



Centrum Indicatiestelling Zorg

Bijlage 1 - Project Start Architectuur (PSA) Data & Analytics





Centrum Indicatiestelling Zorg

Documentbeheer

Titel	Project Start Architectuur (PSA) Data & Analytics
Versie	1.0
Datum	29-06-2022
Auteurs	Reza Ahmadi (Enterprise Architect - CIO Office)
Status	Definitief

Inhoudsopgave

1	Inleiding	4
2	Referentiearchitecturen	5
2.1	Nederlandse Overheid Referentie Architectuur	5
2.2	Enterprise Architectuur Rijksdienst	5
2.3	CIZ architectuurprincipes	5
2.4	ISO-25010	6
2.5	Microsoft Cloud Adoption Framework	6
2.6	Microsoft Azure Well-Architected Framework	6
3	Architectuur kaders	8
3.1	Uitgangsdocumenten	8
4	Business architectuur	9
4.1	Data & Analytics processen	9
4.2	Data & Analytics organisatie	10
4.3	Business architectuur principes	11
5	Informatie architectuur	13
5.1	Schematisch overzicht (IST)	13
5.2	Informatie architectuur principes	14
6	Applicatie architectuur	18
6.1	Data & Analytics landschap (IST)	18
6.2	Data & Analytics landschap (SOLL)	19
6.3	Applicatie architectuur principes	22
7	Technische architectuur	25
7.1	Technische architectuur componenten (IST)	25
7.2	Tool stack (IST)	26
7.3	Technische architectuur componenten (SOLL)	27
7.4	Tool stack (SOLL)	27
7.5	Technische architectuur principes	28
8	Informatiebeveiliging en Privacy	31
8.1	Normenkaders voor informatiebeveiliging	31
8.1.1	Voorschrift Informatiebeveiliging Rijksdienst (VIR)	31
8.1.2	Baseline Informatiebeveiliging Overheid (BIO)	31
8.1.3	Algemene verordening gegevensbescherming (AVG)	32
8.1.4	Forum Standaardisatie	32
8.1.5	NEN 7510-7513	32
8.2	Informatiebeveiliging principes	33
8.3	Logging & monitoring	33

1 Inleiding

Voor u ligt de “Project Start Architectuur Data & Analytics” (PSA) van het Centrum Indicatiestelling Zorg (CIZ). De PSA geeft een beeld van het bestaande Datawarehouse (DWH), Business Intelligence (BI), informatiebronnen en applicaties (IST situatie) maar ook de gewenste situatie (SOLL situatie) van het CIZ m.b.t. de nieuwe Data & Analytics architectuur. Als uitgangspunt voor het vastleggen van de architectuur is gebruik gemaakt van de bestaande documenten (zie 3.1) en huidige DWH/BI inrichting.

Het CIZ wordt geconfronteerd met een groot aantal ontwikkelingen dat van invloed is op haar informatievoorziening. Denk hierbij aan nieuwe architectuur en applicatie landschap voor de primaire processen. Deze ontwikkelingen voor het CIZ leiden tot een wijziging in de huidige DWH en BI architectuur.

Het bestaande DWH moet in zijn geheel worden vervangen door een Data & Analytics architectuur op basis van nieuwe architectuur. De technologie stack inclusief applicaties en tools moeten het CIZ een toekomstbestendig Data & Analytics platform bieden die solide gebouwd is en vanuit die basis flexibel is om mee te bewegen met de behoefte uit de business en de functionele vraag kan vertalen naar echte businesswaarde.

Het CIZ wil beschikken over een nieuwe Data & Analytics architectuur met de volgende kenmerken:

- De nieuwe Data & Analytics architectuur wordt in Public Cloud gerealiseerd en geïmplementeerd.
- De nieuwe Data & Analytics architectuur wordt ontworpen en gerealiseerd op basis van Platform as a Service (PaaS) componenten.
- Het nieuwe Data & Analytics platform wordt ingericht op Microsoft Azure Cloud omgeving.
- De As-Is aanpak en/of Lift en Shift strategie zijn niet van toepassing. Het CIZ wil samen met de leverancier bepalen welk(e) component(en) van het huidige DWH/BI landschap hergebruikt kunnen worden voor het nieuwe Data & Analytics platform.

Dit document beschrijft de Project Start Architectuur wat als basis dient voor het ontwerp en implementatie van een nieuw Data & Analytics architectuur binnen het CIZ. Na dit inleidende hoofdstuk wordt in hoofdstuk 2 en 3 ingegaan op de architectuur referenties en kaders. Vervolgens wordt in hoofdstuk 4 en 5 uitleg gegeven over de Business en Informatie architectuur. Hoofdstuk 5 beschrijft de huidige applicatie architectuur (IST) die momenteel binnen het CIZ gebruikt wordt en de toekomstige applicatie architectuur (SOLL) gebaseerd op oplossingsrichting van het CIZ. Tot slot treft u in hoofdstuk 6 het technische architectuurlandschap.

2 Referentiearchitecturen

Het CIZ maakt deel uit van de rijksoverheid c.q. de rijksdienst en tevens van de zorgketen, waarbinnen publieke en private partijen samenwerken om de uitvoering van de zorg conform de daarvoor geldende wetgeving uit te voeren. Het aansluiten bij gemeenschappelijke standaarden en voorzieningen binnen de overheid en de zorgketen vormt dan ook één van de doelstellingen van de IV-strategie van het CIZ. Dit betekent dat het CIZ zich conformeert aan de referentiearchitecturen en de daaraan gerelateerde technische standaarden die voor deze sectoren beschikbaar zijn.

2.1 Nederlandse Overheid Referentie Architectuur

De Nederlandse Overheid Referentie Architectuur (NORA) bevat kaders en afspraken voor het inrichten van de informatiehuishouding van de Nederlandse overheid. NORA omvat principes, standaarden, bouwstenen en een begrippenkader.

De kern van de NORA is een set van overheidsbrede afspraken, die gericht zijn op het mogelijk maken en verbeteren van digitale dienstverlening. De afspraken zijn bindend voor alle overheidsorganisaties onder het regime van Pas toe of Leg uit. Er zijn twee soorten bindende afspraken: basisprincipes en afgeleide Principes. De 10 basisprincipes zijn stellingen over de overheid en de dienstverlening die je eigenlijk in alle gevallen moet kunnen onderschrijven. Het zijn tien waarden, waar je in elke nieuwe dienst en in elke doorontwikkeling aan moet werken om goede dienstverlening te kunnen leveren.

