstructuur van de rampenbestrijding en crisisbeheersing;
 - b. andere bij de ramp of crisis betrokken partijen, voor zover zij deze gegevens nodig hebben voor de uitvoering van hun taken en bevoegdheden, en
 - c. Onze Minister.

Dankwoord

VeRA is tot stand gekomen door een gezamenlijk inspanning van vele personen binnen en buiten de veiligheidsregio's. We willen de volgende personen danken voor hun medewerking aan VeRA:

Kernteam

Bart den Dulk	-	Veiligheidsregio Haaglanden / ArchiXL
Sandra McEwan-Verver	-	Veiligheidsregio Noord- en Oost-Gelderland
Rob Peters	-	Veiligheidsregio Kennemerland
Eurydice van Vliet	-	Veiligheidsregio Brabant-Zuidoost
Edith Langerak	-	Veiligheidsregio Rotterdam-Rijnmond
Jolande van Balen	-	Veiligheidsregio Midden- en West-Brabant
Arno van der Laan	-	Veiligheidsregio Gelderland-Midden

Eindredactie

Jan-Willem van Aalst	-	Imergis
Team Communicatie	-	Bureau Brandweer Nederland

Landelijk Netwerk Kwaliteit

Maaïke van Etten	-	Veiligheidsregio Haaglanden
Wouter Duiniveld	-	Veiligheidsregio Haaglanden
Lineke Berendsen	-	Veiligheidsregio Noord- en Oost-Gelderland
Sietske Houkes	-	Veiligheidsregio Noord-Holland-Noord
Hein Jan Plat	-	Veiligheidsregio Gooi en Vechtstreek
Yvon Bronkhorst	-	Veiligheidsregio Rotterdam-Rijnmond
Linda Hanstede	-	Veiligheidsregio Twente

NIM, Landelijk Netwerk Informatiemanagement

Jan Wiebe Land	-	Noord-Holland-Noord, voorzitter
Bart Groothuis	-	Groningen
Florian Ruijs	-	Fryslân
Nathalie Wobben	-	Drenthe
Richard Kamphuis	-	IJsseland
Gerke Spaling	-	Twente
Susan Stegeman	-	Noord- en Oost-Gelderland
Isabelle van Zadelhoff	-	Gelderland Midden
Josien Ooserhoff	-	Gelderland-Zuid
Gerald Lekkerkerker	-	Utrecht
Wout Buteijn	-	Noord-Holland-Noord
Erwin van Doleweerd	-	Zaanstreek-Waterland
Guido Legemaate	-	Amsterdam-Amstelland
Martin van Loveren	-	Gooi en Vechtstreek
Marieke van den Berg	-	Haaglanden
Marijn Riemens	-	Hollands Midden
Ronald van Leeuwen	-	Rotterdam-Rijnmond
Johan van Ballegooijen	-	Zuid-Holland-Zuid
Erwin Paardekooper	-	Zeeland
Luud Verheijen	-	Midden- en West-Brabant
Piet van Beurden	-	Brabant-Noord
Mario van Wanrooij	-	Limburg-Noord
Ton Borm	-	Zuid-Limburg
Hans Esser	-	Flevoland

Begeleiding Workshops

Edwin de Vries	-	Novius
----------------	---	--------

Afkortingen

BAG	Basisregistratie Adressen en Gebouwen	NVBR	Nederlandse Vereniging voor Brandweezorg en Rampenbestrijding
BGT	Basisregistratie Grootchalige Topografie (v.a. 2016)	PETRA	Provinciale Referentie Architectuur
BISL	Business Information Services Library	PRK	Provinciale Risicokaart
BRP	Basisregistratie Personen	PSA	Project startarchitectuur
BRT	Basisregistratie Topografie	PSH	Psycho Sociale Hulpverlening
COPI	COmmando Plaats-Incident	PSHOR	Psychosociale Hulpverlening bij Ongevallen en Rampen
DPG	Directeur Publieke Gezondheidszorg	PURA	Publieke Gezondheid Referentie Architectuur
EAR	Enterprise Architectuur Rijksoverheid	RUD	Regionale Uitvoerings Dienst (Omgevingsdienst)
EPD	Elektronisch Patiënten Dossier	RGBZ	Referentiemodel Gemeentelijke Basisgegevens Zaken
GEMMA	Gemeentelijk Model Architectuur	RRC	Raad van Regionaal Commandanten
GGD	Gemeenschappelijke Gezondheidsdienst	SGBO	Staf Grootchalig Bijzonder Optreden (politie)
GHOR	Geneeskundige Hulpverlening Organisatie in de Regio	TBO	Team Brand Onderzoek
GRIP	Gecoördineerde Regionale Incidentbestrijdings Procedure	VeRA	Veiligheidsregio Referentie Architectuur
IASV	Informatiearchitectuur Sector Veiligheid	VNG	Vereniging Nederlandse Gemeenten, koepel van gemeenten
IBV	Informatiebeleid Veiligheid (Min. BZK)	Wabo	Wet algemene bepalingen omgevingsrecht
IOOV	Inspectie Openbare Orde en Veiligheid, thans Inspectie VenJ	WILMA	Waterschaps Informatie & Logisch Model Architectuur
IPO	Inter Provinciaal Overleg, koepel van provincies	WBP	Wet bescherming persoonsgegevens
LMO	Landelijke Meldkamer Organisatie	WOZ	Waardebepaling Onroerende Zaken
MMI	Medische Milieukunde en Infectieziektebestrijding	WPG	Wet publieke gezondheid
NHR	Nieuwe Handelsregister, bedrijfsgegevens	Wvr	Wet veiligheidsregio's
NMS	Nieuw Meldkamer Systeem		
NORA	Nederlandse Overheid Referentie Architectuur		

