Regionale Enterprise Architectuur

Dit document beschrijft de Regionale Enterprise Architectuur van de Gemeenten Arnhem, Renkum, Rheden en De Connectie

Auteur Gerhard Striekwold

Publicatiedatum 15-06-2022
Printdatum 20-06-2022
Versie 2022.2

Inhoud

1 Document Informatie 4
1.1 Versiebeheer 4
1.2 Distributielijst 4
1.3 Goedkeuring 4
1.4 Doelgroep 5
1.5 Bronnen 5
1.6 Definities 6
2 Inleiding 8
2.1 Business drijfveren Gemeente Arnhem 8
2.2 Business drijfveren Gemeente Renkum 10
2.3 Business drijfveren Gemeente Rheden 10
2.4 Business drijfveren De Connectie 12
3 Context Regionale Enterprise Architectuur document 14
3.1 De Regionale Business Architectuur Principes 14
3.2 De Regionale Informatie Architectuur principes 17
3.3 De Regionale Technische Architectuur principes 21
3.4 De Regionale Beveiliging Architectuur principes 26
4 Het Architectuur Model 30
5 Gebruik van de Regionale Enterprise Technische architectuur 31
5.1 Producten & Diensten Catalogus 31
5.2 Architectuurcyclus 32
5.3 Het Architectuur proces en architectuur document 33
6 Architectuur roadmap 34
7 Architectuur Kaders 36
7.1 Sourcing 36
7.2 Netwerk Design 36
7.3 Intergemeenschappelijk verkeer – samenwerking 36
7.4 Voortbrengingsmethodiek ICT middelen 36
7.5 De Werkplek 37
7.6 Common Ground, de toekomstige informatievoorziening 37
7.6.1 Gegevens laag 38
7.6.2 Service- en Integratie laag 38
7.6.3 Business Rules en Interactie laag 38
8 Dataclassificatie 39
9 Beheer 48
10 Bijlage A – Services Store 49
10.1 Datacenter diensten 49
10.2 IaaS diensten 50

10.3 PaaS diensten....50
10.4 SaaS diensten....50
10.5 Workspace diensten....50
11 Bijlage B – Operations....50
12 Bijlage C – Katern GEMMA Architectuurprincipes....51
12.1 Onze gemeente biedt de klant een goede informatiepositie....52
12.2 Onze gemeente denkt vanuit de positie van de klant....52
12.3 Onze gemeente digitaliseert haar diensten en processen....53
12.4 Onze gemeente gaat op een vertrouwelijke manier met gegevens om....54
12.4.1 Onze gemeente gebruikt generieke processen en functies....54
12.4.2 Onze gemeente hergebruikt gegevens....55
12.4.3 Onze gemeente stelt openbare gegevens als open data beschikbaar....56
12.4.4 Onze gemeente voert regie over uitbestede diensten....56

1 Document Informatie

1.1 Versiebeheer

Versie:	Datum:	Naam:	Omschrijving / Documentaanpassingen:
2019.1	26-02-2019	Gerhard Striekwold; Simeon Bakker	Geaccordeerde versie MT-ICT
2019.2	29-10-2019	Gerhard Striekwold	Geaccordeerde versie TLO – ICT & Strategisch Architectuur Overleg
2020.1	18-11-2019	Gerhard Striekwold	Aanpassingen en aanvullingen
2020.1	18-03-2020	Gerhard Striekwold	Aanpassingen BIO (Hoofdstuk 7), uitwerking van de principes
2020.2	01-07-2020	Gerhard Striekwold	Aanpassingen CISO en TLO op 2020.1 verwerkt
2020.2	30-09-2020	Gerhard Striekwold	Document aangepast met het ontwikkelperspectief 2020-2024
2021.1	01-05-2021	Gerhard Striekwold	Regulier onderhoud en toevoeging/uitbreiding van de Common Ground kaders.
2021.2	10-11-2021	Gerhard Striekwold	De 1e versie van de Regionale Enterprise Architectuur
2022.1	22-02-2021	Gerhard Striekwold	Aanpassingen Doelen Connectie en de Regionale Business principes, De Regionale Informatieprincipes.
2022.2	01-07-2022	Gerhard Striekwold	Verwerken opmerkingen 2022.1

1.2 Distributielijst

	Versie	
Naam	Datum	2022.2
Architectuur Team	01-10-2022	
REAT		
Informatiemanagers		
RCISO		
RCIOO		

1.3 Goedkeuring

Versie	Datum	Naam	Opmerking
2019.1	26-02-2019	Gerhard Striekwold; Simeon Bakker	Geaccordeerde versie MT-ICT
2019.2	29-10-2019	Gerhard Striekwold	Geaccordeerde versie TLO – ICT & Strategisch Architectuur Overleg
2020.2	28-01-2021	Gerhard Striekwold	Geaccordeerde versie TLO - ICT
2021.2	13-12-2021	Gerhard Striekwold	Geaccordeerde versie RCIOO
2022.1	13-06-2022	Gerhard Striekwold	Geaccordeerde versie RCIOO

1.4 Doelgroep

Dit document is primair bestemd voor Management, Informatie Managers, het Regionaal CIO overleg (RCIO), het Regionaal Chief Information Security Officer overleg (RCISO) en Medewerkers van de gemeenten en De Connectie.

1.5 Bronnen

Document / Bron	Versie / Datum	Status / Auteur
Uitgangspunten Technische ICT-Infrastructuur	1.0 / 01-03-2017	Vastgesteld MT ICT De Connectie
Oplegnotitie Sourcing Strategie	1.0_1 / 04-04-2017	Vastgesteld Directeur de Connectie
Governance Architectuur ICT De Connectie	1.0 / 20-09-2017	Vastgesteld MT ICT De ConnectieOR
Architectuur regionale werkplek	0.1 / 31-01-2017	Gemaakt overleg IM gemeenten
Sourcing Strategie Right Sourcing	0.9 / 21-06-2018	Ter goedkeuring aan gemeenten en de Connectie
I-visie 2018-2021	1.0 / 07-03-2018	Vastgesteld MT De Connectie
Informatiebeveiligingsplan De Connectie 2017-2018	1.0 / 01-05-2018	Vastgesteld MT De Connectie
MARA Hoe het spel wordt gespeeld	1.0 / 27-01-2014	Gemeente Arnhem
Beheren onder Architectuur		Bart de Best
1!Connect architectuur en werkwijze 2020	0.1 / 19-07-2019	Mark Messink
Baseline Informatiebeveiliging Overheid (BIO) ; Handreiking Dataclassificatie BIO	v1.04 26-01-2021	BIO-overheid.nl; https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
Key2Control	1.0	Bestuurlijke principes voor informatiebeveiliging bij gemeenten.
HLD- Centrale Werkplek VDI	0.9 /	Henny Louwers
VNG Gemeentelijk gegevenslandschap	0.2 / januari 2018	VNG – Ad Gerrits
VNG De 10 bestuurlijke principes voor informatiebeveiliging	2019	VNG
API Strategie Algemeen / Geonovum Handreiking	04-02-2020	https://docs.geostandaarden.nl/api/API-Strategie/
API Design Rules (Nederlandse API strategie IIa) 1.0	09-07-2020	https://publicatie.centrumvoorstandaarden.nl/api/adr/
Ontwikkelperspectief 2020-2024 Bedrijfsvoeringsorganisatie De Connectie	2020	Vastgesteld Bestuur en MT De Connectie
https://www.gemmaonline.nl/index.php/Overzicht_GEMMA_Architectuurprincipes	2021	VNG / GEMMA

Regionale Informatievisie en -strategie	2021	RCIOO

1.6 Definities

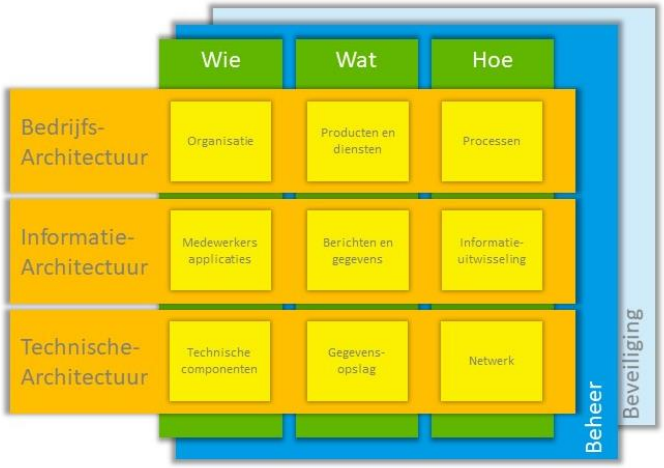
Begrip	Omschrijving
3GDC	Gemeenten Arnhem, Renkum en Rheden en De Connectie
GEMMA	GEMeentelijke Model Architectuur, GEMMA is een verzameling samenhangende kaders, richtlijnen, referentiemodellen en standaarden die gemeenten helpt bij het inrichten van hun IT-omgeving en processen. GEMMA helpt gemeenten om ICT-ontwikkelingen in samenhang aan te sturen. Ontwikkelen, bouwen, aanschaffen en implementeren onder architectuur zorgt ervoor dat oplossingen onderling goed samenwerken. GEMMA zorgt ook voor inzicht en overzicht, waarop bestuur en management besluitvorming kan baseren. En GEMMA helpt om de steeds belangrijker wordende samenwerking tussen gemeenten onderling en met ketenpartners te verbeteren.
Cloud	Cloud computing is het via internet op aanvraag beschikbaar stellen van hardware, software en gegevens, net zo eenvoudig als het elektriciteit uit het lichtnet.
Private Cloud	Een private cloud is een oplossing waarbij de diensten en services aangeboden/gerealiseerd worden vanuit een netwerk op eigen locatie (on premise). Deze diensten worden alleen ingezet voor de eigen organisatie. De Connectie is de IaaS leverancier voor de deelnemende partijen.
Community Cloud	Een community cloud in computing is een gezamenlijke inspanning waarbij de infrastructuur wordt gedeeld tussen verschillende organisaties uit een specifieke gemeenschap met gemeenschappelijke zorgen (beveiliging, compliance, jurisdictie, enz.), Hetzij intern beheerd of door een derde partij en intern of extern gehost. Dit wordt gecontroleerd en gebruikt door een groep organisaties die een gedeeld belang hebben. De kosten zijn verdeeld over minder gebruikers dan een public cloud (maar meer dan een private cloud), waardoor slechts een deel van het kostenbesparingspotentieel van cloud computing wordt gerealiseerd. Dit is voor gemeenten en de bij de VNG belegde Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)
Public Cloud	Een public cloud is een oplossing waarbij de diensten en services aangeboden/gerealiseerd worden vanuit een externe leverancier waarbij de hardware ook bij deze leverancier staat en vaak ook door deze leverancier wordt beheerd en onderhouden. Deze diensten zijn publiekelijk toegankelijk en worden aan meerdere partijen geleverd. Deze diensten worden ontsloten via het internet (IAAS, PAAS, SAAS, DAAS, etc.).
Hybrid Cloud	Een hybrid cloud is een combinatie van een private - en een public cloud. Vaak wordt voor deze oplossing gekozen zodat gevoelige data op eigen locatie kan blijven staan en tevens kan er gebruik gemaakt worden van de mogelijkheden die een public cloud biedt (IAAS, PAAS, SAAS, DAAS, etc.).

Hybrid Multi Cloud	Een hybrid multi cloud is een combinatie van een private- en meerdere public cloud oplossingen. Deze vorm geeft mogelijkheden tot het reduceren van kosten door voor elke component de op dat moment meest financieel gunstige optie te kiezen. Ook geeft dit de mogelijkheid om de best geëquipeerde leverancier te kiezen.
Infrastructure As A Service (IAAS)	Hierbij wordt er infrastructuur afgenomen en installeert de afnemer zelf het besturingssysteem en daarop eventuele applicaties of services.
Platform As A Service (PAAS)	Hierbij wordt er infrastructuur inclusief een besturingssysteem afgenomen en installeert de afnemer zelf een applicatie of services.
Software As A Service (SAAS)	Hierbij wordt een applicatie als dienst afgenomen zoals bijvoorbeeld Office365. Deze applicatie wordt meestal ontsloten vanuit het internet.
Desktop As A Service (DAAS)	Hierbij wordt de desktop functionaliteit als dienst afgenomen. Elk geautoriseerd device kan gebruik maken van dezelfde functionaliteit.
API	Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties. Je kan een API zien als een digitale stekkerdoos die applicaties met elkaar verbindt. Voor de Common Ground gaat het in het bijzonder over APIs waarmee je applicaties over het Internet kan koppelen. Zogenaamde REST APIs doen voor applicaties wat websites voor mensen doen. Websites presenteren informatie aan mensen, REST APIs maken applicaties en gegevens over het Internet beschikbaar voor andere applicaties. De technologie achter websites en REST APIs heeft daarom veel gemeen.

2 Inleiding

Dit is de volgende versie van de Regionale Enterprise Architectuur. In de vorige versie zijn de drijfveren van de Gemeenten Arnhem, Renkum, Rheden en De Connectie vertaald naar Regionale Bedrijfsprincipes. In de deze halfjaarlijkse versie, 2022.2, zijn de informatieprincipes van de genoemde organisaties in regionale informatieprincipes samengevoegd om uiteindelijk vorm te geven aan een Regionale Enterprise Architectuur met kaders en richtlijnen. Deze Regionale Enterprise Architectuur zal elk halfjaar worden bijgewerkt, architectuur is altijd in beweging.

De Enterprise Architectuur bestaat uit de bedrijfs-, informatie-, technische- , beheer- en beveiligingsarchitectuur. Onderstaand schema geeft de relaties tussen deze architecturen aan.



De bedrijfsdoelen van de aangesloten organisaties worden vertaald in richtinggevende principes zoals in dit document wordt weergegeven.
Het gebruik van de Regionale Enterprise Architectuur is beschreven in hoofdstuk 5 waar het architectuur proces aansluit bij het regionale portfolio proces.
Ook stelt de Regionale Enterprise Architectuur kaders op waarbinnen gebruik gemaakt wordt binnen de projecten. Deze kaders worden in hoofdstuk 7 en volgende van dit document uitgewerkt.

2.1 Business drijfveren Gemeente Arnhem

De gemeente Arnhem onderschrijft volgende doelen:

D1 - Gezicht naar de stad
We werken met het gezicht naar de stad, in dialoog en in gelijkwaardige samenwerking met partners
Motivering:
Ons organisatiebesluit beschrijft dit principe:
Het bestuur zoekt permanent het gesprek op en de samenwerking met de inwoners van Arnhem, het maatschappelijk middenveld en private partners. Dit vertaalt zich in adequaat reageren op initiatieven en ontwikkelingen die uit de stad zelf komen: uitnodigen, ruimte bieden en faciliteren. De gemeentelijke organisatie ondersteunt dit principe door zich vragend en open naar de burger en anderen partijen op te stellen en in te zetten op de dialoog met de stad.

D2 - Samenwerken vanuit vertrouwen
We verbeteren de samenwerking in en met de stad en binnen de gemeentelijke organisatie

Motivering:
Ons organisatiebesluit zegt hierover:
Een vraaggestuurde en regisserende gemeente met een kleine gemeentelijke organisatie is een antwoord op de wens om meer verantwoordelijkheid bij burgers, organisaties en instellingen in de samenleving neer te leggen en op de noodzaak en om flexibel en efficiënt om te gaan met de middelen. Kernwaarden in het werken zijn focus aanbrengen, denken vanuit het grotere geheel, samenwerken vanuit vertrouwen en resultaatgericht handelen.

D3 - Meer verantwoordelijkheid bij burgers, organisaties en instellingen in de samenleving neerleggen
We ontwikkelen ons naar een vraaggestuurde en regisserende gemeente met een kleine gemeentelijke organisatie als antwoord op de wens om meer verantwoordelijkheid bij burgers, organisaties en instellingen in de samenleving neer te leggen en op de noodzaak en om flexibel en efficiënt om te gaan met de middelen.
Motivering:
De gemeente wil burgers en organisaties meer verantwoordelijkheid geven en zoveel mogelijk zelfredzaam maken.

D4 - Een flexibel netwerk
Onze organisatie is ingericht als een flexibel netwerk. Medewerkers doen het werk, organisatorische eenheden niet. De plek in het in- en externe netwerk is voor het werk van een medewerker primair van belang, de organisatorische plek secundair.
Motivering:
Ons organisatiebesluit zegt hierover:
Een vraaggestuurde en regisserende gemeente met een kleine gemeentelijke organisatie is een antwoord op de wens om meer verantwoordelijkheid bij burgers, organisaties en instellingen in de samenleving neer te leggen en op de noodzaak en om flexibel en efficiënt om te gaan met de middelen. Kernwaarden in het werken zijn focus aanbrengen, denken vanuit het grotere geheel, samenwerken vanuit vertrouwen en resultaatgericht handelen.

D5 - Verantwoordelijkheid laag in de organisatie
Medewerkers zijn professionals die betrokken zijn bij de stad Arnhem. Medewerkers hebben een zelfbewuste positief-kritische houding en zijn extern georiënteerd. Medewerkers werken vanuit een onderlinge afhankelijkheid samen om de totaalopgave en ambitie waar we met het bestuur voor staan te realiseren.
Motivering:
Verantwoordelijkheid krijgen en nemen is een principe dat bijdraagt aan het principe met het gezicht naar de stad.
Effecten:
Dit principe betekent dat ook besluitvorming zo laag mogelijk in de ambtelijke organisatie wordt belegd. Deze cultuur is vertaald in een medewerkersprofiel. Dit profiel is gebaseerd op vier pijlers: ik geef richting, ik ken de regels, ik geef en neem ruimte en ik ben gericht op resultaat.
Dit principe wordt ondersteund door een management dat leiderschap toont en als boegbeeld functioneert voor de organisatie waar het al deze leidende principes betreft.