De afgeleide principes van de NORA maken de basisprincipes concreet: wat is er bijvoorbeeld nodig om diensten en informatie vindbaar te maken? Het zijn als het ware de normen die je helpen om de waarden te realiseren in je project. Samen vormen ze een checklist van kwaliteitskenmerken die je kunt gebruiken om je dienst te verbeteren.

2.2 Enterprise Architectuur Rijksdienst

De Enterprise Architectuur Rijksdienst (EAR) biedt een samenhangende beschrijving van de organisatie en de inrichting van de informatiediensten en voorzieningen van de rijksdienst, met als belangrijkste doel het verbeteren van de samenwerking tussen de delen van de rijksdienst. EAR richt zich daarom enerzijds op de interoperabiliteit van de dienstverlening. Hiertoe worden de beginselen uit NORA nader gespecificeerd en gedetailleerd. Anderzijds richt EAR zich op een uniforme beschrijving van de inrichting van organisatie en informatievoorziening.

De EAR is gebaseerd op een indeling in domeinen. Door architectuur te ontwikkelen vanuit logische domeinen wordt EAR verdeeld in behapbare compartimenten. De rijksdienst als geheel is ook te beschouwen als een afgebakend gebied en dus een domein met subdomeinen. De EAR zelf is dus de overkoepelende domeinarchitectuur.

2.3 CIZ architectuurprincipes

Architectuurprincipes zijn richtlijnen ten aanzien van het inrichten en onderhouden van de informatievoorziening en de informatiesystemen van het CIZ. Vanuit de verschillende externe referentiearchitecturen zoals NORA worden al een groot aantal architectuurprincipes aangereikt. In toevoeging daarop hanteert het CIZ een aantal eigen architectuurprincipes die specifiek zijn voor de omstandigheden en behoeften van het CIZ. Hierbij kan onderscheid worden gemaakt tussen enerzijds basisprincipes (of algemene principes), die generiek van toepassing zijn op de integrale informatievoorziening, en anderzijds domeinprincipes (of afgeleide principes), die geldig zijn voor specifieke onderdelen (domeinen) daarbinnen.

Principe	Toelichting
CIZ-BP01	Het CIZ kiest voor Werken met Architectuur.
CIZ-BP02	Het principe Comply-or-Explain is onverkort op alle afwijkingen van toepassing.
CIZ-BP03	Het CIZ volgt architectuur standaarden.
CIZ-BP04	De inrichting van processen en systemen voldoet aan relevante Europese en Nederlandse wet- en regelgeving.
CIZ-BP05	De inrichting van processen en systemen binnen het CIZ houdt rekening met de flexibiliteit en wendbaarheid die de IV-strategie van het CIZ, alsmede de buitenwereld van het CIZ vraagt.
CIZ-BP06	De inrichting van processen en systemen binnen het CIZ houdt er rekening mee dat wij een maatschappelijke functie hebben die wordt uitgevoerd met gemeenschapsgeld.
CIZ-BP07	Het CIZ streeft naar vermindering van de complexiteit van de processen en IV-ICT omgeving, met behoud van betrouwbaarheid, integriteit en vertrouwelijkheid.
CIZ-BP08	Generieke diensten/systemen, die gebruikt kunnen worden voor de gehele organisatie, hebben de voorkeur boven specifieke oplossingen voor slechts een deel van de organisatie.

Onderstaande tabel is een weergave van de architectuur referenties binnen het CIZ architectuurlandschap.

Referentie Architectuur	Niveau
<i>NORA: Nederlandse Overheid Referentie Architectuur</i> De NORA is voortgekomen uit kabinetsbeleid waar veel aandacht was voor verbetering van de dienstverlening (IV-ICT) en de vermindering van de regeldruk voor burgers en bedrijven.	Overheid
<i>EAR: Enterprise Architectuur Rijksdienst</i> De Enterprise Architectuur Rijksdienst (EAR) biedt een samenhangende beschrijving van de organisatie en de inrichting van de informatiediensten en voorzieningen van de rijksdienst, met als belangrijkste doel het verbeteren van de samenwerking tussen de delen van de rijksdienst.	Rijksoverheid

2.4 ISO-25010

Het doel van ISO-25010 is het ondersteunen van de ontwikkeling en verwerving van softwareproducten door hulp te bieden bij de specificatie en evaluatie van kwaliteitseisen. ISO-25010 bestaat uit een tweetal submodellen: Productkwaliteit en Kwaliteit tijdens gebruik. Bij het verzamelen, definiëren en vaststellen van de set van Functional Requirements en Non-Functional Requirements wordt gebruik gemaakt van deze norm.

2.5 Microsoft Cloud Adoption Framework

Het Microsoft Cloud Adoption Framework voor Azure is een volledig levenscyclusframework waarmee Cloud architecten, IT-professionals hun doelstellingen voor Cloud implementatie kunnen bereiken. Het biedt best practices, documentatie en hulpprogramma's waarmee CIZ technologiestrategieën voor de Cloud kunt maken en implementeren. Het Cloud Adoption Framework brengt best practices voor Cloud implementatie samen van Microsoft werknemers, partners en leveranciers. Het framework biedt hulpmiddelen en richtlijnen.

2.6 Microsoft Azure Well-Architected Framework

Het Azure Well-Architected Framework is een raamwerk in de vorm van een set leidende grondbeginselen. Het framework helpt om de kwaliteit van workloads te verbeteren, waardoor de flexibiliteit en schaalbaarheid van Azure Cloudarchitectuur naar een hoger niveau tilt. Het framework bestaat uit vijf pijlers van uitstekende architectuur:

- **Betrouwbaarheid:** Het vermogen van een systeem om te herstellen van fouten en te kunnen blijven functioneren.
- **Beveiliging:** Toepassingen en gegevens beveiligen tegen bedreigingen.
- **Kostenoptimalisatie:** Kosten beheren om de geleverde waarde te maximaliseren.
- **Operationele topprestaties:** Operationele processen die ervoor zorgen dat een systeem blijft werken.
- **Prestatie-efficiëntie:** Het vermogen van een systeem om zich aan te passen aan wijzigingen in de belasting.