Begrippen

Basisregistratie	Eén van de gegevensverzamelingen die door de Rijksoverheid zijn benoemd in het Stelsel Basisregistraties. Dit betreft authentieke gegevens die niet sectorspecifiek zijn. Voorbeeld: de Basisregistratie Personen.
Bedrijfsfunctie	Een aandachtsgebied waaraan het bedrijf structureel aandacht wil besteden (= energie in wil stoppen, structureel middelen voor wil inzetten) om zijn bedrijfsdoelstelling te realiseren. Een bedrijfsfunctie kan daarom ook gezien worden als een groepering van intern gedrag op basis van een bepaald criterium (bijvoorbeeld plaats (dezelfde afdeling), communicatie, benodigde competenties, gedeelde bronnen en gedeelde kennis). Een bedrijfsfunctie representeert een stuk toegevoegde waarde van de organisatie.
Bedrijfsproces	Een geordende reeks werkprocessen die binnen één organisatie wordt uitgevoerd met als doel om een (combinatie van) dienst(en) te leveren aan een burger, bedrijf of andere organisatie.
Handeling	Kleinst mogelijke eenheid van werk, uitgevoerd door één persoon of machine op één plek op één moment.
Informatiesysteem	Systeem waarmee informatie over objecten of personen beheerd, verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd kan worden. Vaak is dit een computerprogramma.
Informatievoorziening	Het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van die organisatie.
Kernregistratie	Gegevensbronnen die door meerdere processen en systemen kunnen worden gebruikt, niet zijnde een basisregistratie. Kernregistraties bevatten voor een sector (of verzameling sectoren) specifieke en authentieke gegevens. Voorbeeld: de Risicokaart.
Ketenproces	Een geordende reeks services die door verschillende organisaties aan elkaar worden geleverd met als doel om via één organisatie een (combinatie van) dienst(en) te leveren aan een klant, bijvoorbeeld het verstrekken van een vergunning.

Koppelvlak	Systeem- en/of organisatie-overschrijdende gegevensuitwisseling.
Linked open data	Het aanbrengen van samenhang in data door betekenis toe te kennen aan de relatie tussen data, en deze geautomatiseerd opvraagbaar en analyseerbaar maken.
Processtap	Een geordende reeks handelingen die ononderbroken wordt uitgevoerd door één persoon of machine (eenheid van tijd, plaats en handelen).
Referentiearchitectuur	Instrument om samenhang aan te brengen in de informatiehuishouding van een overheidssector en mogelijke samenwerking met partners vorm te geven
Servicegerichte architectuur	Software-architectuur gericht op het ontwikkelen (zo veel mogelijk uit bestaande applicaties en/of softwarecomponenten), doen functioneren en beheren van diensten (services) voor de ondersteuning van systematisch gedefinieerde bedrijfsprocessen met als doel bedrijfsfuncties te kunnen vervullen tegen afgesproken condities.
Werkproces	Een geordende reeks van processtappen die binnen één organisatorische eenheid binnen een organisatie wordt uitgevoerd met als doel een specifieke bijdrage (prestatie) te leveren aan een burger, bedrijf of andere organisatie.

¹ Bron: [NORA 2.0]

² Bron: NORA 2.0

³ Zie artikel 2.2.1 Besluit Veiligheidsregio's

⁴ Alarmering kan niet plaatsvinden zonder uitvoerig overleg tussen kolom en meldkamer.

⁵ Zie ook Wet Veiligheidsregio's : artikel 48 en besluit Veiligheidsregio's , artikel 2.4.1