D6 - Antwoord op sturing uit wijken en bestuur

Motivering:

De programma's Wijksturing en Stad op de Kaart vragen van ons een goede (ver)binding met de stad en met sturing vanuit de wijken. Daardoor boeken we sneller resultaten. Meer dan ooit gaan we in gesprek met de partners in de stad en stellen we (maatschappelijke) opgaven centraal. Ook hier geldt dus dat we anders gaan werken en het vooral anders gaan 'doen'.

D7 - Regiegemeente zijn

Motivering:

Het verzelfstandigingen van onderdelen van het cluster Stadsbedrijven en de stappen die we in het kader van De Connectie zetten met Renkum en Rheden, zijn op zich los staande ontwikkelingen, die echter wel grote invloed hebben op de krimpende kernorganisatie.

2.2 Business drijfveren Gemeente Renkum

Onze visie is kort en krachtig:
1. We zijn een wendbare organisatie,
2. bieden betrouwbare dienstverlening,
3. we zijn een goede werkgever
4. we werken samen met partners waar dat slimmer is.

De gemeente onderschrijft de volgende bedrijfswaarden: Wendbaarheid, Helderheid, Gemak, Aandacht en Verantwoordelijkheid. Deze waarden worden ingezet op 3 pijlers, het waarborgen van beveiliging en privacy, aansluiting op strategische opgaven en behoeften en op een Wendbare IV-dienstverlenging.

Om richting te geven aan deze bedrijfswaarden en pijlers worden volgende bedrijfsprincipes gehanteerd:
(RNK) B1 – We werken planmatig
(RNK) B2 – We doen het samen
(RNK) B3 – We faseren en prioriteren

2.3 Business drijfveren Gemeente Rheden

De organisatiedoelen van de gemeente Rheden zijn de basis voor de vormgeving van de architectuur. Ontwikkelingen in de samenleving bepalen de steeds veranderende eisen aan de organisatie. Het bestuur en de gemeentelijke organisatie vertalen deze ontwikkelingen, onder andere op politiek en maatschappelijk terrein, naar de doelen voor de organisatie.

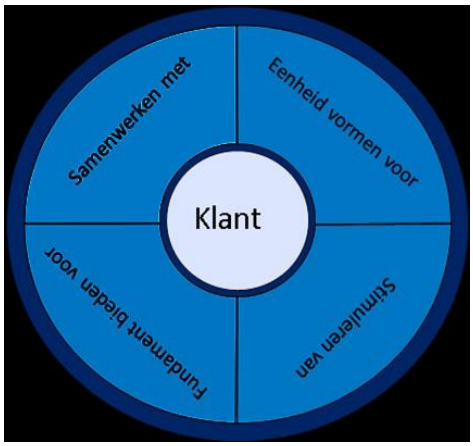
Uit deze doelen zijn belangrijke principes afgeleid voor de sturing op het gebied van procesinrichting en inrichting van de informatievoorziening. Om volgens deze kernprincipes te kunnen handelen zijn er vereisten in de verschillende domeinen. Deze domeinen zijn: Bedrijf, Informatie, Techniek, Informatieveiligheid, Beheer.

De veranderende verhouding tussen burger en overheid leidt tot een aantal afgeleide strategische doelen:

- De gemeente werkt vanuit klantperspectief;
- De gemeente is een betrouwbare partner;
- De gemeente deelt gegevens.

Gegevensmanagement is rand voorwaardelijk om invulling te kunnen geven aan deze doelen.

De door de organisatie vastgestelde klantdoelen zijn nader omschreven:



GEMMA-RHE-D1 - We willen een eenheid vormen voor de klant
We werken als één gezicht naar de klant, in dialoog en in gelijkwaardige samenwerking met partners.

GEMMA-RHE-D2 - Samenwerken intern en met de klant vanuit vertrouwen
We verbeteren de samenwerking in en met de gemeente en binnen de gemeentelijke organisatie.

GEMMA-RHE-D3 - Stimuleren kracht en verantwoordelijkheid van burgers, organisaties en instellingen in de samenleving
We ontwikkelen ons naar een vraag-gestuurde en regisserende gemeente als antwoord op de wens om meer verantwoordelijkheid bij burgers, organisaties en instellingen in de samenleving neer te leggen en op de noodzaak om flexibel, efficiënt en duurzaam om te gaan met de middelen.

GEMMA-RHE-D4 – Een stevig fundament bieden voor de klant
Centraal in onze dienstverlening staat samenredzaamheid. Dit betekent één ingang voor alle voorliggende voorzieningen, we werken vanuit vertrouwen in eigen kracht, samenredzaamheid is duurzaam en we schalen op waar nodig en af waar kan.

GEMMA-RHE-D5 Een flexibel netwerk
Onze organisatie is ingericht als een flexibel netwerk. Medewerkers doen het werk, organisatorische eenheden niet. De plek in het in- en externe netwerk is voor het werk van een medewerker primair van belang, de organisatorische plek secundair.

GEMMA-RHE-D6 - Verantwoordelijkheid laag in de organisatie
Medewerkers zijn professionals die betrokken zijn bij de gemeente Rheden. Medewerkers hebben een zelfbewuste positief-kritische houding en zijn extern georiënteerd. Medewerkers werken vanuit een onderlinge afhankelijkheid samen om de totaalopgave en ambitie waar we met het bestuur voor staan te realiseren.

GEMMA-RHE-D7 - Antwoord op sturing uit wijken en bestuur
Met een integrale wijkaanpak wil gemeente Rheden vanuit de inwoners, in samenspraak en samenwerking met partners de opgaven voor een wijk formuleren en samenbrengen in een wijkagenda. Dit betekent een omgekeerd proces. Niet uitgaan van 'externe' belangen in de wijk, maar juist de belangen en wensen van de inwoners centraal stellen.

GEMMA-RHE-D8 - Regiegemeente zijn
We hebben een openhouding waardoor we de kansen die er liggen onderzoeken en maken we voortdurende de afweging of het wenselijk en haalbaar is om werkzaamheden uit te besteden of samen te werken met andere gemeenten of partners. Het samen met gemeente Arnhem en Renkum, via een gemeenschappelijke regeling, onderbrengen van bedrijfsvoerende taken bij De Connectie hebben grote invloed op de kernorganisatie en vraagt om het ontwikkelen van een regieorganisatie voor de noodzakelijke sturing.

2.4 Business drijfveren De Connectie

De Connectie is een Bedrijfsvoering organisatie opgericht in 2017 door de gemeenten Arnhem, Renkum en Rheden. De oprichting werd ingegeven om samen te werken – in tijden van financiële schaarste – om het hoofd te kunnen bieden aan een groeiend takenpakket, de toenemende complexiteit daarvan en de steeds hogere eisen die de samenleving stelt aan de kwaliteit van de gemeentelijke dienstverlening.
In de Ontwikkelperspectief 2020-2024 nota die begin 2020 is opgesteld wordt, na het eerste bedrijfsplan, een stip op de horizon geplaatst.
Er wordt in deze nota richting gegeven aan de ontwikkeling om de partner in bedrijfsvoering te worden. Het uitgangspunt van de dienstverlening van De Connectie zijn de 5 K's: Klant, Kosten, Kwaliteit, Kwetsbaarheid en Kansen.

*De Connectie denkt en werkt vanuit de klant en zet de **klant** altijd centraal. De Connectie levert producten en diensten tegen een gezamenlijk afgesproken **kwaliteit**. De Connectie investeert in medewerkers en biedt hen **kansen** zich te ontwikkelen, speelt daar op in en vertaalt deze in samenwerking met de klant naar haar bedrijfsvoering. Hierdoor zijn partners in staat om zich volledig te richten op hun inwoners, bedrijven en toeristen. Ze zijn daardoor minder **kwetsbaar**. Door producten en diensten te harmoniseren en te digitaliseren werkt De Connectie efficiënter. Dit leidt ertoe dat de **kosten** voor de partners omlaaggaan.*

De missie die De Connectie wil bereiken is Dé allround partner in bedrijfsvoering, zodat klanten zich 100% kunnen richten op burgers, bedrijven en toeristen.

De regionale I-visie, met thema's als dienstverlening, informatie gestuurd werken, werkplek, harmonisatie, doorontwikkeling van de IV organisatie en basis op orde gaat deze missie ondersteunen.
Onderdeel van basis op orde is de Regionale Enterprise Architectuur, waar dit document ook aan bijdraagt.

De bedrijfsdoelen van De Connectie zijn:

(DC) D1 In onze dienstverlening staat de Klant op één

- Wij zijn één organisatie voor onze klanten
- Wij zijn een betrouwbare partner en doen alles in één keer goed
- Onze diensten, producten en adviezen zijn direct vindbaar en zijn veilig toe te passen
- Wij zijn dé partner voor onze klanten
- Afspraak is afspraak

(DC) D2 Continuïteit van de dienstverlening is geborgd
Wij hebben onze processen beschreven en voor deze processen een bedrijfscontinuïteitsplan vastgesteld. Daar waar wij diensten uitbesteden zal de ISO22301 als leidraad gelden. Dit is dé internationale norm voor certificering van bedrijfscontinuïteitsmanagement.

(DC) D3 Optimale inzet van middelen tegen de laagste kosten en risico's
We maken gebruik van standaarden zoals de GEMeentelijke Model Architectuur (GEMMA) 2.0 waarbij wij voor elke functionaliteit één toepassing gebruiken. Dit levert een besparing op maar brengt tevens met zich mee dat er goede keuzes moeten worden gemaakt (must, need, nice to have).

(DC) D4 Regionaal wat kan, lokaal wat moet
Het uitgangspunt is "Regionaal wat kan, lokaal wat moet". Dit draagt bij aan het verminderen van de kosten. Per situatie zal op basis van een businesscase bepaald worden wat de meest wenselijke samenwerkingsvorm is.

(DC) D5 Business, Informatie en technologie zijn in afstemming met elkaar
We brengen de architectuurlagen in balans om de doelen van onze organisaties te bereiken.

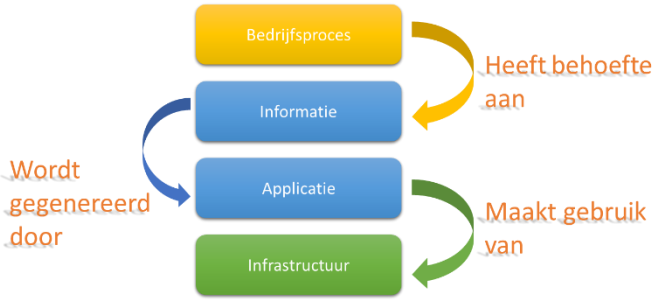
(DC) D6 We zijn een anticiperende organisatie
Veranderingen in de samenleving vereisen veranderingen in de organisatie, het is ons doel om hier volgend in op te treden.

(DC) D7 We werken plaats en tijdonafhankelijk
We werken op de beschikbare locaties van de gemeenten als het moet, thuis is zoveel mogelijk de werkplek

3 Context Regionale Enterprise Architectuur document

Dit Regionale Enterprise Architectuur document is opgesteld om de visie op architectuur verder te concretiseren. Dit document voorziet in een sturend raamwerk waarbinnen ontwikkelingen plaatsvinden. Het document beschrijft welke Regionale Enterprise Architectuur wordt nagestreefd, en via welke transitiestappen hiernaartoe zal worden gewerkt. Hierbij is de Regionale Enterprise Architectuur zoveel mogelijk afgestemd op de wensen en eisen, die vanuit de gemeenten en De Connectie, worden gesteld.

Met gemeenten als primaire klanten past het Regionaal Enterprise Architectuur Team de GEMMA[1] als referentie architectuur toe die voor de gemeentelijke organisaties van toepassing is. Binnen de referentie architectuur wordt een samenhang beoogd tussen Business-, Informatie en Technologie architecturen. Deze structuur is overgenomen in de Enterprise Architectuur Tool BlueDolphin waarbij gebruik maken van de archimate standaarden.



Het figuur illustreert hoe de behoefte aan Infrastructuur afhankelijk is van de bovenliggende applicatie. Die applicatie voorziet in de informatiebehoefte vanuit de bedrijfsprocessen zoals deze uitgevoerd worden.

Het is dan ook van groot belang om de bedrijfsprocessen te kennen en de beoogde veranderingen in deze processen nauwlettend te volgen. Met de opkomst van dynamische en kort cyclische werkvormen (Agile) dient de Regionale Enterprise Architectuur hierop voorbereid te zijn om haar klanten goed te kunnen blijven bedienen.

3.1 De Regionale Business Architectuur Principes

Business Architectuurprincipe	
A01	Onze organisatie denkt vanuit de positie van de klant
	• De **gemeente** is er voor burgers en bedrijven en zorgt ervoor dat deze de dienstverlening krijgen die ze kunnen verwachten. Zij kunnen immers niet zomaar naar een andere aanbieder als zij niet tevreden zijn. De administratieve lasten voor deze klanten moeten daarbij zoveel mogelijk worden beperkt. Klanten stellen steeds hogere eisen aan de kwaliteit van de dienstverlening van gemeenten. Diensten moeten aansluiten bij de klantbehoefte en klanten zouden geen hinder moeten ondervinden van de interne organisatie van gemeenten en andere (overheids)organisaties waarmee de gemeente samenwerkt. Anderzijds wordt ook van klanten verwacht dat ze waar mogelijk zelf verantwoordelijkheid nemen. Daarnaast zijn burgers en bedrijven niet alleen maar klant; met een aantal gemeentelijke taken krijgen zij ongevraagd te maken (zoals handhaving). **De Connectie** is de bedrijfsvoering organisatie die de gemeente als één organisatie, als betrouwbare partner, ondersteunt in de dienstverlening naar inwoners en bedrijven. De diensten, producten en adviezen die De Connectie biedt aan haar klanten zijn direct vindbaar en veilig toe te passen.

[1] GEMMA, GEMeentelijke Model Architectuur, afgeleide van de NORA, Nederlandse Overheid Referentie Architectuur.

Business Architectuurprincipe	
A02	Onze organisatie gebruikt generieke processen en functies
	• Gemeenten worden door de overheid geconfronteerd met bezuinigingsmaatregelen en krijgen tevens extra taken. Door te denken in generieke processen en functies kunnen diensten eenvoudiger worden gedeeld met andere gemeenten en kosten worden bespaard. Ook kan eenvoudiger gebruik worden gemaakt van standaard oplossingen die beschikbaar zijn in de markt en wordt maatwerk voorkomen. Klanten willen de overheid in haar dienstverlening ook zo veel mogelijk ervaren als één organisatie en generieke processen dragen daar aan bij. Gemeenschappelijke diensten hoeven niet in tegenspraak te zijn met het hebben van een eigen identiteit. De "couleur locale" kan grotendeels tot uitdrukking worden gebracht via specifieke beleidskeuzes en de persoonlijke aandacht van medewerkers. De Connectie die taken uitvoert voor meer dan één opdracht gevende gemeente werkt volgens het principe: één proces, één informatie inrichting, één ICT inrichting. Hierbij kiest zij voor integrale oplossingen, waarbij gebruik wordt gemaakt van oplossingen die al in huis zijn (bij één of meer gemeenten) zoals beschreven in de regionale informatievisie en -strategie.

Business Architectuurprincipe	
A03	Onze organisatie voert regie over uitbestede diensten
	• Gemeenten willen graag kwalitatief hoogwaardige dienstverlening bieden, maar wel tegen acceptabele kosten. De gemeente kijkt daarom kritisch of zij taken zelf uitvoert of dat het logischer is deze gezamenlijk met andere gemeenten of partners uit te voeren, of uit te besteden aan de markt. Voor verschillende taken zijn gespecialiseerde organisaties beschikbaar die dat beter of efficiënter kunnen dan de gemeente. In een aantal gevallen is samenwerking verplicht, bijvoorbeeld op regionale schaal. Cloud computing is een belangrijke ontwikkeling die ook als een vorm van outsourcing kan worden gezien. Als taken elders worden belegd is het belangrijk dat de gemeente hier de regie op blijft voeren. De verantwoordelijkheid blijft namelijk bij de gemeente.

Business Architectuurprincipe	
A04	Onze organisatie biedt de klant een goede informatiepositie
	• Een goede informatiepositie is voor klanten cruciaal om snel en gemakkelijk hun weg te vinden binnen de overheid. Het zorgt er ook voor dat zij de verantwoordelijkheid kunnen nemen die in toenemende mate van hen wordt verwacht vanuit een nieuw evenwicht tussen samenleving en overheid. Dat gaat niet alleen over het ontvangen van informatie; het gaat ook over het aan het stuur zetten van de klant omtrent het gebruik van zijn gegevens. Klanten moeten in staat zijn incorrecte registratie van hun gegevens te signaleren, zodat ze voor zichzelf op kunnen komen.