3 Architectuur kaders

Het CIZ hanteert voor de inrichting van haar informatievoorziening een werkwijze waarbij de planning en uitvoering van vernieuwingen plaatsvinden onder architectuur. Hierbij worden kaders en richtlijnen gehanteerd die moeten borgen dat de genoemde vernieuwingen passen binnen de algehele structuur en samenhang van de CIZ informatievoorziening en die bijdragen aan de ontwikkeling daarvan.

De architectuur kaders en principes voor de CIZ informatievoorziening (IV) worden voor een belangrijk deel extern aangereikt vanuit de specifieke positie en taakstelling van het CIZ als publieke uitvoeringsorganisatie met de primaire rol van indicatiesteller in het kader van de Wet Langdurige Zorg, Wet zorg en dwang en Besluit uitvoering kinderbijslag. Het gaat dan om de toepasselijke wet- en regelgeving alsmede de verschillende relevante normen, richtlijnen, afspraken en generieke voorzieningen binnen de (rijks)overheid en/of binnen de zorgsector.

De architectuur kaders en principes voor de CIZ informatievoorziening kunnen worden gehanteerd als stuurinstrument bij het formuleren en beoordelen van wijzigings- en projectvoorstellen en van systeemontwerpen op impact, risico, haalbaarheid en toekomstvastheid. Daarnaast vormen ze een belangrijk instrument bij de uitvoering van projecten. Voor elk project moet daarom een Project Start Architectuur worden opgesteld. Hierin wordt bij aanvang van een project aangegeven in hoeverre wordt voldaan aan de Architectuur Kaders en Richtlijnen alsmede welke aanvullende project-specifieke ontwerpkeuzen worden gemaakt.

In deze PSA wordt ingegaan op de volgende architectuurlagen. Deze architectuurlagen en genoemde principes worden tijdens het inrichten van Data & Analytics platform verder geconcretiseerd en in detail uitgewerkt:

- Business architectuur
- Informatie architectuur
- Applicatie architectuur
- Technische architectuur

Per architectuur laag worden de verschillende componenten/onderdelen toegelicht. Daarnaast worden per architectuur laag principes beschreven.

3.1 Uitgangsdocumenten

Voor deze PSA zijn de volgende referentiekaders en documenten als basis of vertrekpunt gebruikt:

- De stip op de Horizon van het CIZ
- Visie op Data CIZ, v1.2
- Cloudbeleid CIZ, v1.3
- Nota Scenario's DWH architectuur en omgeving, v1.2
- Architectuur Kaders en Richtlijnen voor CIZ Informatievoorziening, v2.0
- iGovernance – Organisatie en besturing van de Informatievoorziening, v0.8
- iStrategie – Doelstellingen van de Informatievoorziening, v0.94
- Informatiebeveiligingsbeleid, v1.4
- Normenkader Niet-financiële informatie, v1.0

4 Business architectuur

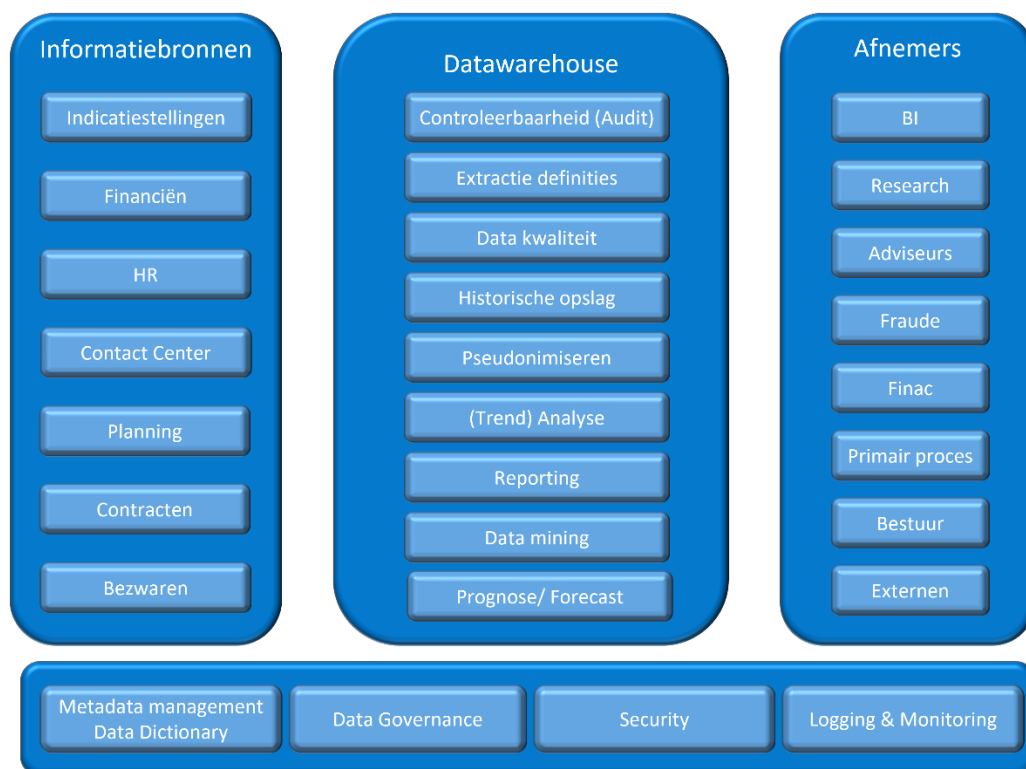
De Business architectuur beschrijft de visie, missie en strategie van het CIZ en de organisatorische contouren die een rol spelen bij de realisatie van de businessdoelen. Deze organisatorische contouren worden in kaart gebracht door een beschrijving te geven van de geldende Bedrijfsfuncties en Bedrijfsprocessen. Zowel bedrijfsfuncties als de bedrijfsprocessen beschrijven de interne gang van zaken binnen CIZ.

De uitwerking van de bedrijfsfuncties vormt de basis voor de uitwerking van de onderliggende architectuurlagen, namelijk de informatie – applicatie - en technische architectuur.

Het Centrum indicatiestelling zorg (CIZ) is een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Sinds 2015 is het CIZ verantwoordelijk voor de afhandeling van aanvragen voor zorg uit de Wet langdurige zorg (Wlz) en het nemen van besluiten op basis van de Wet zorg en dwang (Wzd) vanaf 2020. De Wzd is samen met de Wet verplichte GGZ de opvolger van de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Bopz). Daarnaast indiceert het CIZ één subsidieregelingen onder de Wlz, de Subsidieregeling ADL-assistentie. Ook heeft het CIZ een adviestaak in het kader van het Besluit uitvoering kinderbijslag (Buk), met als opdrachtgever het ministerie van Sociale Zaken en Werkgelegenheid (SZW). Het CIZ was in 2020 verantwoordelijk voor de afhandeling van circa 196.000 aanvragen voor de Wlz, de Wzd, de subsidieregelingen Wlz en Buk advies.

4.1 Data & Analytics processen

Onderstaand figuur geeft een beeld van de processen en diensten die opgenomen kunnen worden binnen het Data & Analytics domein (SOLL) dan wel randvoorwaardelijk zijn. De processen en diensten zijn geïdentificeerd binnen het CIZ.



De belangrijke aspecten en kenmerken zijn hieronder verder toegelicht:

- **Controleerbaarheid:** Om aan de externe verplichtingen (wetgeving) te kunnen voldoen dient elk informatie item en elke rij gecontroleerd te worden op volledigheid en correctheid.
- **Historische opslag:** Om de verschillende wijzigingen op de informatie items correct te verwerken dient historische opslag aanwezig te zijn. Het data platform (zie 6.2) van het primaire proces biedt de mogelijkheid voor historische opslag. Data & Analytics volgt historische opslag van de bron.
- **Pseudonimiseren:** Met pseudonimiseren worden persoonsgegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. Om dit te doen worden de direct identificeerbare elementen van een persoonsgegeven weggehaald.
- **Data Kwaliteit:** Data Kwaliteit dient continue gemonitord te worden om zo een uitspraak te kunnen doen over de kwaliteitsprocessen bij de informatiebronnen. De verantwoordelijkheid van data kwaliteit ligt altijd bij informatiebronnen. Data kwaliteit moet tevens gemonitord worden voor de afnemers.
- **Data dictionary en Metadata management:** Met behulp van Data dictionary wordt éénduidige definities binnen het CIZ gehanteerd.
- **Data Governance:** Geeft inzicht in de herkomst van en bewerkingen op de informatie van informatiebronnen tot afnemer.
- **Afnemers:** Business Intelligence en Research team (BI&R), adviseurs binnen het CIZ, Fraude (Bijzonder onderzoek afdeling), Financiële afdeling (FINAC), gebruikers binnen het primaire proces en bestuur, externe organisaties (ontvangen slechts rapportages).

4.2 Data & Analytics organisatie

De verantwoordelijkheid voor, en de uitvoering van de informatievoorziening (IV) regietaken zijn binnen het CIZ belegd bij de CIO en de CIO Office. Het betreft hier enerzijds regie op de vraag die vanuit de business wordt gesteld omtrent de levering van ICT-diensten (vraagverheldering en bundeling). Anderzijds betreft het de aansturing van de levering van diensten door ICT- en Applicatie-dienstverleners. De daarvoor benodigde IV-regiefunctie moet dus passen binnen de algehele organisatiestructuur van het CIZ.

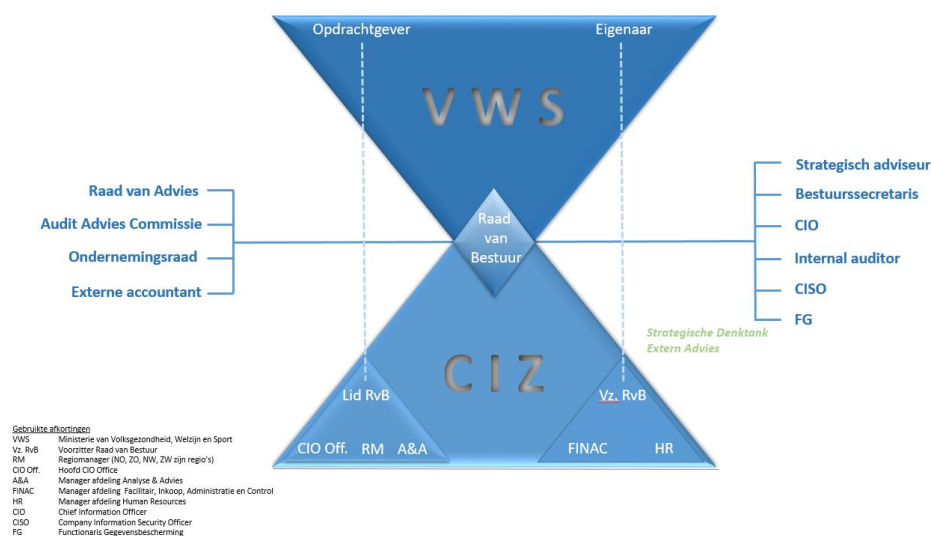
Conform het gehanteerde IV-besturingsmodel bestaat er een duidelijke verantwoordelijkheidsverdeling tussen de IV-gebruikers binnen de CIZ organisatie enerzijds ("de business") en IV-regiefunctie die onder verantwoordelijkheid valt van de CIO (de CIO Office) anderzijds. De "business" moet aangeven wat zij nodig heeft aan informatievoorziening om de taken en bedrijfsprocessen effectief te kunnen uitvoeren en motiveren waarom. Zij is dus verantwoordelijk voor het formuleren van de (functionele) eisen, behoeften en randvoorwaarden aan de IV-ondersteuning. De IV-regiefunctie bepaalt in samenspraak met de externe ICT dienstenaanbieders hoe de informatievoorziening wordt ingericht in termen van IV-applicaties en diensten (en laat de specifieke technische inrichting daarbij zoveel mogelijk over aan de ICT dienstenaanbieders). Uiteraard voert de CIO de regie over het totale Applicatie landschap.

BI & Research

Het team BI en Research hierna (BI & R) is er verantwoordelijk voor dat de verschillende operationele stuur- en verantwoordingsrapportages aansluiten bij de behoefte van de organisatie waaronder management en bestuur en externe klanten. Er wordt proactief meegewerkt aan analyses die het indicatieproces (onze kernactiviteit) verbeteren en meer inzichten bieden in de werking van het Wlz-stelsel. Er wordt in toenemende mate Intelligentie aan de systemen toegevoegd. Hierdoor wordt het systeem lerend en ondersteunend aan het vakmanschap van onze medewerkers tijdens het indicatieproces (machine learning). Ook innovatie is een belangrijk thema. Het team draagt hieraan bij onder andere middels het CIZ Datalab.