Business Architectuurprincipe	
A05	Onze organisatie digitaliseert haar diensten en processen
	• Voor een modern proces is een papieren document een obstructie; het is niet efficiënt en het hindert tijd- en plaats onafhankelijk werken. Daarom worden klanten verleid gebruik te maken van het digitale kanaal, processen zo veel als mogelijk geautomatiseerd en worden papieren documenten voorkomen. Klanten verwachten tegenwoordig ook dat dienstverlening digitaal wordt aangeboden. Dit is ook een expliciete ambitie van de overheid en uitgewerkt in de

	visiebrief 'Digitaal 2017' [13]. Er moet niet uit het oog worden verloren dat niet iedereen beschikt over voldoende digitale vaardigheden en dat persoonlijk contact op bepaalde momenten of voor bepaalde zaken belangrijk kan zijn. Het opslaan van gegevens in elektronische vorm maakt het veel eenvoudiger om deze te delen. Elektronische gegevens kunnen ook geautomatiseerd worden verwerkt door IT-systemen. Het elektronisch uitwisselen van gegevens is veel efficiënter en minder foutgevoelig dan het handmatig uitwisselen van gegevens.

Business Architectuurprincipe	
A06	Onze organisatie stelt openbare gegevens als open data beschikbaar
	• De overheid stelt hoge eisen aan de transparantie van overheidsorganisaties. Toegang tot informatie uit overheidsorganisaties is een kernwaarde in de democratie en is wettelijk vastgelegd. Overheidsinformatie is in beginsel vrij beschikbaar, tenzij de WOB, WBP of andere wetgeving bepaalt dat de gevraagde informatie niet geschikt is om openbaar te maken. Het openbaar, vindbaar en herbruikbaar aanbieden van open data heeft positieve maatschappelijke en economische effecten: het voorziet in een behoefte, heeft economische waarde en leidt tot meer transparantie en participatie. Zo kunnen anderen nieuwe toepassingen ontwikkelen en/of deze gegevens via (mobiele) applicaties laagdrempelig ontsluiten richting klanten. Het versterkt ook de informatiepositie van de klant zodat deze over dezelfde informatie kan beschikken als de gemeente. Het faciliteert ook publiek/private samenwerking en ontlast de gemeente van de ontwikkeling van allerlei eindgebruikerstoepassingen.

Business Architectuurprincipe	
A07	Onze organisatie hergebruikt gegevens
	• Binnen de Nederlandse overheid is afgesproken dat burgers niet wordt gevraagd om gegevens waar de overheid zelf al over beschikt. In het algemeen is de beschikbaarheid en kwaliteit van gegevens belangrijk. Door duidelijke afspraken te maken over waar gegevens worden beheerd en waarvandaan ze worden verstrekt wordt het delen ervan veel eenvoudiger en worden mogelijke inconsistenties voorkomen. Op landelijk niveau zijn er hiertoe basisregistraties gedefinieerd die door alle overheidsorganisaties moeten worden gebruikt. Binnen de gemeente is ook hergebruik van andere breed gebruikte gegevens relevant (kerngegevens). In de visie op de verdere ontwikkeling van het stelsel wordt ook landelijk breder gekeken dan basisgegevens. Ook is de burger zelf nadrukkelijk benoemd als gebruiker van de landelijke basisregistraties en wordt ook hergebruik van gegevens van/door private organisaties voorgesteld.

Business Architectuurprincipe	
A08	Onze organisatie gaat op een vertrouwelijke manier met gegevens om
	• Klanten verwachten dat de gemeente op een zorgvuldige manier met hun gegevens om gaat en dat deze niet in handen komen van onbevoegden. De visiebrief digitale overheid (Visiebrief digitale overheid 2017, dr. R.H.A. Plasterk, ministerie van BZK, 23 mei 2013) besteedt daarom specifiek aandacht aan informatieveiligheid. Ontwikkelingen als consumerization en tijd- en plaatsonafhankelijk werken vragen ook om extra aandacht voor de beveiliging van informatie. Grenzen van organisaties vervagen en traditionele beveiligingsmaatregelen passen niet meer. Cybercriminaliteit kan zorgen voor ernstige ontregeling van organisaties. Het is daarom belangrijk de risico's expliciet te maken. Hierdoor kunnen de meest passende maatregelen

	worden genomen en worden overmatige maatregelen vermeden. De Connectie als uitvoeringsorganisatie draagt hier aan bij door te voldoen aan de door de overheid opgelegde veiligheidseisen zoals beschreven in de Baseline Informatiebeveiliging Overheid (BIO) en in de informatiebeveiliging van de aangesloten deelnemers, het adopteren het High Level Structure (HLS) om de informatiebeveiligingsprocessen van het management system te waarborgen conform BIO en door het classificeren onze gegevens conform de geldende securityrichtlijnen, de BIO, en kiezen per klasse een bijpassend niveau (= minimaal BBN2) voor de regionale informatiebeveiliging.

3.2 De Regionale Informatie Architectuur principes

De gemeenten hanteren de het katern GEMMA Architectuurprincipes met de bijbehorende implicaties (Katern GEMMA Architectuurprincipes - GEMMA Online). Een uitwerking van deze webpagina is als bijlage C toegevoegd. De regionale informatievisie en -strategie van de gemeenten en De Connectie geeft tevens richting aan het kader en strategie voor harmonisatie en standaardisatie in de regio. Deze visie is vertaald in de onderstaande principes.

Informatie Architectuurprincipe	
I1	Richt digitale dienstverlening in zoals de klant dat zelf ook prettig vindt • De basis voor hoe wij digitale diensten aanbieden is vanuit de klantbeleving. Simpele dingen lopen goed en moeiteloos. Op het juiste moment, waarbij gemak voorop staat. • De inzet van (informatie)technologie draagt bij aan het behalen van onze organisatie doelen/ambities. De behoefte van onze inwoners staat hierbij centraal. • Onze informatiehuishouding (architectuur) past bij de organisatiedoelen en is flexibel en samenhangend (integraal) van opzet.

Informatie Architectuurprincipe	
I2	Gebruik end-to-end processen • Wij richten onze digitale dienstverlening in van begin tot eind, waarbij de behoefte van de klant centraal staat. • Wij werken daarbij functie- en afdeling overstijgend gezamenlijk aan het gehele proces om een product of dienst aan te bieden.

Informatie Architectuurprincipe	
I3	Gebruik data • Wij gebruiken beschikbare gegevens voor sturing op basis van empirie in plaats van onderbuikgevoel. Wij gebruiken data voor het verbeteren van de digitale dienstverlening. Wij vragen informatie eenmaal uit en ontkoppelen zoveel mogelijk data van de applicatie. Wij bieden ruimte voor experimenten met data om de digitale dienstverlening te verbeteren. • Informatie en data worden ingezet bij operationele, tactische en strategische besluiten • We geven inzicht wat er met de data gebeurt en hoe processen werken (Common Ground)

Informatie Architectuurprincipe	
I4	Wij maken keuzes in de volgorde gebruik – data – applicatie
	• Bij het vormgeven van digitale dienstverlening gaan we uit van hoe we het zelf zouden gebruiken, daarna wat dit betekent voor de data en als laatste welke applicaties we hiervoor nodig hebben.

Informatie Architectuurprincipe	
I5	Biedt selfservice
	• Wij zetten maximaal in op digitale selfservice voor producten en diensten en geven klanten inzicht in onze eigen prestaties en afspraken. Door middel van selfservice hebben onze opdrachtgevers zicht op afspraken, leveringsovereenkomsten, prestaties en producten en diensten. Wij leveren snelle, adequate on demand dienstverlening, digitaal waar het kan, persoonlijk waar het moet. Wij sluiten aan bij wat klanten gewend zijn en dragen zo bij aan onze doelstellingen.

Informatie Architectuurprincipe	
I6	Werk iteratief en verbeter snel
	• Wij transformeren onze dienstverlening stap voor stap. Hierdoor reageren wij gemakkelijk op wijzigingen in het beleid die van invloed zijn op de producten en diensten en zorgen we ervoor dat onze dienstverlening blijft voldoen aan de behoeften van de klant. Informatie architectuur bestaat daarmee niet uit theoretische beschouwingen maar uit concrete architectuur voor lopende en actuele ontwikkelingen.

Informatie Architectuurprincipe	
I7	We werken met componenten
	• We werken met componenten die afgebakende functionaliteit kennen en via gestandaardiseerde interfaces communiceren in plaats van met grote geïntegreerde (silo)systemen. We gebruiken hierbij een lagenmodel waarin we onderscheid maken tussen ‘interactie’,‘processen’,‘integratie’, ‘diensten’ en ‘gegevens’. Een hierop gebaseerd informatielandschap stelt gemeenten in staat om wendbaar en innovatief te opereren omdat wijziging of vervanging per component mogelijk wordt.

Informatie Architectuurprincipe	
I8	We zijn transparant waar mogelijk
	• De overheid stelt hoge eisen aan de transparantie van overheidsorganisaties. We willen transparant zijn in hoe we informatie en software gebruiken. Het delen en gebruiken van gegevens wordt slechts beperkt door wetgeving en niet door ideeën over het gebruik van gegevens. Gebruik van open standaarden en het beschikbaar stellen van gegevens als (linked) open data draagt hieraan bij, en geeft ook andere partijen dan de overheid de mogelijkheid om hierop diensten te ontwikkelen. Vanuit de maatschappij komt steeds meer vraag naar inzicht in hoe de overheid werkt en hoe beslissingen tot stand komen. Door als overheid open te zijn waar dit kan, wordt de informatiepositie van klanten versterkt, wordt publiek/private samenwerking gefaciliteerd en neemt het vertrouwen in de overheid toe.

Informatie Architectuurprincipe	
I9	We zorgen dat informatiebeveiliging en privacy op orde zijn
	• In een steeds meer informatie gedreven samenleving moeten burgers op gemeenten kunnen blijven vertrouwen. We garanderen daarvoor dat we ons houden aan wettelijke richtlijnen, nemen maatregelen om risico's te minimaliseren, en verantwoorden naar betrokkenen wat we doen. We zorgen voor een goede beveiliging van gegevens en garanderen privacy. Om invulling te kunnen geven aan zowel verwachtingen van de burger als de wettelijke vereisten realiseren we een samenhangend geheel van technische, organisatorische, fysieke en procedurele maatregelen. Veilige informatie vraagt om maatregelen in techniek, proces en organisatie. Beveiliging en gebruikersgemak is een spanningsveld waarbij voorop moet staan dat we medewerkers faciliteren in het veilig kunnen werken. Informatieveiligheid moet een integraal onderdeel zijn van de bedrijfsvoering voor zowel de organisatie, het proces en de techniek. • Wij passen de middelen op een veilige wijze toe met respect voor een ieders privacy en wet- en regelgeving.

Informatie Architectuurprincipe	
I10	We leggen gegevens eenmalig vast en vragen op bij de bron
	• We winnen gegevens eenmalig in, leggen ze eenmalig vast en gebruiken ze vervolgens, overeenkomstig het doel waarvoor ze ingewonnen zijn, meervoudig. Net zoals bij de landelijke basisregistraties is gebeurd, standaardiseren we ook andere bronbestanden. Eenmalig opgeslagen brongegevens worden alleen bewerkt bij de bron en komen beschikbaar voor processen die ze nodig hebben. Die slaan geen kopieën van die gegevens meer op maar vragen ze via gestandaardiseerde interfaces op bij de bron. (Common Ground)

Informatie Architectuurprincipe	
I11	We faciliteren regie op gegevens
	• Partijen die daartoe gerechtigd zijn, moeten regie kunnen voeren op welke gegevens aan wie, op welk moment en voor welk doel, worden verstrekt. Persoonlijk datamanagement draagt bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen. We geven daarom inzicht in wie welke gegevens bijhoudt en welke gegevens uitgewisseld worden. Burgers krijgen de mogelijkheid om toestemmingen t.a.v. uitwisseling van gegevens te beheren en, waar mogelijk, gegevens die op hen betrekking hebben te wijzigen. (Common Ground)

Informatie Architectuurprincipe	
I12	We standaardiseren maximaal
	• Gemeenten werken samen met steeds meer partijen. Afspraken en standaarden zijn nodig om effectief, efficiënt en veilig samen te werken en informatie uit te wisselen. Ze zijn ook nodig om voldoende onafhankelijk te blijven en de juiste samenwerkingspartners te kunnen kiezen. Standaardiseren is van belang binnen alle (lagen van) functionaliteit. Als gemeenten gaan we op ieder gebied waar dit meerwaarde biedt standaarden toepassen, en waar nodig ook zelf ontwikkelen. (Common Ground)

Informatie Architectuurprincipe	
I13	Informatie is een asset
	• Dit principe helpt de strategische doelen te bereiken (door gebruik te maken van een Data Strategy Map) en daarmee wordt informatie een kwantificeerbare waarde.

Informatie Architectuurprincipe	
I14	Gemeenschappelijke terminologie en gegevensdefinities
	• We gebruiken binnen onze organisatie een gemeenschappelijke terminologie gebaseerd op de GEMMA referentie architectuur. We benoemen o.a. de processen om deze manier om verwarring in terminologie te voorkomen. De ISO20000 biedt hiervoor tevens handvaten.

Informatie Architectuurprincipe	
I15	Onze informatiehuishouding is ingericht op het samenwerken met ketenpartners
	• Onze regels, voorzieningen, activiteiten en processen zijn gericht op de informatiestromen en op het beheer van informatie. Onze informatiehuishouding ondersteunt de primaire processen, waarbij er duidelijkheid ontstaat over de informatie naar ketenpartners.

Applicatie Architectuurprincipe	
AP1	Applicaties zijn technologie onafhankelijk
	• Applicaties maken gebruik van standaarden en hebben geen afhankelijkheden naar andere applicaties. Data dient ontkoppeld van de applicatie te zijn. Door gebruik te maken van webservices geldt dit ook voor de technologische laag

Applicatie Architectuurprincipe	
AP2	Applicaties zijn eenvoudig te gebruiken
	• Applicaties dienen op elk apparaat dezelfde functionaliteit en ‘look and feel’ te hebben, waarbij er voortdurende innovatie plaatsvindt.

Applicatie Architectuurprincipe	
AP3	Componenten zijn logisch en herbruikbaar
	• Bouwblokken uit de applicatie-architectuur worden hergebruikt, waarbij de logische applicatie architectuur het wat beschrijft en de technische applicatie architectuur het hoe beschrijft.

Applicatie Architectuurprincipe	
AP4	Applicaties dragen bij aan de bedrijfsdoelen
	• De Enterprise architectuur geeft richting aan de doelen van de gemeenten en De Connectie. Applicaties dienen zich dan ook te conformeren aan deze doelen.

Applicatie Architectuurprincipe	
AP5	Enterprise architectuur is ook van toepassing op externe applicaties • In de Enterprise architectuur is sprake van een Cloud first strategie, ook deze applicaties dienen zich aan de enterprise architectuur te conformeren om de doelen van de gemeenten en De Connectie te ondersteunen.

Applicatie Architectuurprincipe	
AP6	Applicaties zijn vluchtig gekoppeld • Applicaties zullen ook geschikt moeten zijn voor mobiele apparatuur

Applicatie Architectuurprincipe	
AP7	Applicaties sluiten aan op de functionele domeinen • We maken gebruik van het GEMMA 2.0 architectuurmodel. In de GEMMA is in kaart gebracht wat de bouwblokken van de gemeentelijke informatievoorziening zijn. Deze bouwblokken, de referentiecomponenten, zijn modulair, zelfstandig inzetbaar en vervangbare delen van softwaresystemen. Referentiecomponenten groeperen logisch bij elkaar horende functionaliteit en bieden deze functionaliteit aan via goed gedefinieerde interfaces. Referentiecomponenten zijn in de GEMMA beschreven voor zowel specifieke als generieke functionaliteit. (https://www.gemmaonline.nl/index.php/GEMMA_2_Applicatiearchitectuur)

Applicatie Architectuurprincipe	
AP8	Bij vervanging van Applicaties, conversie tenzij • Bij elke vervanging van een applicatie dient bij de aanbesteding en/of offerte uitvraag een conversie van de bestaande applicatie meegenomen te worden. Het niet converteren van de data naar een nieuwe applicatie zorgt voor extra beheer last, licenties en onderhoud en draagt niet bij aan de doelen van de gemeenten en De Connectie (kosten). Het in stand houden van verouderde, niet meer door de leverancier onderhouden omgevingen zorgt tevens voor beveiligingsrisico's.

Applicatie Architectuurprincipe	
AP9	Applicaties moeten geschikt zijn voor multitenancy • De software architectuur waarbij een enkel exemplaar (instance) van de software draait op een server en verschillende tenants bedient. Een tenant is een groep gebruikers die een gemeenschappelijke toegang heeft, met specifieke rechten om de software-instantie te delen.

3.3 De Regionale Technische Architectuur principes

ICT is een afdeling van De Connectie waarbij de missie, zoals in het ontwikkelperspectief van De Connectie beschreven is, de leidraad voor alle medewerkers van ICT moet zijn. We verliezen onze klant niet uit het oog en gebruiken de regionale I-visie en de Regionale Enterprise Architectuur om onze visie als volgt te definiëren:

Wij zijn zakelijk gestuurd zonder winstoogmerk, hebben focus voor onze enige doelgroep waarbij we met veel relevante kennis en ervaring weten we wat er speelt, mede door ons partnerschap zijn we aanwezig in de haarvaten van de gemeenten

Bij het maken van de regionale architectuur principes zijn ook de afgeleide richtinggevende principes van de Technische Architectuur beschreven. Het samenspel van regie voeren, beheer en de inrichting van de infrastructuur volgens deze principes maakt dat we flexibel, snel en met ruimte voor experimenten adequaat in kunnen spelen op de behoeften van onze klanten.

Technische Architectuurprincipe	
TP01	Wij voeren regie over alle ICT diensten • Als partner van onze klanten voeren wij regie over de ICT diensten. Dit geeft onze Klanten de vrijheid om hun kerntaken uit te voeren en zich te richten op hun inwoners, bedrijven en toeristen.