Het team BI & R samen met de externe leverancier is binnen het CIZ verantwoordelijk voor de dataverzameling, analyse en rapportages voor verantwoording intern en extern, datavoorziening naar verschillende partijen en rapportages ter ondersteuning van de sturing intern in het CIZ. De afdeling bestaat uit ruim 25 medewerkers (in- en extern). Een externe leverancier zorgt voor ontwikkeling, beheer en onderhoud van het Datawarehouse (huidige situatie) in nauwe samenwerking met interne medewerkers.

Het team BI&R is onderdeel van de afdeling Analyse en Advies (A&A). Deze afdeling ondersteunt het CIZ als slimme, deskundige en lerende organisatie. Het team BI&R richt zich op beheer/onderhoud, change en op data-exploratie/onderzoek.



4.3 Business architectuur principes

De belangrijke principes voor de Business Architectuur (BA) binnen Data & Analytics worden in deze paragraaf geschreven. Deze principes zijn samengesteld uit de uitgangsdOCUMENTEN genoemd in hoofdstuk 3.

BA01	
Principe	Eenduidige verantwoordelijkheid: CIZ hanteert een heldere en eenduidige verantwoordelijkheid en zijn daarop aanspreekbaar.
Motivatie	De verantwoordelijkheden tussen CIO team, BI&R team en leveranciers worden eenduidig gehanteerd. Het moet duidelijk zijn wie aansprakelijk is voor welke diensten en producten, zodat CIZ medewerkers en management duidelijkheid hebben wie zij kunnen aanpreken over de dienstverlening. Met name demarcatie van de verantwoordelijkheden tussen de leverancier van de Data & Analytics dienstverlening en de interne medewerkers van het BI&R team. De escalatie lijnen dienen ook duidelijk te zijn.

BA02	
Principe	Verantwoord gebruik: We dragen zorg voor de bescherming van persoonsgegevens.
Motivatie	Bescherming van persoonsgegevens en het vertrouwen daarin is essentieel voor een goede werking binnen het CIZ. Een verantwoord gebruik in de geest van wet- en regelgeving voor gegevensbescherming is dan ook noodzakelijk. Dit betekent dat maatregelen voor gegevensbescherming proactief worden geïmplementeerd, niet

	reactief. In het ontwerp van een Data & Analytics architectuur moet uitdrukkelijk de maatregelen voor gegevensbescherming worden benoemd en goedgekeurd door de Privacy officer.
--	--

BA03	
Principe	Bruikbaar en gebruiksvriendelijk: Data & Analytics diensten zijn bruikbaar en gebruiksvriendelijk, en dragen bij aan een goede gebruikservaring.
Motivatie	CIZ medewerkers maken gebruik van de Data & Analytics diensten met een doel voor ogen en willen dat doel op een eenvoudige en gebruikersvriendelijke manier kunnen bereiken. De succesfactoren zijn consistentie, voorspelbaarheid (Forecasting), beschikbaarheid en betrouwbaarheid van gegevens. De tooling om tot het Data & Analytics platform te komen is bruikbaar en gebruiksvriendelijk voor eindgebruikers in rapporten en self service omgevingen. Low-code tooling (bedoeld voor rapporten) voor het BI&R team waarbij de nadruk op configureren ligt en er weinig/geen programmeertaal aan te pas komt.

BA04	
Principe	Transparant in kwaliteit: CIZ is transparant over de kwaliteit van zijn gegevens en diensten.
Motivatie	Gebrek aan gegevenskwaliteit is een van de meest beperkende factoren voor het realiseren van de potentie van gegevens. Er is een duidelijk verband tussen gebruikerservaring en de kwaliteit van gegevens. Kwaliteit van gegevens gaat niet alleen over de inhoud, maar ook over de beschikbaarheid van data via diensten. Informatie over de kwaliteit van gegevens en diensten moeten de gebruiker daarom helpen bij het op waarde schatten van de dienst en het gebruik van de gegevens van de dienst.

BA05	
Principe	Processen hebben een eigenaar: Zonder een duidelijke eigenaar is het niet duidelijk wie zich verantwoordelijk voelt en wie over wijzigingen besluit. Eigenaarschap is belangrijk om de kwaliteit van de procesuitvoering te garanderen.
Motivatie	Processen hebben een eigenaar toegewezen die verantwoordelijk is voor de procesdefinitie en de kwaliteit van de procesuitvoering binnen CIZ en met name het interne proces van Data & Analytics. De eigenaar heeft een duidelijk belang in het proces. Wijzigingen in het proces worden niet aangebracht zonder goedkeuring van de proceseigenaar.

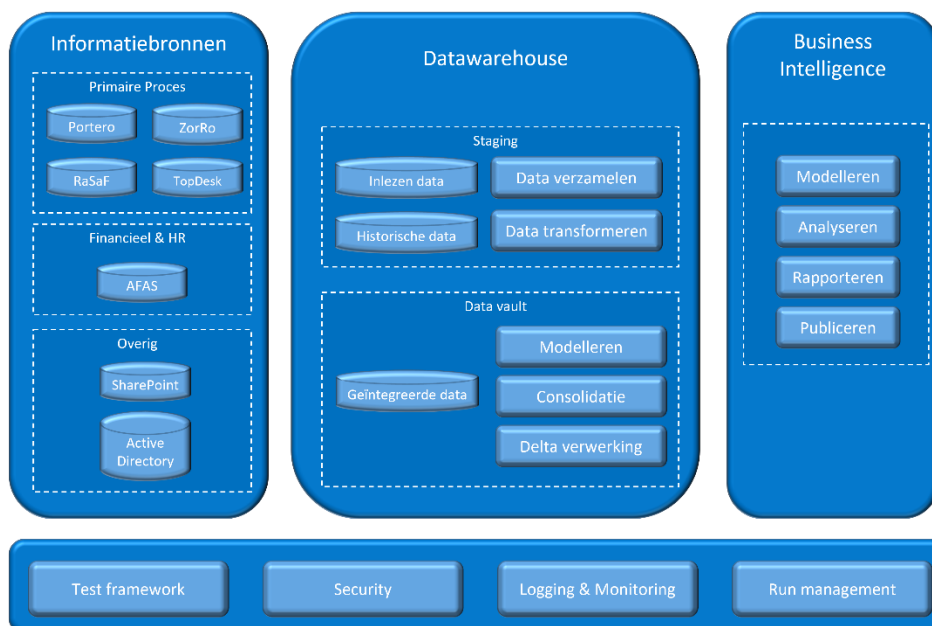
BA06	
Principe	Processen zijn gestandaardiseerd waar mogelijk: Standaard processen zijn herhaalbaar, voorspelbaar, schaalbaar en meer efficiënt. Door iedereen dezelfde standaard processen te laten hanteren wordt maximaal schaal- en synergievoordeel bereikt en kennis over een betere procesuitvoering gedeeld. Voor data science processen kan afgeweken worden.
Motivatie	Er zijn voor alle processen binnen het CIZ standaard procesbeschrijvingen. Voor ieder proces is er een proceseigenaar aangewezen die verantwoordelijk is voor de procesdefinitie en de kwaliteit van de procesuitvoering. Standaard processen worden geïmplementeerd bij alle bij het proces betrokken afdelingen.

5 Informatie architectuur

Volgens TOGAF (The Open Group Architecture Framework) bestaat de informatiearchitectuur uit een data-architectuur (met name gericht op de informatiemodellen) en de applicatiearchitectuur (de functies die de informatie bewerken). De applicatiearchitectuur wordt behandeld in het volgende hoofdstuk. De data-architectuur bevat op hoofdlijnen een overzicht van gegevensstromen van en naar DWH omgeving en Data & Analytics platform moet passen binnen de data-architectuur. Er wordt tevens een overzicht van de functionaliteiten van het Datawarehouse beschreven.

5.1 Schematisch overzicht (IST)

In onderstaand figuur zijn de belangrijkste informatiebronnen, kernfuncties van datawarehouse en Business Intelligence voor de huidige Datawarehouse architectuur weergegeven. Onder het figuur is een beschrijving van de kenmerken en informatiebronnen opgenomen.



De functionaliteit per component zijn hieronder verder toegelicht:

Portero: is de centrale applicatie voor de ondersteuning van de primaire processen van het CIZ. Het kan worden getypeerd als een zaakstelsel dat zorgt voor het volgen van de voor de belangrijkste CIZ taken gedefinieerde werkstromen en de bijbehorende informatievastlegging en dossiervorming.

ZorRo: is een maatwerkapplicatie voor de ondersteuning van de inzetplanning van medewerkers in het primaire proces en het vastleggen en raadplegen van afspraken voor huisbezoeken en/of gesprekken met cliënten. Afspraken kunnen zowel rechtstreeks in ZorRo worden aangemaakt, als uit Portero geïmporteerd.

RaSaF: De maatwerkapplicatie RaSaF wordt gebruikt voor Contractbeheer en Contactbeheer van externe organisaties (met name zorgaanbieders). Contractbeheer bevat alle activiteiten die samenhangen met het aanvragen, toekennen, beheren en verlengen van contracten met zorgaanbieders, om digitaal aanvragen in te kunnen dienen in Portero. In Contactbeheer wordt vastgelegd welke contactmomenten er zijn geweest met organisaties en over welke onderwerpen. Deze organisaties kunnen wel of geen contract hebben met het CIZ voor het digitaal indienen van aanvragen.

TopDesk (Module Bijzonder Onderzoek): registratie van onderzoeksactiviteiten in kader van fraudebestrijding.

AFAS: Een ERP systeem, waarmee een groot aantal bedrijfsfuncties kunnen worden geautomatiseerde en bestaat uit CRM, Financieel, HRM en Payroll.

Active Directory: Voor de authenticatie en autorisatie van gebruikers binnen de CIZ omgeving.

SharePoint: Locatie van huidige documenten.

Staging: Data wordt in staging deel ingeladen, verzameld en getransformeerd.

Data vault: In data vault wordt data uit diverse informatiebronnen geïntegreerd, geconsolideerd en gemodelleerd.

5.2 Informatie architectuur principes

De belangrijke principes voor de Informatie Architectuur (IA) binnen Data & Analytics worden in deze paragraaf geschreven. Deze principes zijn samengesteld uit de uitgangsdOCUMENTEN genoemd in hoofdstuk 3.

IA01	
Principe	Centraal : CIZ en met name Data & Analytics houden gegevens centraal en maken deze gegevens toegankelijk binnen Data en Analytics domein.
Motivatie	Het uitgangspunt is dat gegevens eenmalig bij de bron worden geregistreerd en bij de bron toegankelijk worden gemaakt. Hoewel aggregatie en publicatie van data binnen Data & Analytics overal kan plaatsvinden vindt CIZ het belangrijk, gedacht vanuit gegevensbescherming dat de bron leidend is. Het data platform van het primaire proces wordt gezien als informatiebron binnen het CIZ architectuurlandschap.

IA02	
Principe	Herbruikbare CIZ-gegevens : CIZ gegevens worden eenmalig geregistreerd bij bron en Data & Analytics en BI borgen herbruikbaarheid voor meervoudig gebruik.
Motivatie	Eenmalige registratie, herbruikbaarheid en meervoudig gebruik van gegevens dient om de last van eindgebruikers te verminderen, in de eerste plaats voor de cliënten en zorgaanbieders. Ze leggen alleen gegevens vast die nodig zijn, vanuit het perspectief van CIZ primaire processen (WLZ, WZD, etc.). Meervoudig gebruik van gegevens moet ook tot lagere kosten leiden, tot administratieve lastenverlichting en tot gebruik voor onderzoek door researchers. De basis hiervoor is dat gegevens vindbaar, toegankelijk en uitwisselbaar zijn. De gegevens wordt van het data platform van het primaire proces samen met andere gegevens van informatiebronnen naar een verzamelbak gebracht.

IA03	
Principe	Regie over gegevens : CIZ stelt de interne afdelingen in staat om controle en regie te nemen over hun gegevens.
Motivatie	Data & Analytics team kunnen de gegevens van het primaire proces, financieel en HR verzamelen en delen, ook bijvoorbeeld t.b.v. onderzoek. De gegevens mogen alleen verzameld en gedeeld worden binnen de context van een doel (doelbinding).