Technische Architectuurprincipe	
TP02	Voor één functie gebruiken we één softwaretoepassing • Naast de actuele, operationele oplossing wordt één toekomstige oplossing ondersteund ten behoeve van onderzoek, testen en implementatie. Ook wordt een uit gefaseerde oplossing ondersteund volgens daarover gemaakte afspraken.

Technische Architectuurprincipe	
TP03	Referentie componenten en Technologie worden hergebruikt • Wij maken gebruik van generieke functionaliteit welke hergebruikt wordt binnen verschillende toepassingsgebieden. • Afgebakende functionaliteiten en gestandaardiseerde interfaces i.p.v. geïntegreerde (silo)systemen. (Common Ground)

Technische Architectuurprincipe	
TP04	Informatietechnologie wordt duurzaam ingericht • De oppervlakte van de aarde is eindig; grondstoffen kunnen opraken en de opnamecapaciteit van de atmosfeer en onze natuurlijke omgeving kent haar grenzen. We realiseren ons allemaal dat we de natuur moeten sparen en de opwarming van de aarde zoveel mogelijk moeten voorkomen. Voor De Connectie betekent duurzaamheid in ieder geval een verplichting om te voldoen aan landelijke doelstellingen. Dit heeft volgende implicaties: • Er wordt bij de aanschaf van IT apparatuur gelet op het energieverbruik, de duurzaamheid van de apparatuur, de gebruikte verpakkingsmaterialen en de correcte afvoer ervan. • Er wordt bij de herinrichting van rekencentra onderzocht in hoeverre uitbesteding of gemeenschappelijke rekencentra helpen bij het realiseren van een grotere mate van duurzaamheid in het algemeen en energie-efficiëntie in het bijzonder. • Duurzaamheid is een vast onderwerp bij aanbestedingen. • Afgevoerde apparatuur wordt her ingezet of duurzaam verwerkt. • Gebruikersapparatuur die langere tijd niet wordt gebruikt wordt automatisch standby geschakeld of zelfs uitgeschakeld. • Servers zijn gevirtualiseerd en geconsolideerd zodat zo min mogelijk fysieke servers noodzakelijk zijn. • Gegevens die niet of nauwelijks meer gebruikt worden en die wettelijk niet bewaard hoeven te blijven worden verwijderd.

Technische Architectuurprincipe	
TP05	Er wordt voldaan aan Open en de facto standaarden en aan het geldend beleid. • Naast de standaarden voor de GEMMA 2.0 processen, standaard berichtformaten en dergelijke worden ook de standaarden[2] voor infrastructuur gehanteerd zoals TCP/IP en HTTP. Het streven is om de niet functionele eisen te matchen op een applicatieplatform zoals dat al in gebruik is. Dit wel met verantwoorde kosten. Tot een platform behoren de hardware en software elementen waarop een applicatie draait.

Technische Architectuurprincipe	
TP06	De Connectie werkt met een servicegerichte architectuur. (webservices) • De Service gerichte Architectuur (SOA) heeft als doel dat diensten losgekoppeld raken van besturingssystemen, programmeertalen en andere technieken die onder de applicatie liggen. SOA valt te definiëren als een groep diensten die met elkaar communiceren. Deze communicerende diensten zijn opgebouwd uit functionaliteiten die zijn gegroepeerd rondom bedrijfsprocessen. Systemen en toepassingen wisselen gegevens met elkaar uit via de interne servicebus van De Connectie. Daarbij gebruiken we open standaarden. Dit geldt niet alleen voor systemen en toepassingen die volledig door de interne infrastructuur van de connectie ondersteund worden, maar ook voor systemen die door een derde partij gehost of als service aangeboden worden ('cloud'-toepassingen) waarbij voor de laatste geldt dat het ophalen van de gegevens verreweg de voorkeur heeft boven het verkrijgen van de gegevens.

Technische Architectuurprincipe	
TP07	We maken gebruik van landelijk en gemeentelijk beschikbare services • We sluiten zo veel als mogelijk aan bij VNG realisatie onderdelen.

Technische Architectuurprincipe	
TP08	We verlenen toegang op basis van rollen, functie en locatie • Toegang (Autorisatie) van de persoon in applicaties en gegevens (logische toegang) en welke rechten de gebruiker heeft van welke locatie (fysieke toegang) op welke momenten zoals bepaald door de eigenaar. Hierdoor kan vertrouwelijk omgegaan worden met gegevens. Een effect dat niet alleen personen worden geautoriseerd maar ook andere informatiesystemen die gegevens uitvragen en/of kopieën aanleggen. Door hiervan gebruik te maken is een goed en duidelijk beheer van licenties mogelijk. Het gebruik van RBAC en IAM draagt bij aan het uitgangspunt least privileged, waarbij de rol bepalend is voor de minimale rechten die benodigd zijn deze rol uit te voeren.

Technische Architectuurprincipe	
TP09	Wij verlenen toegang vanuit één portaal. • Toegang tot onze infrastructuur geschiedt vanuit 1 portaal naar alle informatiesystemen.

[2] https://forumstandaardisatie.nl/open-standaarden

Technische Architectuurprincipe	
TP10	We gebruiken alleen bewezen producten en technieken • Door gebruik te maken van dit principe zal de beheer last en verstoringen voor gebruikers verkleind worden. Er dienen minimaal 2 referenties voorgelegd te worden van zaken die echt geïmplementeerd zijn. Het inzetten van systemen en software die zich nog niet bewezen hebben leidt over het algemeen tot het moeten overwinnen van kinderziektes in deze nieuwe producten. Door het gebruik van bewezen producten en technieken kan er gewerkt worden met informatievoorziening die doet wat men ervan verwacht.

Technische Architectuurprincipe	
TP11	We werken op basis van een multi tier architectuur • Binnen De Connectie werken we op basis van de multi tier architectuur. De gedachte achter een multi tier architectuur is software op te delen in meerdere componenten die met elkaar samenwerken. Hiermee kunnen componenten worden ontkoppeld van functionaliteit en hergebruik van functionaliteit te stimuleren. Iedere component heeft nu zijn eigen verantwoordelijkheden. Bij de Connectie architectuur wordt een 3-tierarchitectuur gebruikt. Bij deze architectuur is er een afzonderlijke tier voor de presentatie, de business logic + datatoegang en dataopslag. Dit wordt verder uitgewerkt in de Internet, Presentatie, Applicatie en Data (IPAD) functies met een fysieke scheiding van elkaar.

Technische Architectuurprincipe	
TP12	Eindgebruikers functionaliteit kan plaats- en tijd onafhankelijk worden gebruikt • Gebruikers krijgen, onafhankelijk van de plaats en tijd waarop zij van toepassingen en systemen gebruik maken, dezelfde functionaliteit (tenzij niet gewenst of geoorloofd) aangeboden. Bestaande infrastructuur, systemen en toepassingen kunnen op dit gebied duidelijke beperkingen hebben in verband met batchverwerkingen en onderhoud. Bij de selectie van nieuwe componenten dienen we hier op te letten. Rekening dient gehouden te worden met geldende wettelijke bepalingen voor de ontsluiting van de gegevens.

Technische Architectuurprincipe	
TP13	Voor een betrouwbare en schaalbare ICT-infrastructuur, maken we gebruik van modulaire en gestandaardiseerde bouwstenen. • Door gebruik te maken van modulaire en gestandaardiseerde bouwstenen kunnen we deze hergebruiken. Deze bouwstenen worden in de Enterprise Architectuur Tool weergegeven. Door telkens dezelfde architectuur bouwstenen toe te passen wordt voldaan aan enkele van de uitgangspunten van De Connectie (kosten, kwaliteit en kwetsbaarheid)

Technische Architectuurprincipe	
TP14	We ondersteunen de toekomstige informatievoorziening (Common Ground) • Community: Gemeenten, marktpartijen en de VNG werken samen in het realiseren van Common Ground • Agile: Kort-cyclisch bruikbare (deel) producten opleveren en continu verwerken van feedback • Nieuw naast oud: De nieuwe architectuur vervangt geleidelijk de bestaande architectuur • Moderne IT: Kansen voor nieuwe technologie moeten benut worden, mits dit meerwaarde heeft.

	• Open Source: stimuleren van open source om afhankelijkheden m.b.t. marktpartijen te beperken. • Uitwisseling: Zorgen voor veilige, betrouwbare, transparante en snelle uitwisseling van gegevens. Met de NLX laten we zien hoe dit kan werken. • We gebruiken het 5 lagen model voor de Common Ground om meer flexibiliteit te creëren, spreiden we risico's en voorkomen dat een component meer doet dan waar het voor bedoeld is.

Technische Architectuurprincipe	
TP15	We passen IT-virtualisatie toe
	• Virtualisatie (van personalisatie, applicatie, desktop en server) wordt toegepast om een hogere mate van flexibiliteit en beschikbaarheid te creëren voor de gebruiker.

Technische Architectuurprincipe	
TP16	Elk object heeft een eigenaar die verantwoordelijk is voor dat object
	• Objecten hebben een eigenaar. Daarbij gaat het niet alleen om tastbare dingen als een PC of een kast. Objecten in deze zin zijn alle dingen die om beheer vragen, dus ook processen, informatiesystemen, overeenkomsten, mailboxen, mappen op het netwerk, architectuurprincipes enz.

Technische Architectuurprincipe	
TP17	We streven naar minimalisering van de beheerlast
	• Geen maatwerk. Maatwerk leidt tot bij noodzakelijk onderhoud, updates en aanpassingen op termijn tot een hoge beheerlast en grote afhankelijkheid van specifieke kennis.

Technische Architectuurprincipe	
TP18	We gebruiken actuele versies van objecten
	• De eigenaar van een object (proces, toepassing, besturingssysteem, protocol etc.) zorgt ervoor dat we bij de tijd blijven door een actuele versie van dat object te gebruiken. Actueel kan voor verschillende objecten een verschillende dimensie in tijd betekenen. We leggen per object in een releasemodel vast welke versie actueel is. Het Life Cycle Management proces dient gevolgd te worden.

Technische Architectuurprincipe	
TP19	Aanpassingen worden gedaan naar aanleiding van business behoefte
	• Aanpassingen binnen de technische architectuur worden geïnitieerd vanuit de business. Deze aanpassingen zullen in de Enterprise Architectuur tool (BlueDolphin) gemodelleerd worden en in een project en/of wijzigingsactiviteit tot uitvoer worden gebracht. • We kiezen die (innovatieve) informatietechnologie, die past bij een moderne en flexibele organisatie • De wijze waarop wij informatietechnologie inzetten, sluit nauw aan bij de vraag van de organisatie / afdelingen

Technische Architectuurprincipe	
TP20	Technologie wordt hergebruikt • We gebruiken voor een functie binnen de architectuur dezelfde technologie. Afwijkingen of gebruik van andere technologie levert een hogere beheerinspanning op en zal kostenverhogend werken.

Technische Architectuurprincipe	
TP21	Het leveranciersaantal is beperkt • Het aantal leveranciers waar wij zaken mee doen zal tot een minimum beperkt worden. Dit komt de relatie als ook de kosten ten goede.

Technische Architectuurprincipe	
TP22	Technologie is compatible • De componenten in de bouwblokken zijn met elkaar compatible, opdat bij het modelleren van een product een goede werking gegarandeerd is.

Technische Architectuurprincipe	
TP23	Technologie wordt ondersteund door een leverancier • We werken met actuele versies en bijbehorende ondersteuning van de leverancier om risico's van uitval tot een minimum te beperken.

3.4 De Regionale Beveiliging Architectuur principes[3]

Beveiliging Architectuurprincipe	
BP1	Vertrouw nooit, verifieer altijd Dit principe ligt aan de basis van het **zero trust** beveiligingsmodel. Dit principe komt voort uit de tekortkomingen die in het traditionele kasteelmodel werden toegepast. Het traditionele model is onder druk komen te staan door de vele cloud toepassingen en de daarbij behorende moderne malware- en ransomeware-aanvallen. Bij dit principe zijn volgende ontwerpprincipes van toepassing: • Identificeer de te beschermen onderdelen van de IT-infrastructuur en beveilig alle paden er naartoe. • Verschaf alleen toegang tot informatie via beveiligde verbindingen, ongeacht de locatie. • Handhaaf strikte toegangscontrole op een *need-to-know*-basis • Bepaal de toegangsrechten op basis van mate van vertrouwen die afgeleid wordt uit verschillende eigenschappen van de toegangsaanvraag: account, apparaat, IP-adres en locatie. • Zorg voor uitgebreide monitoring en logging.

[3] 2 t/m 11 Afkomstig uit de VNG 10 bestuurlijke principes voor informatiebeveiliging. Op het moment dat er vanuit RCISO een document aangeleverd wordt zal dit hier worden geplaatst.

Beveiliging Architectuurprincipe	
BP2	Informatiebeveiliging is van iedereen • Naast de inzet van een technisch veilige omgeving zijn het de collega's en hun handelen die de omgeving écht veilig (of onveilig) maken. Het veilig omgaan met informatie is de verantwoordelijkheid van alle collega's. Met als verantwoordelijkheid van de werkgever om hier een stimulerende en toetsende rol in te spelen. Bewustwording is namelijk meer dan alleen maar het 'zenden' van informatie. Je moet zorgen voor een blijvende en meetbare gedragsverandering, ook bij het bestuur. Zorg dat alle inhoudelijk betrokken functionarissen met elkaar samenwerken en dat er communicatie capaciteit beschikbaar is.

Beveiliging Architectuurprincipe	
BP3	Informatiebeveiliging is risicobeheersing • Als organisatie ben je afhankelijk van de beschikbaarheid van informatie en de continuïteit van de informatievoorziening voor je dienstverlening naar burgers en bedrijven. Informatiebeveiliging hoort dus thuis in de lijn want de verantwoordelijkheden houden direct relatie met de bedrijfsvoering. Lijnmanagers zijn verantwoordelijk voor risicomanagement en maak heldere afspraken over wat er van hen verwacht wordt. Risicobewustzijn dient ook standaard onderdeel te zijn van samenwerkingen en uitbestedingen.

Beveiliging Architectuurprincipe	
BP4	Risicomanagement is onderdeel van de besluitvorming • Het is uiteraard belangrijk om risico's en maatregelen te monitoren en te toetsen, zodat de maatregelen, indien gewenst per afdeling, verantwoordelijkheidsgebied of onderwerp, hierop kunnen worden bijgesteld. Maak risicomanagement daarom onderdeel van besluitvorming en laat lijnmanagement hierover rapporteren. Bestuurders zijn verantwoordelijk voor kaderstelling (vaststellen). Tevens kan besluitvorming ook inhouden dat risico's toch bewust, al dan niet tijdelijk, gelopen worden. Ook dan ben je 'in control'.

Beveiliging Architectuurprincipe	
BP5	Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking • Als gemeente en De Connectie werk je met veel (keten)partners samen. Hierbij geldt 'de ketting is zo sterk als de zwakste schakel', juist als het gaat om informatiebeveiliging. Elke organisatie heeft immers in meer of mindere mate te maken met digitale dreigingen. Wanneer je met verschillende organisaties samenwerkt, vraagt dit dus niet alleen om een inschatting van de eigen risico's, maar ook van die van andere. Als organisatie in een keten ben je afhankelijk van elkaar en daarbij is het belangrijk dat je ook in kaart hebt wat de risico's van ketenpartners zijn. Zorg dat je de risico's die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en de risico's die voortkomen uit ketensamenwerking goed in kaart brengt. Ook bij diensten die je uitbesteedt, dienen de risico's in kaart te worden gebracht. Ken verantwoordelijkheden toe en tref de juiste maatregelen. Dit is dus ook van toepassing op alle bestuurlijke samenwerkingen.

Beveiliging Architectuurprincipe	
BP6	Informatiebeveiliging is een proces • Informatiebeveiliging betekent niet eenmalig een checklist doorlopen (implementatie), alle vinkjes zetten en klaar. Het is een continu proces waar je als organisatie aan moet blijven werken. Elke dag brengt nieuwe uitdagingen, projecten, processen et cetera. Het vraagt om structurele borging en moet onderdeel worden van (bestaande) processen. Maak hierbij gebruik van een gedocumenteerd 'Information Security Management System' (ISMS). ISMS gaat uit van de Plan Do Check Act cyclus (PDCA-cyclus), een continu en interactief proces.

Beveiliging Architectuurprincipe	
BP7	Informatiebeveiliging kost geld • Risicomanagement vraagt niet om snelle acties maar om constante aandacht. En hiervoor moeten middelen beschikbaar worden gesteld. Je hebt als organisatie de morele verplichting om zorgvuldig en veilig met gegevens om te gaan. Een incident kan leiden tot (grote) materiële en immateriële schade voor je organisatie. Denk aan datalekken die grote gevolgen voor het imago en de bedrijfsvoering van je organisatie en onze klanten hebben, tevens legt het veel (politieke) druk op de gemeente wat weer kan leiden tot reputatieschade. Stel voldoende middelen beschikbaar zodat er maatregelen getroffen kunnen worden bij risico's die een gevaar zijn voor de continuïteit van de bedrijfsvoering.

Beveiliging Architectuurprincipe	
BP8	Onzekerheid dient te worden ingecalculeerd • De input voor risicomanagement is gebaseerd op wat er in het verleden is gebeurd (ervaringen) en op actuele informatie. Daarnaast dien je rekening te houden met wat je in de toekomst kunt verwachten. Dit is uiteraard lastiger in te schatten, houdt daarom rekening met eventuele beperkingen en onzekerheden die nu nog niet met zekerheid zijn vast te stellen en afhankelijk zijn van toekomstige ontwikkelingen. Op het moment dat er besluiten genomen moeten worden, dient er rekening gehouden te worden met deze risico's. Dit vergt goede en actuele informatie over de risico's die de organisatie en onze klanten lopen.