IA04	
------	--

Principe	Open waar het kan, besloten waar het moet: CIZ-gegevens binnen CIZ domein zijn open waar het kan en besloten, geauthentiseerd, geautoriseerd en gepseudonimiseerd, waar het moet.
Motivatie	Hergebruik van gegevens kan alleen plaatsvinden als gegevens toegankelijk zijn. Hierbij is hergebruik voor andere doeleinden dan waarvoor de gegevens zijn vastgelegd ook van belang, bijvoorbeeld voor onderzoek. Door binnen de wettelijke kaders (lees AVG kaders) toegang te verschaffen tot gegevens kunnen deze hergebruikt worden voor andere doeleinden dan waarvoor ze zijn vastgelegd. Het gebruiken van gelogde informatie (logging en monitoring) wordt ingericht om de digitale veiligheid van het CIZ en de privacy van de cliënten te waarborgen.

IA05	
Principe	Een gemeenschappelijk CIZ data dictionary: CIZ gegevens zijn uitwisselbaar met een gemeenschappelijk data dictionary zodat we binnen CIZ elkaar kunnen begrijpen.
Motivatie	Gegevens uitwisselbaar maken betekent dat partijen met elkaar moeten kunnen praten, elkaar moeten kunnen begrijpen. Binnen CIZ en met name voor primaire proces applicaties en datawarehouse moet een gemeenschappelijk data dictionary aangemaakt worden, waarin betekenis van een onderwerp eenduidig is gedefinieerd, maar waar ook relaties tussen onderwerpen eenduidig kunnen worden gedefinieerd. Het doel is om elkaar te begrijpen, om verschillen te kunnen overbruggen.

IA06	
Principe	Zo weinig mogelijk, zo veel als nodig: CIZ minimaliseert de hoeveelheid gegevens die zij registreert en uitwisselt, zowel vanuit gegevensbescherming als vanuit efficiëntie en effectiviteit.
Motivatie	Het registreren en uitwisselen van grote hoeveelheden data heeft een effect op de privacy van een persoon, het verhoogt de risico's voor gegevensbescherming en extra kosten vooral in Cloud omgeving qua opslag. Daarnaast zorgt een grote hoeveelheid data ook voor een hogere belasting van de infrastructuur, maar ook voor een hogere belasting van degene die de data moet vastleggen (registratielast) en degene die de data ontvangt en moet verwerken (mogelijke overbelasting). Vanuit het belang van doelbinding, gegevensbescherming, efficiency, kostenbesparing en doelmatigheid wordt daarom gekozen voor minimalisatie van de hoeveelheid gegevens. Afhankelijk van het doel van de uitwisseling wordt bepaald wat echt nodig is.

IA07	
Principe	De gegevensverzameling is een geïntegreerd geheel: Voor alle gegevens worden dezelfde principes gehanteerd, er wordt geen onderscheid gemaakt tussen gegevenstypen m.b.t. principes.
Motivatie	Door de gescheiden domeinen binnen het CIZ (primaire proces, bedrijfsvoering, financieel, HR, etc..) aan te houden, zijn losstaande eilanden in het gegevensbeheer ontstaan. Door de gegevenshuishouding als een geheel te beschouwen, kan het volle potentieel worden benut. Het gaat hierbij vooral om een integrale beschouwing van de gegevens en het hanteren van dezelfde uitgangspunten en eisen aan gegevens. Of er sprake is van technische integratie hangt vooral af van de afweging van behoefte ten opzichte van de kosten en inspanningen.

IA08	
Principe	Online gegevensuitwisseling: Voor gegevensuitwisseling worden online koppelingen gerealiseerd tussen Data & Analytics en informatiebronnen.
Motivatie	Gebruikers verwachten de meest recente gegevens in veel van hun werkprocessen. Besluiten die worden gemaakt op basis van verouderde gegevens en door fouten van

	traditionele batch proces/aanpak hebben een lagere betrouwbaarheid en kunnen tot fouten of inconsistenties leiden.
--	--

IA09	
Principe	Een bron per gegevenstype: Voor alle gegevenstypen binnen Data & Analytics is er één bron die leidend is. In de bron heeft gestructureerde opslag de voorkeur boven niet-gestructureerde opslag. De bron is geëigend voor het type gegevens.
Motivatie	Het hanteren van bronnen voor breed gebruikte kerngegevens leidt tot een hogere consistentie in de gegevensverzameling, verminderen van ongewenste redundantie en optimaliseert meervoudig gebruik van gegevens. Bijvoorbeeld, AFAS is de bron voor de CIZ medewerkersgegevens en niet de geregistreerde medewerkersgegevens in primaire applicatie.

IA10	
Principe	Informatie over gegevens: Gegevens, documenten, bestanden en berichten worden voorzien van metadata. Metadata wordt geregistreerd op het moment dat gegevens worden ontvangen of gewijzigd, bij voorkeur geschiedt dit automatisch.
Motivatie	Metadata bevorderen de vindbaarheid (ontsluiting), geven informatie voor beheerdoeleinden en duurzame bewaring en over de kwaliteit en bruikbaarheid. Metadata management kan verschillende vormen aannemen. Idealiter, bevat metadata architectuur zowel business (business terminologie en definities) als technische (tabellen, kolommen en transformaties) metadata die onderling met elkaar gerelateerd zijn. De business metadata wordt beschikbaar gesteld aan eindgebruikers, die deze informatie kunnen gebruiken om correcte beslissingen te maken gebaseerd op de informatie aanwezig in Data & Analytics; de technische metadata is beschikbaar voor Data & Analytics medewerkers, zodanig dat zij er voor kunnen zorgen dat alle technische definities steeds in sync zijn.

IA11	
Principe	Heldere eisen t.a.v. gegevenskwaliteit: Eisen ten aanzien van de gegevenskwaliteit binnen Data & Analytics voor informatiebronnen worden helder geformuleerd. Gegevens voldoen aan de vereiste kwaliteitseisen, meer en niet minder.
Motivatie	De kwaliteit van de gegevensverzameling wordt afgestemd tussen gegevenseigenaren van informatiebronnen en Data & Analytics.

IA12	
Principe	Traceerbaarheid naar bron: Gegevens in het Data & Analytics zijn herleidbaar naar de originele gegevensbronnen.
Motivatie	Het is belangrijk dat inzichtelijk kan worden gemaakt dat gegevens die gebruikt zijn binnen Data & Analytics herleidbaar zijn naar de originele informatiebronnen. Hierdoor kunnen er geen twijfels ontstaan over de kwaliteit van de gegevens. Daarnaast is het ook vanuit wet- en regelgeving belangrijk om aan te kunnen geven waarop bijvoorbeeld verantwoordingsrapportages zijn gebaseerd.