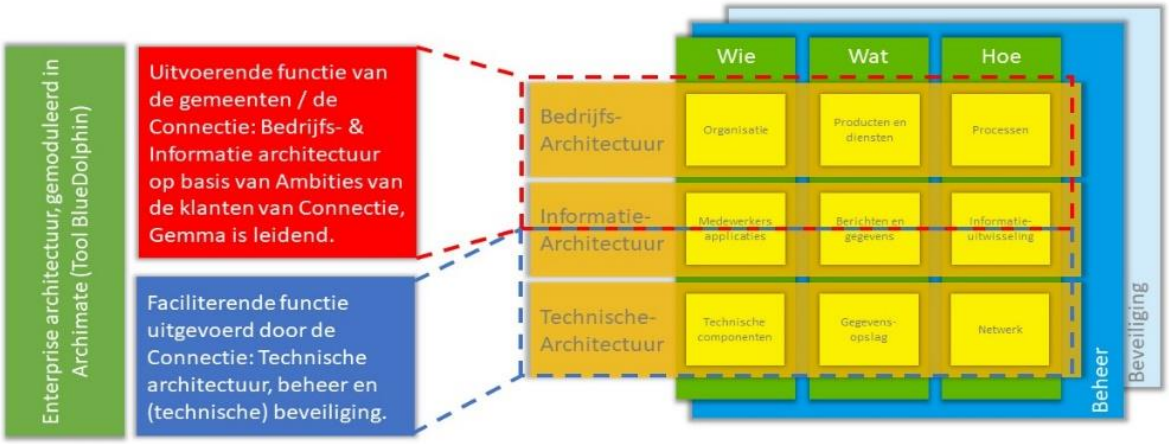
Beveiliging Architectuurprincipe	
BP9	Verbetering komt voort uit leren en ervaring • Het is niet de vraag of je als De Connectie slachtoffer wordt van een incident, maar wanneer. Hoe goed je informatiebeveiliging ook is, incidenten zullen altijd voorkomen. Voorkomen ga je het dus niet. Het is daarom belangrijker om na te denken hoe je er mee omgaat en wat je ervan kunt leren. Zorg dat je veerkrachtig bent als organisatie (resilient) en rekening houdt met kansen en risico's van nieuwe ontwikkelingen. Transparant zijn over incidenten helpt, leer ervan en realiseer en accepteer dat risico's niet geheel zijn uit te sluiten. Reflecteer op risico's en betrek ook de medewerkers bij het delen van hun ervaringen als het gaat om risico's die processen binnen de informatievoorziening bedreigen. Zo zorg je dat De Connectie kan leren van incidenten en tevens leer je zo te ontdekken wat wel en wat niet werkt. Dit helpt bij het nemen van toekomstige besluiten.

Beveiliging Architectuurprincipe	
BP10	Het bestuur controleert en evalueert • Het is belangrijk om te controleren wat de status is van de implementatie van het informatiebeveiligingsbeleid en om te kijken of risicomanagement ook daadwerkelijk is ingebed binnen de organisatie. Dit kan door lijnmanagement hierover te laten rapporteren. Op die manier krijg je als bestuurder goed inzicht in waar de organisatie staat en komen verbeterpunten aan het licht. Laat daarnaast de organisatie op effectiviteit en efficiency toetsen, door een (externe) auditor.

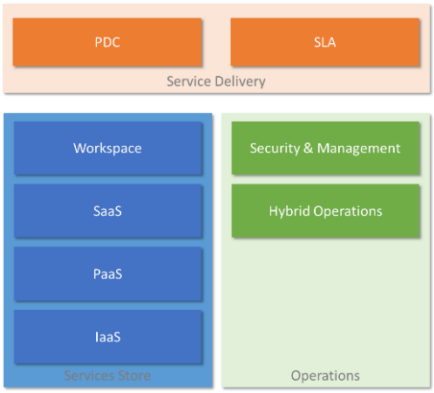
Beveiliging Architectuurprincipe	
BP11	Bestuurders bevorderen een veilige cultuur • Bij een informatieveilige omgeving hoort ook een veilige (meld)cultuur. Zo is het belangrijk dat collega's niet bang zijn om incidenten te melden. Tevens wil je bevorderen dat iedereen risico's signaleert en deze ook meldt en elkaar aanspreekt op onveilig gedrag. Wees je als bestuurder bewust van je voorbeeldfunctie en draag dat ook uit naar de rest van de organisatie. Spoor lijnmanagement in de ambtelijke organisatie aan om hun verantwoordelijkheid als het gaat om risicomanagement te pakken.

4 Het Architectuur Model

De architectuur maakt gebruik van de Gemma referentie architectuur[4]. Onderstaande figuur illustreert hoe de drie architecturen samenkomen en hoe deze gemodelleerd wordt.



De Gemma referentie architectuur biedt een verdeling op hoofdlijnen waarbij geen nadere specificatie wordt gegeven aan hoe de technische architectuur verder ingevuld dient te worden. Voor De Connectie is gekozen om de technische referentiearchitectuur, in deze regionale enterprise architectuur, vanuit het afnemersperspectief te benaderen. Welke diensten worden nu en in de nabije toekomst gevraagd is daarbij het vertrekpunt.



Zowel de klanten van De Connectie als De Connectie zelf kunnen in de markt van vandaag de dag alle gewenste functionaliteit afnemen als dienst. Door De dienstverlening van De Connectie in gelijke indeling aan te bieden kan De Connectie enerzijds eenvoudiger diensten positioneren ten opzichte van Cloud aanbieders. Tegelijkertijd wordt het voor De Connectie zelf ook mogelijk om Cloud diensten af te nemen en in te zetten voor klanten.

Het figuur illustreert de diensten die de Connectie levert:
- Service delivery, PDC en bijbehorende SLA's
- Services store, de te leveren diensten
- Operations, dat wat nodig is om de diensten in stand te houden.

[4] De Gemma referentie architectuur kent een 2.0 versie waarbij de weergave anders is, de onderwerpen zijn nog altijd valide en toepasbaar.

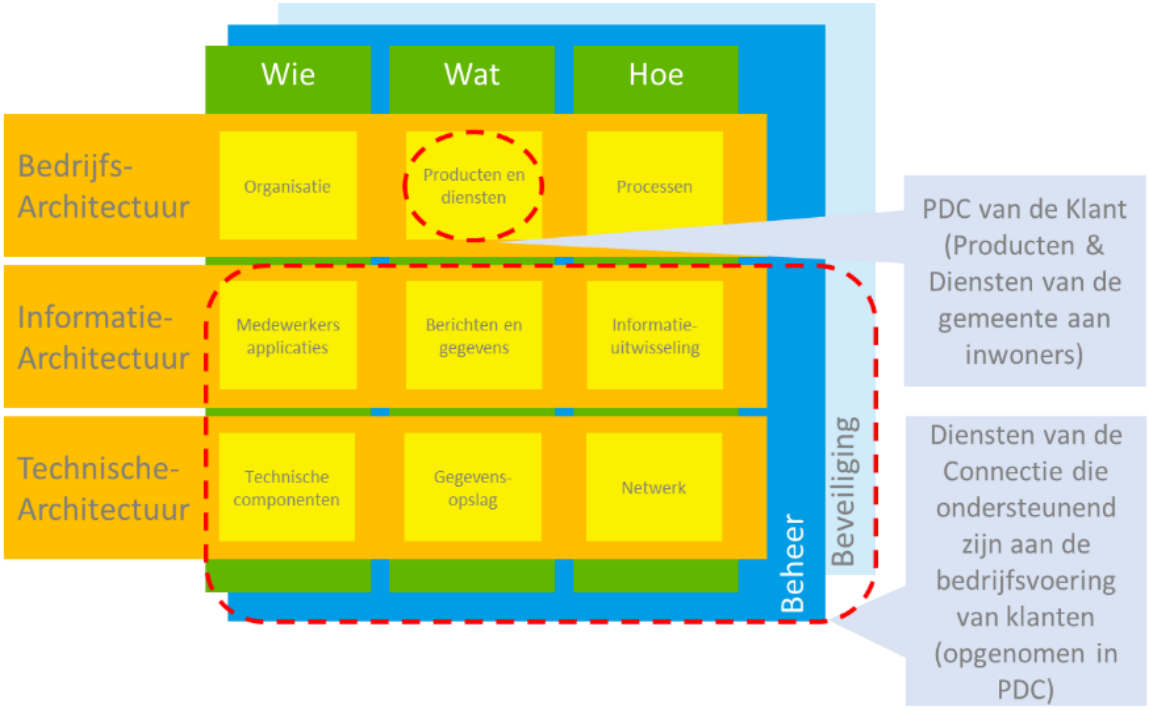
Binnen de Services store worden de diensten primair verdeeld volgens de Cloud standaard verdeling van IaaS, PaaS en SaaS. Om de werkplekomgeving eveneens op te nemen worden de workspace services toegevoegd aan de collectie.
In de Operations verzameling zijn de groepen Security & Management en Hybrid Operations (Hybrid operations omvatten de diensten die vereist zijn om hybride Cloud oplossingen te kunnen realiseren en beheren) opgenomen. Hierin worden de diensten opgenomen die nodig zijn voor het onderhoud van de diensten uit de Services Store. De invulling van deze diensten staan opgenomen in BlueDolphin. (BlueDolphin (valueblue.nl))

5 Gebruik van de Regionale Enterprise Technische architectuur

De Regionale Enterprise Architectuur bepaalt welke ICT diensten ingezet worden door De Connectie. Daarbij kunnen verschillende diensten toegepast worden om samen een geheel te vormen. De diensten worden opgenomen in de Enterprise Architect tool waar de drie architectuurlagen (Business-, Informatie- en Technische laag) samenkomen. Als modelleertaal wordt daarbij gestandaardiseerd op de Archimate (van The OpenGroup) standaard. We gebruiken de BlueDolphin Enterprise Architectuur Tool ter registratie van de objecten.

5.1 Producten & Diensten Catalogus

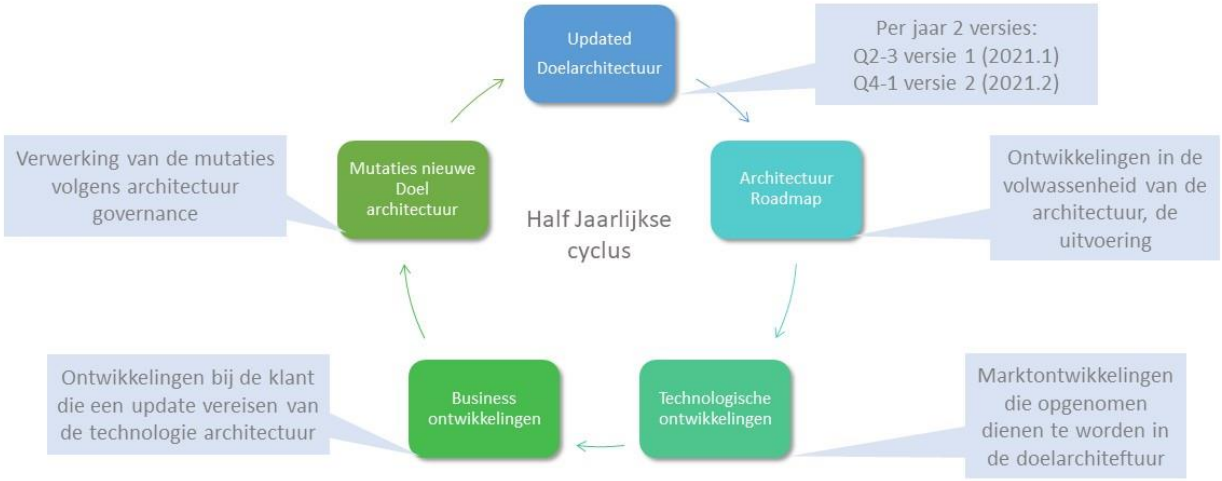
De producten en diensten zoals deze beschreven zijn in de producten en diensten catalogus (PDC) bevatten de diensten zoals deze aan de klanten van De Connectie aangeboden worden. Aan de hand van deze PDC wordt een vertaling gemaakt naar de benodigde bouwblokken (standaard producten). Binnen de Gemma referentie architectuur bevat de PDC van De Connectie de verzameling van producten en diensten zoals die aan de klanten worden geleverd. De PDC in het 9-vlaks model bevat de producten en diensten zoals de klanten van De Connectie die aan klanten leveren.



Doordat De Connectie als externe leverancier gezien wordt vanuit de klanten is het logisch om de producten en diensten aan te bieden middels een PDC.

5.2 Architectuurcyclus

De Regionale Enterprise Architectuur is continu aan verandering onderhevig. Dat maakt dat de verschillende architecturen niet statisch zijn maar veranderen. Door de veranderingen in zowel de technologie als bedrijfsarchitectuur dient de Enterprise architectuur herijkt te worden. Initieel zal deze 2x per jaar worden bijgewerkt.



De 3 triggers voor een mutatie van de Enterprise architectuur zijn achtereenvolgens:

- Wijzigingen vanuit de architectuur roadmap, de manier waarop onder architectuur gewerkt wordt is afhankelijk van de volwassenheid van het architectuurproces. De Regionale Enterprise Architectuur is een product van de architectuur en dient dan ook aan te sluiten bij de architectuurvolwassenheid van de stakeholders die hiermee werken. Door de architectuurvolwassenheid te betrekken in dit document ontstaat een passende en begeleidende architectuur die helpt bij verdere ontwikkeling van het architectuur proces;
- Technologische ontwikkelingen die opgenomen worden in de PDC, de technologische ontwikkelingen staan niet stil. De Connectie vormt de brug tussen deze technologieën en de klant. De Connectie dient

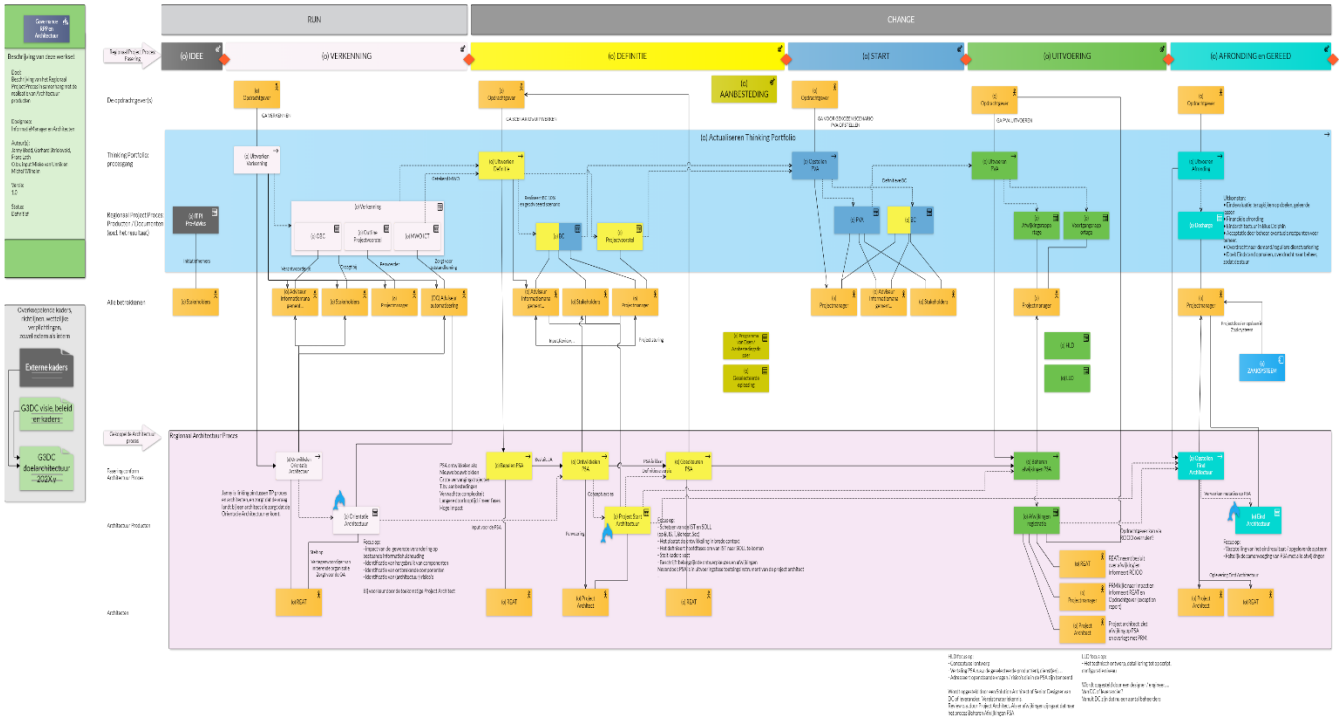
bijvoorbeeld klaar te zijn voor ontwikkelingen op o.a. RPA[5], IoT[6], artificiële intelligentie (AI) [7], Data wetenschap vlak;

- Ontwikkelingen bij de business, zoals aanpassingen van de visie en missie, die een mutatie van de Regionale Enterprise Architectuur vereisen, de rol en taak van de gemeenten veranderd. Dat maakt ook de behoefte aan technologiearchitectuur anders. Deze veranderingen dienen dan ook opgenomen te worden in de Regionale Enterprise Architectuur.

5.3 Het Architectuur proces en architectuur document

In BlueDolphin is de governance tussen het regionale portfolio proces en de architectuur opgetekend, deze link gaat naar de betreffende pagina, BlueDolphin (valueblue.nl).

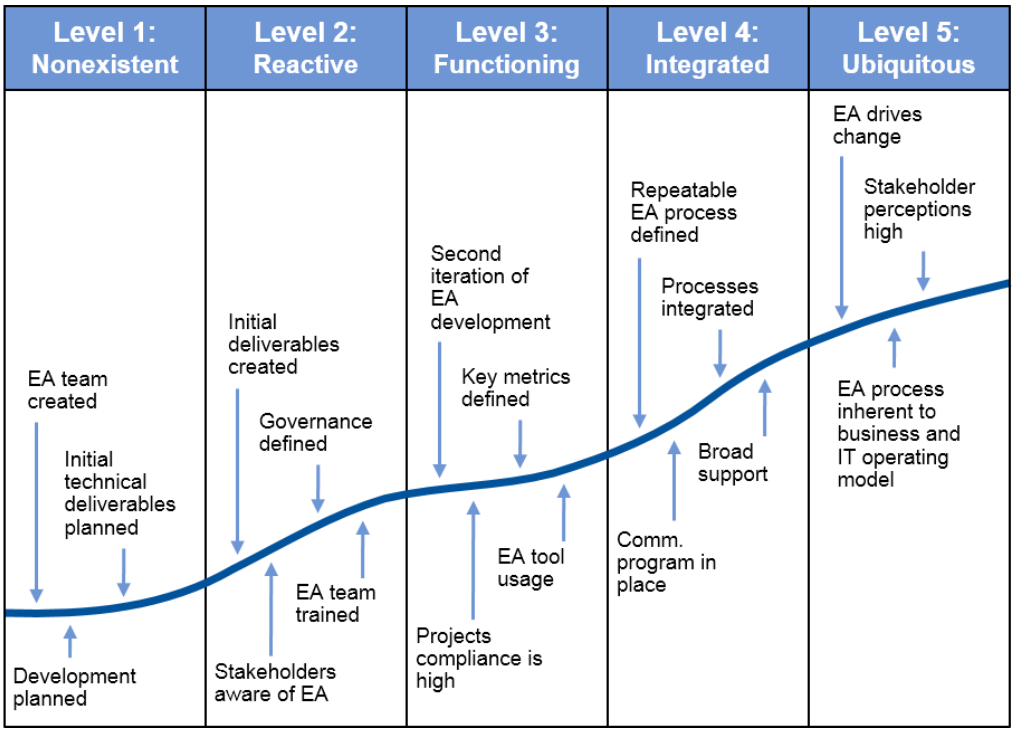
Onderstaand schema geeft de onderdelen Idee, verkenning, definitie, start, uitvoering en evaluatie weer.



[5] Robotgestuurde procesautomatisering
[6] Internet of Things
[7] Kunstmatige intelligentie

6 Architectuur roadmap

Om de Enterprise Architectuur optimaal tot zijn recht te laten komen is het van groot belang de architectuur als geheel te gaan zien. Voor de ontwikkeling van de architectuurfunctie binnen De Connectie wordt uitgegaan van het architectuur volwassenheidsmodel van Gartner zoals hieronder weergegeven:



Ten opzichte van de huidige stand van architectuur volwassenheid wordt gedurende de architectuur cyclus bepaald wat het huidige niveau is en hoe toegewerkt kan worden naar een volgend niveau. Binnen het Regionaal Enterprise Architectuur Team (REAT) zullen afspraken gemaakt worden over de doelstellingen en acties genomen worden om deze doelstellingen te halen.

Onderwerp	*Huidig Volwassenheidsniveau*	*Doelstelling volgende Enterprise architectuur*	*Niveau na afronding*
EA Team	Level 2: er is een EA team.	Samenwerking op EA niveau tussen verschillende architectuur disciplines	Level 3: het architectuurproces dient binnen de organisatie gestalte te krijgen.
EA Tools	Level 3: BlueDolphin EA gedeeltelijk in gebruik voor EA	BlueDolphin EA in gebruik voor EA	Level 4: EA tool is in gebruik bij de projecten.
PDC	Level 1: Technische producten zijn in gebruik	Afstemming tussen PDC klant, PDC De Connectie en producten	Level 2: initiële deliverables defined.
Governance	Level 1: Governance is vastgesteld binnen De Connectie	Governance vastgesteld voor de gehele EA	Level 2: Governance defined
Stakeholders	Level 1: Stakeholders zijn geïdentificeerd	Vanuit EA team de stakeholders bekend maken met de rol van EA	Level 2: EA Stakeholders zijn aangewezen en bekend met het bestaan van EA
Projectuitvoering	Level 1: maatwerk oplossingen per project	Afstemming PDC met EA	Level 2: Projecten aan de hand van PDC
EA Proces	Nvt	Vormgegeven EA proces	

7 Architectuur Kaders

7.1 Sourcing

Vanuit de 3GDC wordt de keuze gemaakt voor **een Hybrid Cloud** oplossing. Een hybrid cloud voldoet aan de eisen en wensen van de sourcing strategie. In deze strategie, Right Sourcing, worden bij elke vernieuwing of wijziging keuzes gemaakt op gebied van sourcing welke invloed hebben op de locatie van de data van de gemeenten en De Connectie, standaard zal de keuze zijn **SaaS first** als onderdeel van de **Cloud first** strategie. De informatieveiligheid, het eigenaarschap van de gegevens/informatie, de mate van vervlechting en privacy als ook een exit-strategie zijn hierbij essentiële aspecten waarmee rekening gehouden moet worden in de sourcingskeuze.

7.2 Netwerk Design

Binnen De Connectie werken we op basis van de multi tier architectuur. De gedachte achter een multi tier architectuur is software op te delen in meerdere componenten die met elkaar samenwerken. Hiermee kunnen componenten worden ontkoppeld van functionaliteit en hergebruik van functionaliteit te stimuleren. Iedere component heeft nu zijn eigen verantwoordelijkheden. Bij de Connectie architectuur wordt een 3-tierarchitectuur gebruikt. Bij deze architectuur is er een afzonderlijke tier voor de presentatie, de business logic + datatoegang en dataopslag. Dit wordt verder uitgewerkt in de Internet, Presentatie, Applicatie en Data (IPAD) functies met een fysieke scheiding van elkaar.

7.3 Intergemeenschappelijk verkeer – samenwerking

De aangesloten gemeenten (Arnhem, Rheden en Renkum) werken zoveel als mogelijk samen. Er is 1 tenant binnen de Microsoft omgeving ingericht om de samenwerking te bevorderen. De eigen identiteit zal daar waar gewenst en mogelijk is gewaarborgd blijven. De beveiliging zal moeten blijven voldoen aan de AVG. Het niet samenwerken leidt o.a. tot een hogere beheerlast en licentiekosten. Deze samenwerking vertaald zich naar de ingestelde governance structuur waarbij het regionale Chief Information Security Officer (CISO) overleg en het Regionale Enterprise Architectuur Team (REAT) adviseren aan de sturing via het Regionaal Chief Information Officer Overleg (RCIOO).

7.4 Voortbrengingsmethodiek ICT middelen

Bij De Connectie is een Test-, Acceptatie- en Productieomgeving ingericht voor de private cloud. Deze omgevingen zijn volledig van elkaar gescheiden, waarbij de Acceptatieomgeving op dezelfde wijze is ingericht als de Productie omgeving.

Alle ICT middelen volgen de Ontwikkeling, Test, Acceptatie en Productie (OTAP) methodiek.

Het pad dat wordt doorlopen is als volgt:

1. O: Ontwikkeling wordt niet bij De Connectie uitgevoerd en valt dus buiten deze architectuur.
2. T: We testen elk functioneel bouwblok inhoudelijk.
3. A: Na goedkeuring van de Test volgt installatie in de Acceptatie omgeving waarbij een gedocumenteerd Productie handboek opgeleverd moet worden.
4. P: Na de Acceptatie van de acceptatieomgeving worden de wijzigingen in Productie doorgevoerd.

7.5 De Werkplek

De huidige werkplekomgeving van de 3GDC is in basis opgeleverd (als Virtual Desktop Infrastructure (VDI) en dient verder geactualiseerd te worden. Hierbij is het nodig om recente veranderingen binnen de lokale overheid, wetgeving en bedrijfsvoering, maar ook de nieuwe ontwikkelingen in de ICT te betrekken, om zo tot een moderne en flexibele nieuwe werkplekomgeving te komen.

Om goed aan te kunnen sluiten bij de eisen en wensen van de gebruiker, is het nodig om de werkplekomgeving te baseren op de behoeften van de gebruiker. Uitgangspunt is dat de werkplekomgeving het werkproces (en daarmee: de gebruiker) zo veel mogelijk ondersteunt. Beperkingen, nodig om bijvoorbeeld de integriteit en veiligheid van systemen te bewaken, zijn onvermijdelijk maar worden wel in het juiste perspectief geplaatst; de werkplek is een middel en geen doel.

Een centraal aangeboden werkplek kent een grote mate van flexibiliteit. Gebruikers kunnen zelf uit de business store de applicaties installeren. De beslissing of deze applicaties en configuratie instellingen behouden blijven heeft impact op de oplossing voor wat betreft beheer en de betrokken beheerkosten. Van belang is dat de genoemde functionaliteit fundamenteel beschikbaar is in de centrale werkplek.

Vanuit De Connectie en haar klanten is er een behoefte om oplossingen naar de Cloud te brengen, op basis van de sourcing strategie (Er is een Cloud First strategie, echter Cloud is geen doel), om de werkplek, het werken op afstand, thuis, onderweg, etc. te kunnen faciliteren.

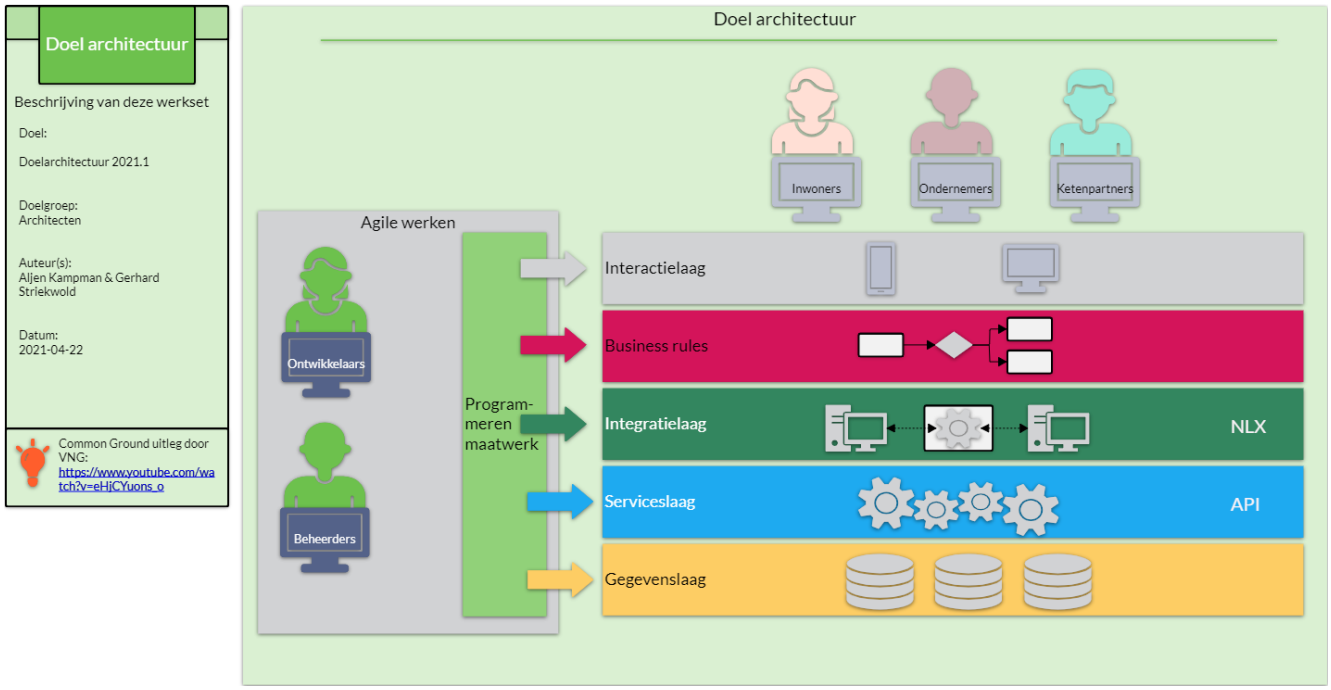
7.6 Common Ground, de toekomstige informatievoorziening

Op dit moment werken de gemeenten aan een toekomstige informatievoorziening die ze in staat stelt op een flexibele en moderne manier informatievraagstukken op te pakken. De Regionale Enterprise Architecten ondersteunen de gemeenten haar gegevenshuishouding volgens de Common Ground principes in te richten opdat het mogelijk is om snel en flexibel te vernieuwen, met in achtneming van de privacywetgeving en efficiënt om te gaan met data.

Een van de implicaties is dat de architectuur een gelaagdheid kent waarin de gegevens gescheiden worden van de interactie en de business rules. Dit komt tot uiting in het onderstaande 5 lagenmodel van Common Ground.

Belangrijke gevolgen zijn:

- Gegevens worden uniform gemaakt
- Gegevens worden opgehaald met zogenoemde API’s
- Er wordt gewerkt met één gemeenschappelijke integratielaag



7.6.1 Gegevens laag

Voor de implementatie is men afhankelijk hoe leveranciers hun applicaties hiervoor geschikt maken om te voldoen aan het standaard informatiemodel van Common Ground. Afhankelijk van de leverancier kan dit langer duren of bijvoorbeeld in geval van internationale leveranciers helemaal niet een doelstelling zijn.

7.6.2 Service- en Integratie laag

De Service laag bestaat uit API's als koppelvlak voor de applicaties. Een API is als een digitale stekkerdoos die applicaties met elkaar verbindt. Voor de Common Ground gaat het in het bijzonder over APIs waarmee je applicaties over het Internet kan koppelen. Zogenaamde REST APIs doen voor applicaties wat websites voor mensen doen. Websites presenteren informatie aan mensen, REST APIs maken applicaties en gegevens over het Internet beschikbaar voor andere applicaties.

NLX sluit aan bij de servicegerichte architectuur die GEMMA voorschrijft. NLX is een open source systeem om peer-to-peer gegevens uit te wisselen op basis van federatieve authenticatie, beveiligde connectiviteit en protocollen die faciliteren in een grootschalig API landschap met meerdere organisaties.

7.6.3 Business Rules en Interactie laag

In deze lagen kunnen processen en applicaties worden ingericht die gebruik maken van de onderliggende API's. Hierbij kan sprake zijn van maatwerk, eventueel in low-code platformen.

8 Dataclassificatie

De 3GDC hanteert de classificatie zoals deze voorgesteld wordt in de Baseline Informatiebeveiliging Overheid (BIO).
Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveau 's (BBN). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare bedreigers nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en is voor de G3DC BBN 2 tenzij minder kan, of meer nodig is.

Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. Elk niveau bouwt voort op het vorige niveau. Daarbij vult BBN2 de controls van BBN1 aan. BBN2 vult ook de overheidsmaatregelen van BBN1 aan of vervangt deze door maatregelen met meer gewicht. Hetzelfde geldt voor BBN3 in relatie tot BBN1 en BBN2. Recentelijk is door de IBD ook BBN2+ geintroduceerd (zie onderstaand schema).

De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd.
De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de Te Beschermen Belangen. De onderverdeling is als volgt:
BBN1: beschikbaarheid = Laag; integriteit = Laag; vertrouwelijkheid = Laag
BBN2: beschikbaarheid = Midden; integriteit = Midden; vertrouwelijkheid = Midden
BBN3: beschikbaarheid = Midden; integriteit = Midden; vertrouwelijkheid = Hoog

De 3GDC hanteert de volgende dataclassificatie classificatie:

Doel architectuur BIO	Basis Beveiligings Niveaus	Baseline Informatiebeveiliging Overheid (BIO)		
Beschrijving van deze werkset Doel: De basis beveiligings niveaus volgens de Baseline informatiebeveiling Overheid (BIO) ten behoeve van de Doelarchitectuur Doelgroep: Medewerkers Auteur(s): Gerhard Striekwold Datum: 2021-05-26	Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
	Geen BBN 0	Niet Nodig Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn.	Niet Zeker Informatie mag worden veranderd.	Openbaar Informatie mag door iedereen worden ingezien.
	Laag BBN 1	Belangrijk Informatie mag incidenteel niet beschikbaar zijn.	Beschermd Het bedrijfsproces staat enkele (integriteits-) fouten toe.	Bedrijfsvertrouwelijk Informatie is toegankelijk voor alle medewerkers van de organisatie.
	Midden BBN 2	Noodzakelijk Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk.	Hoog Het bedrijfsproces staat zeer weinig fouten toe.	Geheim Informatie is alleen toegankelijk voor een beperkte groep gebruikers.
	Hoog BBN 2+	Essentieel Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten.	Absoluut Het bedrijfsproces staat geen fouten toe.	Geheim Informatie is alleen toegankelijk voor direct geadresseerde(n).

Informatiesystemen op BBN1 niveau zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.
Controls en overheidsmaatregelen komen voort uit:

- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen).

BBN1	
Beschikbaarheid = Laag	Het informatiesysteem mag incidenteel uitvallen (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 28 uur; • maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen.
Integriteit = Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen. Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
Vertrouwelijkheid = Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: • financiële gevolgen: op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien:

- er vertrouwelijke informatie wordt verwerkt;

- mogelijke incidenten leiden tot bestuurlijke commotie;
- er onzekerheid bestaat of ook alle informatie van derden open is;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

BBN2	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/ gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatie brede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatie brede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.

Vertrouwelijkheid = Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of • bindende aanwijzing van de AP in verband met schending van de privacy; of • directe imagoschade, bijvoorbeeld door negatieve publiciteit.

BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threat's (APT's)[1],
die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien:

- verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;
- informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden;
- aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen);

Dit Basis Beveiligings Niveau zal niet van toepassing zijn bij gemeenten.

BBN3	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Organisatie brede negatieve publiciteit (imagoschade) of

	significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit **= Midden**	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Organisatie brede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid **= Hoog**	Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; • informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of • aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of • weerstand tegen statelijke actoren is noodzakelijk.

[1] Een Advanced Persistent Threat is een langdurige en doelgerichte cyberaanval waarbij een onbevoegd persoon onopgemerkt en langdurig toegang krijgt tot een netwerk. Het doel is om continu toegang te krijgen en gegevens te stelen.

Hieronder volgens achtereenvolgens de integriteits- en veiligheids- niveaus en maatregelen.

Niveau	**Authenticatie**	**Autorisatie**	**Monitoring**	**Beveiliging**
Niet zeker	Geen	Geen	Geen	Geen
Bedrijfs-vertrouwelijk (laag) (BBN1)	Authenticatie 'basis'	Autorisatie vereist	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van 1/2 jaar.	Inputvalidatie. Controleren op mutatie tijdens transport. Transportbeveiliging of berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Geheim (Midden) (BBN2)	Authenticatie 'midden'	Autorisatie vereist. 4-ogen principe vereist	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van maximaal 2 jaar of langer bij een vermoed beveiligings-incident.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Geheim, statelijke actoren (Hoog) (BBN3)	Authenticatie 'hoog' (geen SSO)	Autorisatie vereist. 4-ogen principe vereist	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van minimaal 3 jaar bij een vermoed beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Gegevens worden niet buiten hun bron opgeslagen (behalve voor beschikbaarheid) en niet buiten hun bron gewijzigd. Na uitvoering van een service blijven gewijzigde gegevens consistent.

De authenticatieniveaus verwijzen naar het vereiste beveiligingsmechanisme:

- Basis: authenticatie gebaseerd op iets wat men weet (naam/wachtwoord).
- Midden: authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat).
- Hoog: authenticatie gebaseerd op eigenschap, bijvoorbeeld irisscan of vingerafdruk.

De autorisatieniveaus verwijzen naar de wijze waarop de controle wordt uitgevoerd. Vanaf beschermd is altijd autorisatie verplicht en vanaf hoog komt daar het 4-ogen principe bij. Het 4-ogen principe bestaat uit één persoon die vastlegt en één persoon die fiatteert.

Bij monitoring van de niveaus 'beschermd' en 'hoog' wordt de term 'relevant' gebruikt. Welke gegevens 'relevant' zijn, is ter beoordeling van de eigenaar. Voorbeelden en richtlijnen voor relevante gegevens zijn stamgegevens (gegevens waarop andere gegevens gebaseerd zijn), gegevens in basis- en kernregistraties, privacygevoelige informatie en gegevens beschermd door wet- en regelgeving.

Bij datatransport is berichtbeveiliging te prefereren boven transportbeveiliging. Echter, transportbeveiliging kan in bepaalde gevallen eenvoudiger en/of goedkoper te implementeren zijn. Daarom is bij classificatieniveau 'beschermd' de keuze voor transportbeveiliging en berichtbeveiliging open gelaten. Bij 'hoog' en 'absoluut' is de classificatie zodanig dat berichtbeveiliging toegepast moet worden.

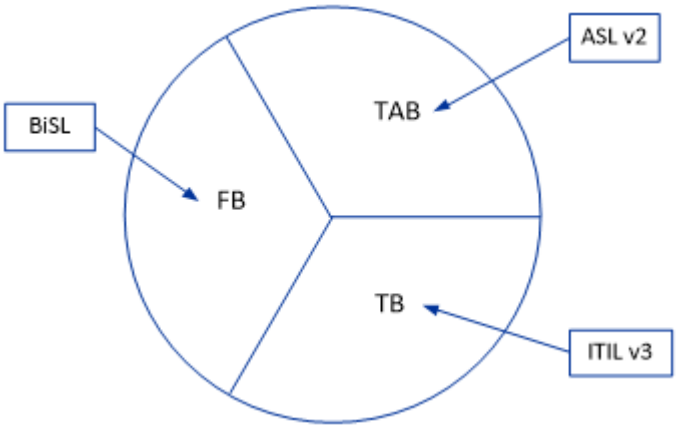
Ten aanzien van de vertrouwelijkheid geldt de onderstaande classificatie en richtlijnen.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Niet zeker	Geen	Geen	Geen	Geen
Bedrijfs-vertrouwelijk (laag) (BBN1)	Authenticatie 'basis'. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgen de foutieve authenticatiepog ingen. Authenticatie 'basis' nodig voor deblokkeren.	Autorisatie vereist (lid van de organisatie)	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van 1/2 jaar.	Outputvalidatie. Versleuteling tijdens transport buiten netwerk van De Connectie via transportbeveiliging of bericht-beveiliging. Kopieën van gegevens moeten net zo goed beveiligd worden. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevens-eigenaar toestemming heeft gegeven.
Geheim (Midden) (BBN2)	Authenticatie 'midden' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute	Autorisatie vereist (specifieke rol)	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk van de Connectie via berichtbeveiliging. Kopieën van

	sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgen de foutieve authenticatiepog ingen. Authenticatie 'midden' nodig voor deblokkeren.			gegevens moeten minimaal net zo goed beveiligd worden. Aantal kopieën minimaliseren. Berichtbeveiliging. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.
Geheim, statelijke actoren (Hoog) (BBN3)	Authenticatie 'hoog' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgen de foutieve Authenticatiepog ingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen SSO toegestaan.	Autorisatie vereist (specifieke rol)	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoringgegevens bewaren voor periode van 7 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van De Connectie. Geen kopieën toegestaan behalve voor beschikbaarheid. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.

9 Beheer

In 1986 heeft prof.Dr.Ir. Maarten Looijen de driedeling van beheer uitgewerkt, dit is tot op vandaag nog steeds van toepassing.



De driedeling bestaat uit:

1. De Functioneel Beheerders die op basis van het in 2005 geïntroduceerde Business Information Services Library (BiSL) raamwerk gebruik maken.
2. De Technisch Applicatiebeheerders die op basis van het Application Services Library v2 (ASL) raamwerk gebruik maken.
3. De Technische Beheerders die op basis van het Information Technology Infrastructure Library v4 (ITIL) raamwerk gebruik maken.

Bij de 3GDC zijn dit de raamwerken waar binnen de behoeften van de gebruikersorganisatie op een procesmatige manier uitgewerkt worden.

10 Bijlage A – Services Store

In dit hoofdstuk worden de diensten beschreven zoals deze aangeboden worden aan de klanten van de Connectie. Deze diensten zijn onderverdeeld in de volgende logische groepen:

- Workspace, alle diensten die vereist zijn voor het leveren van een digitale werkomgeving;
- SaaS (Software as a Service), de verzameling applicatiediensten zoals deze technisch onderhouden worden en geleverd worden;
- PaaS (Platform as a Service), infrastructuur platform bestaande uit IaaS aangevuld met Besturingssysteem, Middleware en Runtime;
- IaaS (infrastructure as a Service), infrastructuur diensten bestaande uit gevirtualiseerde hardwarecomponenten.

In de volgende paragrafen worden de diensten per groep verder uitgewerkt. De samenstelling van de diensten in een groep is dynamisch. Veranderingen in de technologie en in de Business-, en Informatiearchitecturen maken dat de behoefte aan technologische diensten veranderd.
Deze diensten zullen in de Enterprise Architectuur Tool (BlueDolphin) worden gedefinieerd en uitgewerkt binnen de projecten.

10.1 Datacenter diensten

De diensten zoals benoemd in de Services Store maken gebruik van technologische componenten (hardware). Deze componenten zijn ondergebracht in een datacenter. Met het datacenter wordt de fysieke locatie bedoeld waar IT-componenten geplaatst worden en waar voorzieningen getroffen zijn voor:

- Stroomvoorziening:
  - Redundant;
  - Ononderbroken;
  - Voorzien van noodstroom voorziening;
- Brandblusinstallatie;
- Redundante koeling;
- Beveiligde toegang.

De Connectie maakt gebruik van de volgende 3 datacentra:

- Stadskantoor;
- Stadhuis (Arnhem);
- Dataplace Arnhem.

Stadskantoor en Dataplace zijn daar bij de 2 primaire datacenterlocaties die logisch als 1 datacenter acteren volgens het stretched datacenter principe[1]. De Stadhuis locatie vormt als derde locatie de witness[2] van de 2 primaire locaties. Er wordt voorzien in toekomstig gebruik van Cloud IaaS diensten als uitbreiding van de hypervisor diensten.

1 Het **Stretched Datacenter** heeft een gunstig effect op de beheerorganisatie. Onderhoud op hardware kan in **principe** overdag plaats vinden in plaats van 's avonds, 's nachts of in de weekenden.

2 een witness is de scheidsrechter die bepaald waar op dat moment een hardware component actief mag zijn.,

10.2 IaaS diensten

Binnen de IaaS diensten worden de diensten in de volgende subgroepen verdeeld:

- Server & Virtualisatie;
- Gegevensopslag;
- Netwerk.

10.3 PaaS diensten

De platform diensten bevatten de diensten die afgenomen kunnen worden waarop applicaties ontwikkeld/ uitgerold kunnen worden.

10.4 SaaS diensten

Als externe leverancier van klanten van De Connectie, levert De Connectie applicatiefunctionaliteit als dienst.

Met behulp van deze diensten is De Connectie in staat om applicaties aan te bieden aan de afnemende klanten. Daarbij ligt de technische verantwoordelijkheid bij De Connectie.

10.5 Workspace diensten

De workspace diensten bestaan uit de diensten die nodig zijn voor het leveren van de werkplekvoorzieningen.

11 Bijlage B – Operations

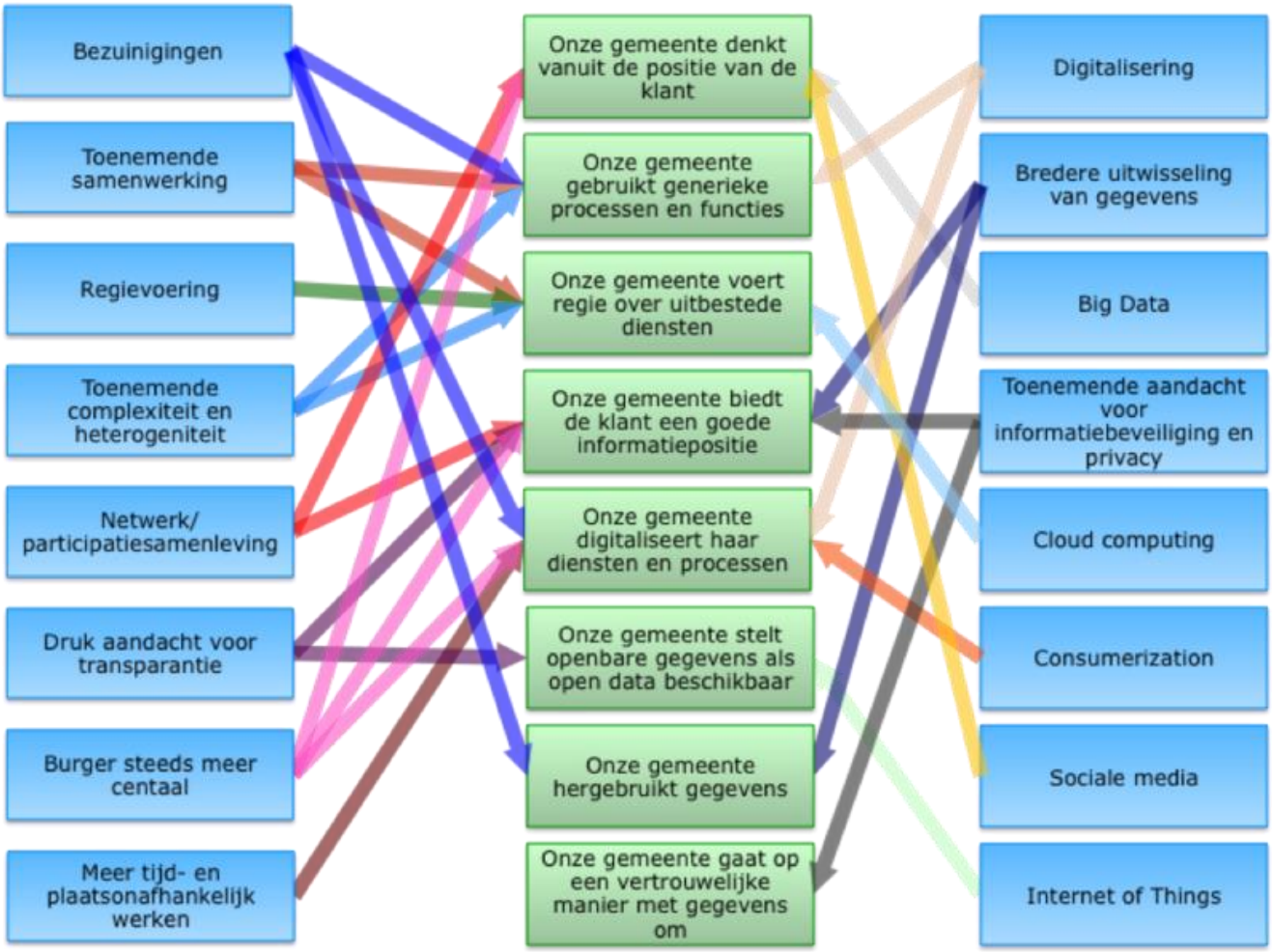
In dit hoofdstuk worden de Operations diensten beschreven. Deze diensten worden primair ingezet voor het onderhouden van de diensten uit de Services Store. De Operations diensten zijn verdeeld in Security & Management en Hybrid Operations groepen.

12 Bijlage C – Katern GEMMA Architectuurprincipes

Principes

Dit hoofdstuk beschrijft de architectuurprincipes. Elk principe is voorzien van een korte motivatie die aangeeft waarom het principe belangrijk is alsook een lijst van implicaties die aangeven wat de consequenties zijn van het hanteren van het principe. Onderstaand figuur geeft een overzicht van de voorgestelde principes en de relaties met de ontwikkelingen die eraan ten grondslag liggen.

De principes starten met "Onze gemeente..." om aan te geven dat ze vanuit het perspectief van de gemeente zijn geformuleerd. In plaats daarvan kan natuurlijk ook worden gelezen "ons samenwerkingsverband" daar waar gemeenten diensten gezamenlijk aanbieden. Overal waar wordt gesproken over "klant" wordt in algemene zin verwezen naar burgers, bedrijven, overheidsorganisaties en instellingen die diensten afnemen van de gemeente. Het is helder dat de gemeente als dienstverlener en de burger als klant slechts één van de rolverdelingen is, naast bijvoorbeeld politieke organisatie-klant. Daar waar de klantrol niet passend is zal daarom de burger in meer algemene zin worden genoemd.



Figuur - Ontwikkelingen en daaruit voortvloeiende principes

12.1 Onze gemeente biedt de klant een goede informatiepositie

Een goede informatiepositie is voor klanten cruciaal om snel en gemakkelijk hun weg te vinden binnen de overheid. Het zorgt er ook voor dat zij de verantwoordelijkheid kunnen nemen die in toenemende mate van hen wordt verwacht vanuit een nieuw evenwicht tussen samenleving en overheid. Dat gaat niet alleen over het ontvangen van informatie; het gaat ook over het aan het stuur zetten van de klant omtrent het gebruik van zijn gegevens. Klanten moeten in staat zijn incorrecte registratie van hun gegevens te signaleren, zodat ze voor zichzelf op kunnen komen.

Implicaties:

- Klanten hebben laagdrempelig toegang tot een actueel en correct beeld van alle voor hen relevante gegevens waarover onze gemeente beschikt, zoals:
  - algemene informatie over producten en diensten;
  - de wet- en regelgeving waaraan zij moeten voldoen;
  - hun eigen gegevens (incl. hun inhoudelijke dossiers en gegevens in sectorale registraties);
  - de status van hun lopende zaken;
  - de gegevens die zijn gebruikt om tot een besluit te komen en de regels die daarbij zijn gehanteerd (traceerbaarheid);
  - wie hun gegevens heeft ingezien en wat de gemeente met gegevens heeft gedaan (transparantiebeginsel).
- Medewerkers hebben minimaal toegang tot dezelfde informatie als klanten (voor zover dat relevant is voor de uitoefening van hun taak).
- Informatie is niet versnipperd over allerlei loketten en applicaties, maar geïntegreerd en zo nodig geaggregeerd beschikbaar.
- Alle verzoeken van klanten die gevolgd moeten worden, worden geregistreerd als zaak en wijzigingen in de status worden op een centrale plaats geregistreerd.
- Klanten geven expliciete toestemming voor het gebruik van hun eigen gegevens door de gemeente of samenwerkingspartners voor taken waarvoor geen expliciete wettelijke grondslag bestaat.
- Klanten hebben de mogelijkheid om onjuistheden in hun gegevens te corrigeren of te laten corrigeren of om de gegevens te laten verwijderen (voor zover dit wettelijk kan).
- Klanten worden proactief door de gemeente geïnformeerd over zaken waarvan zij hebben aangegeven dat zij daarover geïnformeerd willen worden.
- Klanten hebben, binnen de kaders van wet- en regelgeving, het recht om vergeten te worden.

12.2 Onze gemeente denkt vanuit de positie van de klant

De gemeente is er voor burgers en bedrijven en zorgt ervoor dat deze de dienstverlening krijgen die ze kunnen verwachten. Zij kunnen immers niet zomaar naar een andere aanbieder als zij niet tevreden zijn. De administratieve lasten voor deze klanten moeten daarbij zoveel mogelijk worden beperkt. Klanten stellen steeds hogere eisen aan de kwaliteit van de dienstverlening van gemeenten. Diensten moeten aansluiten bij de klantbehoefte en klanten zouden geen hinder moeten ondervinden van de interne organisatie van gemeenten en andere (overheids)organisaties waarmee de gemeente samenwerkt. Anderzijds wordt ook van klanten verwacht dat ze waar mogelijk zelf verantwoordelijkheid nemen. Daarnaast zijn burgers en bedrijven niet alleen maar klant; met een aantal gemeentelijke taken krijgen zij ongevraagd te maken (zoals handhaving).

Implicaties:

- Onze gemeente heeft een goed beeld van klantbehoeften die bestaan, onder andere door pro-actief te onderzoeken wat er leeft in de maatschappij (bijvoorbeeld via sociale media) en door klanten te vragen hoe zij de dienstverlening ervaren.
- Onze gemeente vertelt klanten duidelijk wat er van hen verwacht wordt en ondersteunt klanten bij het helder krijgen van hun vraag.
- Medewerkers hebben alle voor hen relevante en toegankelijke informatie over klanten beschikbaar, inclusief informatie over hun contact met de gemeente en hun lopende en afgeronde zaken.
- Diensten worden ontwikkeld vanuit het perspectief van, en in samenwerking met klanten.
- Diensten zijn eenvoudig vindbaar (bijv. snel te vinden op website) en laagdrempelig toegankelijk.
- Klanten wordt op relevante momenten gevraagd om hun voorkeuren en specifieke wensen en daarmee wordt rekening gehouden bij de diensten die worden geleverd.
- Klanten wordt niet gevraagd naar gegevens die de gemeente zelf al beschikbaar heeft of die toegankelijk zijn voor de gemeente (m.u.v. gegevens om zichzelf te identificeren).
- Wanneer de gemeente een dienst realiseert in samenwerking met andere (overheids)organisaties dan ervaren klanten een geïntegreerde dienst.
- Bij de inrichting van processen en systemen wordt in eerste instantie vanuit de meerwaarde en behoefte voor de klant geredeneerd, voordat wordt gedacht in termen van oplossingen.
- De gemeentelijke informatievoorziening is nadrukkelijk ook ontwikkeld om samenwerking met en participatie van klanten en samenwerkingspartners te faciliteren.

12.3 Onze gemeente digitaliseert haar diensten en processen

Voor een modern proces is een papieren document een obstructie; het is niet efficiënt en het hindert tijd- en plaatsonafhankelijk werken. Daarom worden klanten verleid gebruik te maken van het digitale kanaal, processen zo veel als mogelijk geautomatiseerd en worden papieren documenten voorkomen. Klanten verwachten tegenwoordig ook dat dienstverlening digitaal wordt aangeboden. Dit is ook een expliciete ambitie van de overheid en uitgewerkt in de visiebrief ‘Digitaal 2017’ [12]. Er moet niet uit het oog worden verloren dat niet iedereen beschikt over voldoende digitale vaardigheden en dat persoonlijk contact op bepaalde momenten of voor bepaalde zaken belangrijk kan zijn. Het opslaan van gegevens in elektronische vorm maakt het veel eenvoudiger om deze te delen. Elektronische gegevens kunnen ook geautomatiseerd worden verwerkt door IT-systemen. Het elektronisch uitwisselen van gegevens is veel efficiënter en minder foutgevoelig dan het handmatig uitwisselen van gegevens.

Implicaties:

- Klanten hebben digitale diensten tot hun beschikking waarmee ze alle veelvoorkomende interacties veilig met de gemeente kunnen afhandelen.
- Digitale diensten voor klanten en medewerkers zijn toegankelijk via verschillende apparaten, ook voor mensen met een functiebeperking en waar nodig 24x7 beschikbaar.
- Ingaande en uitgaande communicatie vindt zoveel mogelijk digitaal plaats en we stimuleren dat via kanaalsturing.
- Medewerkers worden gefaciliteerd in het digitaal aanbieden, ontsluiten en bewerken van alle gegevens.
- Handmatige invoer of uitwisseling van gegevens wordt zoveel mogelijk voorkomen, met name als er sprake is van hoge volumes.
- Binnenkomende fysieke gegevensdragers (documenten) worden omgevormd in elektronische vorm, gestructureerd en voorzien van metadata (zoals een classificatie en toegangsregels).

- Gegevens worden bij creatie direct voorzien van metadata en op dat moment en bij alle wijzigingen van inhoud of context wordt bepaald of het bewaard moet worden als archiefobject.
- Gegevens worden in gestructureerde vorm beheerd en alleen ten behoeve van communicatie in de vorm van documenten verpakt en gecommuniceerd.
- Archivering van gegevens (incl. documenten) vindt digitaal plaats en zorgt ervoor dat deze beschikbaar, vindbaar, leesbaar en authentiek blijft en dat toegangsregels, bewaar- en vernietigingstermijnen worden bewaakt.
- Er zijn voorzieningen voor elektronische parafen en handtekeningen beschikbaar voor medewerkers en klanten.
- De voortgang van processen wordt digitaal bewaakt.

12.4 Onze gemeente gaat op een vertrouwelijke manier met gegevens om

Klanten verwachten dat de gemeente op een zorgvuldige manier met hun gegevens om gaat en dat deze niet in handen komen van onbevoegden. De visiebrief digitale overheid [12] besteedt daarom specifiek aandacht aan informatieveiligheid. Ontwikkelingen als consumerization en tijd- en plaatsonafhankelijk werken vragen ook om extra aandacht voor de beveiliging van informatie. Grenzen van organisaties vervagen en traditionele beveiligingsmaatregelen passen niet meer. Cybercriminaliteit kan zorgen voor ernstige ontregeling van organisaties. Het is daarom belangrijk de risico's expliciet te maken. Hierdoor kunnen de meest passende maatregelen worden genomen en worden overmatige maatregelen vermeden.

Implicaties:

- Onze gemeente is aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD).
- Onze gemeente heeft een informatiebeveiligingsbeleid gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) [4].
- Voor alle gegevens en applicatiefuncties (autorisatie-objecten) zijn verantwoordelijken aangewezen.
- Voor alle autorisatie-objecten is aangegeven welke rollen of gebruikers geautoriseerd toegang kunnen krijgen.
- Alle toegang tot autorisatie-objecten wordt expliciet geauthenticeerd en geautoriseerd, tenzij deze openbaar toegankelijk zijn.
- Gegevens zijn voorzien van een BIV classificatie die aangeeft wat het gewenste niveau van Beschikbaarheid, Integriteit en Vertrouwelijkheid is.
- Informatiebeveiligingsmaatregelen zijn gebaseerd op het informatiebeveiligingsbeleid, de BIV classificatie van de betrokken gegevens en een risico-analyse vanuit procesperspectief.
- Alle toegang tot gevoelige gegevens wordt gelogd en regelmatig beoordeeld.
- Uitwisseling van gevoelige gegevens vindt niet in bulk plaats, maar is toegespitst op de vraag zodat het beperkt is tot wat noodzakelijk is.
- Informatiebeveiliging wordt integraal meegenomen bij het ontwerp en de inrichting van applicaties en infrastructuur.
- Informatiebeveiliging wordt ook geborgd in afspraken (en controle op naleving ervan) met samenwerkingspartners en leveranciers van diensten of IT-systemen.
- Alle betrokkenen zijn zich bewust van informatiebeveiligingsmaatregelen en deze worden onder meer geborgd door periodieke interne en externe audits.

12.4.1 Onze gemeente gebruikt generieke processen en functies

Gemeenten worden door de overheid geconfronteerd met bezuinigingsmaatregelen en krijgen tevens extra taken. Door te denken in generieke processen en systemen kunnen diensten eenvoudiger worden gedeeld

met andere gemeenten en kosten worden bespaard. Ook kan eenvoudiger gebruik worden gemaakt van standaard oplossingen die beschikbaar zijn in de markt en wordt maatwerk voorkomen. Klanten willen de overheid in haar dienstverlening ook zo veel mogelijk ervaren als één organisatie en generieke processen dragen daar aan bij. Gemeenschappelijke diensten hoeven niet in tegenspraak te zijn met het hebben van een eigen identiteit. De "couleur locale" kan grotendeels tot uitdrukking worden gebracht via specifieke beleidskeuzes en de persoonlijke aandacht van medewerkers.

Implicaties:

- De gemeente voert processen op een voor elke burger herkenbare manier uit.
- Processen worden gebaseerd op generieke en landelijk beschikbare procesmodellen.
- Functionele specificaties worden gezamenlijk met andere gemeenten opgesteld en niet specifiek gemaakt voor de eigen gemeente.
- Bij het specificeren van functionaliteit wordt een goede balans gezocht tussen genericiteit en voldoende procesondersteuning.
- Processen en systemen worden niet ingericht op uitzonderingen.
- Gemeentespecifieke keuzes worden uitgedrukt in (beleids)regels die binnen de generieke processen en functionaliteiten gehanteerd kunnen worden.
- Er worden alleen gemeentespecifieke beleidsregels opgesteld als dat noodzakelijk is voor de specifieke gemeentelijke context.
- Er zijn soms concessies nodig bij het inrichten van processen en systemen om ervoor te zorgen dat deze op meerdere gemeenten passen.
- Applicaties kunnen door meerdere gemeenten worden gebruikt (incl. hun eigen beleidsregels), zonder ze volledig voor alle gemeenten specifiek in te richten, te beheren en te betalen.
- Als er landelijke voorzieningen of bouwstenen beschikbaar zijn dan wordt daar gebruik van gemaakt om zo gemeentespecifieke oplossingen te voorkomen.

12.4.2 Onze gemeente hergebruikt gegevens

Binnen de Nederlandse overheid is afgesproken dat burgers niet wordt gevraagd om gegevens waar de overheid zelf al over beschikt. In het algemeen is de beschikbaarheid en kwaliteit van gegevens belangrijk. Door duidelijke afspraken te maken over waar gegevens worden beheerd en waarvandaan ze worden verstrekt wordt het delen ervan veel eenvoudiger en worden mogelijke inconsistenties voorkomen. Op landelijk niveau zijn er hiertoe basisregistraties gedefinieerd die door alle overheidsorganisaties moeten worden gebruikt. Binnen de gemeente is ook hergebruik van andere breed gebruikte gegevens relevant (kerngegevens). In de visie op de verdere ontwikkeling van het stelsel wordt ook landelijk breder gekeken dan basisgegevens. Ook is de burger zelf nadrukkelijk benoemd als gebruiker van de landelijke basisregistraties en wordt ook hergebruik van gegevens van/door private organisaties voorgesteld.

Implicaties:

- Klanten wordt niet gevraagd naar gegevens die de gemeente zelf al beschikbaar heeft of die eenvoudig toegankelijk zijn voor de gemeente (en passen bij de doelbinding).
- Reeds bekende gegevens worden vooringevuld in formulieren, waarbij klanten de mogelijkheid krijgen om aan te geven of deze gegevens kloppen.
- De gemeente heeft een aantal kernregistraties ingericht voor andere gegevens die breed binnen de gemeente worden gebruikt (kerngegevens).
- Er zijn duidelijke afspraken over gegevens die worden uitgewisseld met anderen zoals over doel, gebruikstermijn en de standaarden, waarbij de standaarden van Forum Standaardisatie leidend zijn.

- Vermeende onjuistheden in gegevens worden teruggemeld aan de desbetreffende bronhouder van de gegevens.
- Iedere gegevensverzameling heeft een eigenaar die verantwoordelijk is voor beschikbaarheid, integriteit, vertrouwelijkheid, volledigheid en kwaliteit.
- Voor alle soorten gegevens is een bron aangewezen en afnemers zorgen ervoor dat zij (direct of indirect) deze bron gebruiken voor het raadplegen en muteren van deze gegevens.
- Gegevens zijn uniek identificeerbaar en voorzien van relevante contextinformatie en metadata.
- Verwijzen naar gegevens heeft de voorkeur boven kopiëren en daarom wordt waar mogelijk alleen een verwijzing (URI) van de hergebruikte gegevens opgenomen.

12.4.3 Onze gemeente stelt openbare gegevens als open data beschikbaar

De overheid stelt hoge eisen aan de transparantie van overheidsorganisaties. Toegang tot informatie uit overheidsorganisaties is een kernwaarde in de democratie en is wettelijk vastgelegd. Overheidsinformatie is in beginsel vrij beschikbaar, tenzij de WOB, WBP of andere wetgeving bepaalt dat de gevraagde informatie niet geschikt is om openbaar te maken. Het openbaar, vindbaar en herbruikbaar aanbieden van open data heeft positieve maatschappelijke en economische effecten: het voorziet in een behoefte, heeft economische waarde en leidt tot meer transparantie en participatie. Zo kunnen anderen nieuwe toepassingen ontwikkelen en/of deze gegevens via (mobiele) applicaties laagdrempelig ontsluiten richting klanten. Het versterkt ook de informatiepositie van de klant zodat deze over dezelfde informatie kan beschikken als de gemeente. Het faciliteert ook publiek/private samenwerking en ontlast de gemeente van de ontwikkeling van allerlei eindgebruikerstoepassingen.

Implicaties:

- Alle gegevensverzamelingen die maatschappelijk of economisch waardevol zijn en waarvoor geen beperkingen vanuit wetgeving of hun classificatie gelden (bijvoorbeeld vanuit het perspectief van privacy) worden als open data beschikbaar gesteld.
- Gegevensverzamelingen met daarin persoonsgegevens worden indien nodig geanonimiseerd zodat deze niet meer herleidbaar zijn tot personen, voordat ze worden gepubliceerd als open data.
- Open data wordt beschikbaar gesteld conform standaarden van het Forum Standaardisatie, bij voorkeur ook betekenisvol (als Linked Open Data) en geoptimaliseerd voor mobiele ontsluiting.
- Bij het selecteren van applicaties wordt expliciet als eis meegegeven dat alle gegevens benaderbaar zijn, zodat ze middels specifieke voorzieningen als open data kunnen worden ontsloten.
- Er wordt aangesloten bij beschikbare landelijke of sectorale voorzieningen voor de ontsluiting van specifieke open data zoals PDOK voor geo-informatie.
- Als er geen specifieke landelijke voorzieningen voor specifieke open data beschikbaar zijn dan borgt de gemeente zelf de bestendigheid, bruikbaarheid en beschikbaarheid.
- Open data wordt ook kenbaar gemaakt op de daarvoor beschikbare publicatiekanalen zoals data.overheid.nl en het Nationaal Georegister voor geo-informatie.

12.4.4 Onze gemeente voert regie over uitbestede diensten

Gemeenten willen graag kwalitatief hoogwaardige dienstverlening bieden, maar wel tegen acceptabele kosten. De gemeente kijkt daarom kritisch of zij taken zelf uitvoert of dat het logischer is deze gezamenlijk met andere gemeenten of partners uit te voeren, of uit te besteden aan de markt. Voor verschillende taken zijn gespecialiseerde organisaties beschikbaar die dat beter of efficiënter kunnen dan de gemeente. In een aantal gevallen is samenwerking verplicht, bijvoorbeeld op regionale schaal. Cloud computing is een belangrijke ontwikkeling die ook als een vorm van outsourcing kan worden gezien. Als taken elders worden

belegd is het belangrijk dat de gemeente hier de regie op blijft voeren. De verantwoordelijkheid blijft namelijk bij de gemeente.

Implicaties:

- Onze gemeente heeft een sourcingstrategie waarin is beschreven welke diensten zelf worden uitgevoerd, welke kunnen worden uitbesteed en hoe met uitbesteding wordt omgegaan, inclusief de positionering van clouddiensten.
- De sourcingstrategie wordt vertaald naar een set van kavels die maximale interne samenhang vertonen en minimale onderlinge afhankelijkheden, waarbij de koppelvlakken expliciet worden toegewezen aan een kavel zodat de gemeente zelf geen systeemintegrator hoeft te zijn.
- Voordat wordt besloten om taken door anderen of gezamenlijk uit te laten voeren wordt een business case opgesteld waarin ondermeer de kosten en baten expliciet worden gemaakt.
- Bij het uitbesteden van diensten worden de volgende zaken ingericht:
  - het bundelen van de behoeften;
  - het vertalen van de behoeften naar producten en diensten, passend binnen organisatie-standaarden en -afspraken
  - het inkopen van producten en diensten en het maken van afspraken met leveranciers;
  - het controleren van afspraken met leveranciers.
- Er wordt geïnvesteerd in medewerkers met competenties die essentieel zijn voor regievoering.
- Er wordt met leveranciers expliciete afspraken gemaakt over o.m. taken en verantwoordelijk-heden, kwaliteit van dienstverlening, uit te wisselen gegevens en mandatering.
- Onze gemeente zorgt ervoor dat ze altijd toegang houdt tot gegevens waarvoor ze verantwoordelijk is.