IA13	
Principe	Standaard definitie en formaat: Gegevens hanteren een standaard definitie en zijn beschikbaar in een gestandaardiseerd formaat.
Motivatie	Om gegevens goed te kunnen uitwisselen is het belangrijk dat het helder is wat hun structuur en definitie is. Door deze definities te standaardiseren wordt een uniforme interpretatie mogelijk en wordt afhankelijkheid van specifieke applicaties of leveranciers voorkomen. Daarbij is ook de vorm (formaat) relevant, omdat anders

	gegevens mogelijk nog steeds niet toegankelijk zijn. Een standaard definitie en formaat maakt zowel integratie tussen applicaties als migraties naar (nieuwe versies van) applicaties veel eenvoudiger.
--	---

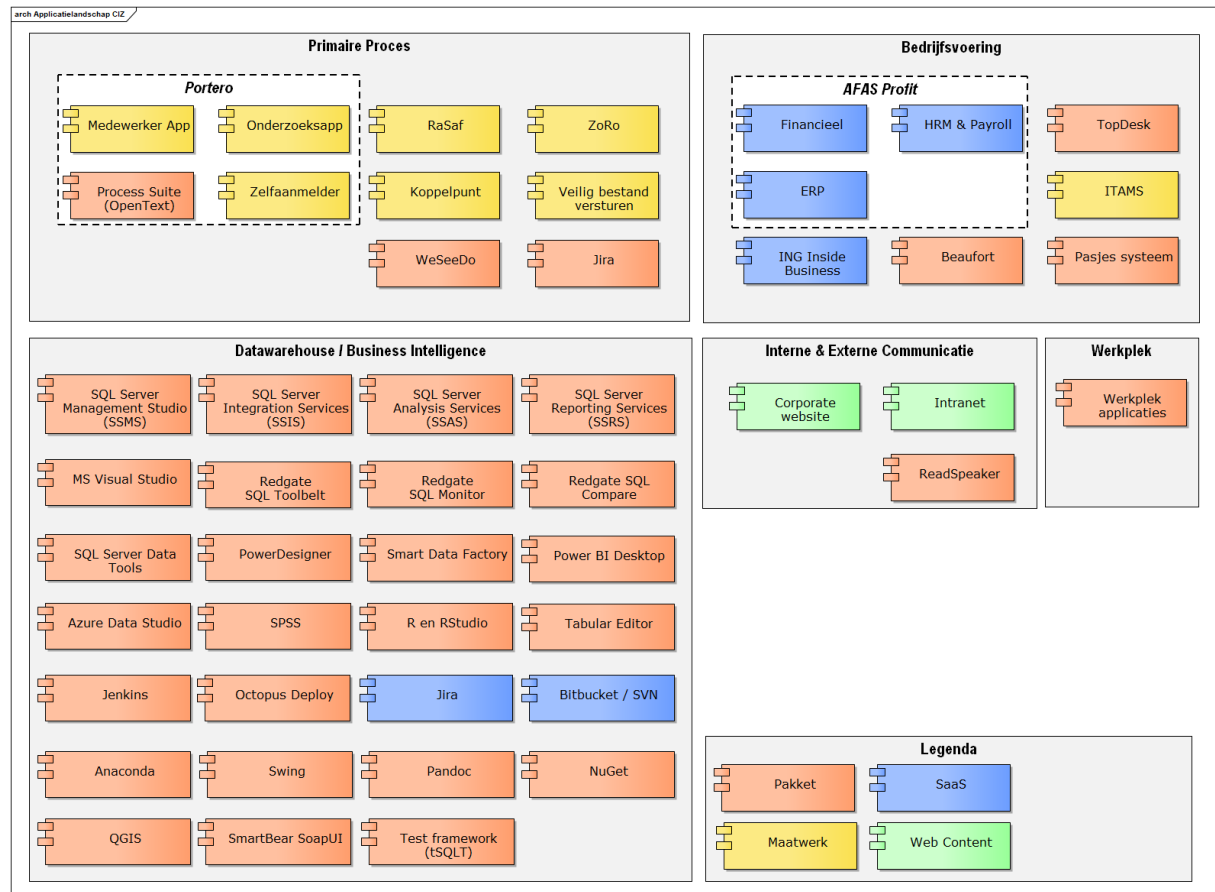
IA14	
Principe	Documenten in DMS: Documenten worden opgeslagen in Document Management Systeem.
Motivatie	Dit zorgt ervoor dat documenten eenvoudig kunnen worden teruggevonden en gedeeld tussen medewerkers. Elektronische opslag van documenten voorkomt transport en verwerking van fysieke documenten vooral binnen de Cloud omgeving. Er wordt een koppeling gerealiseerd tussen DMS en Data & Analytics platform.

6 Applicatie architectuur

De applicatie architectuur beschrijft de applicatiecomponenten en informatiesystemen binnen Data & Analytics. Het is een modelmatige beschrijving van het applicatielandschap, de daadwerkelijk in productie zijn de systemen.

6.1 Data & Analytics landschap (IST)

In de volgende tekening is het huidige applicatie landschap (IST) van het CIZ met daarin de applicatiecomponenten en tools die binnen het Data & Analytics op dit moment ten aanzien van de onderkende datawarehouse en BI functionaliteiten inzet (in productie zijn) weergegeven.



De belangrijke aspecten en kenmerken zijn hieronder verder toegelicht:

- SQL Server Management Studio (SSMS): wordt gebruikt om SQL Server database correct te beheren.
- SQL Server Integration Services (SSIS): wordt gebruikt om data te verplaatsen, laden, transformeren en te aggregeren. Alle bewerkingen op de data worden middels deze applicatie uitgevoerd.
- SQL Server Analysis Services (SSAS): geeft de mogelijkheid om snel toegang te krijgen tot grote hoeveelheden data. In SSAS kunnen met Data Tools rapportage modellen worden gemaakt en enig component waarop de kubus(sen) draaien.
- SQL Server Reporting Services (SSRS): met deze tool kunnen rapporten op maat gecreëerd worden met tabellen in de vorm van grafieken, gegevens en afbeeldingen. De rapporten worden ontwikkeld met Visual studio (Data tools) en Power BI desktop voor Power BI rapporten.
- MS Visual Studio: is een grafische code-editor en geïntegreerde development omgeving.

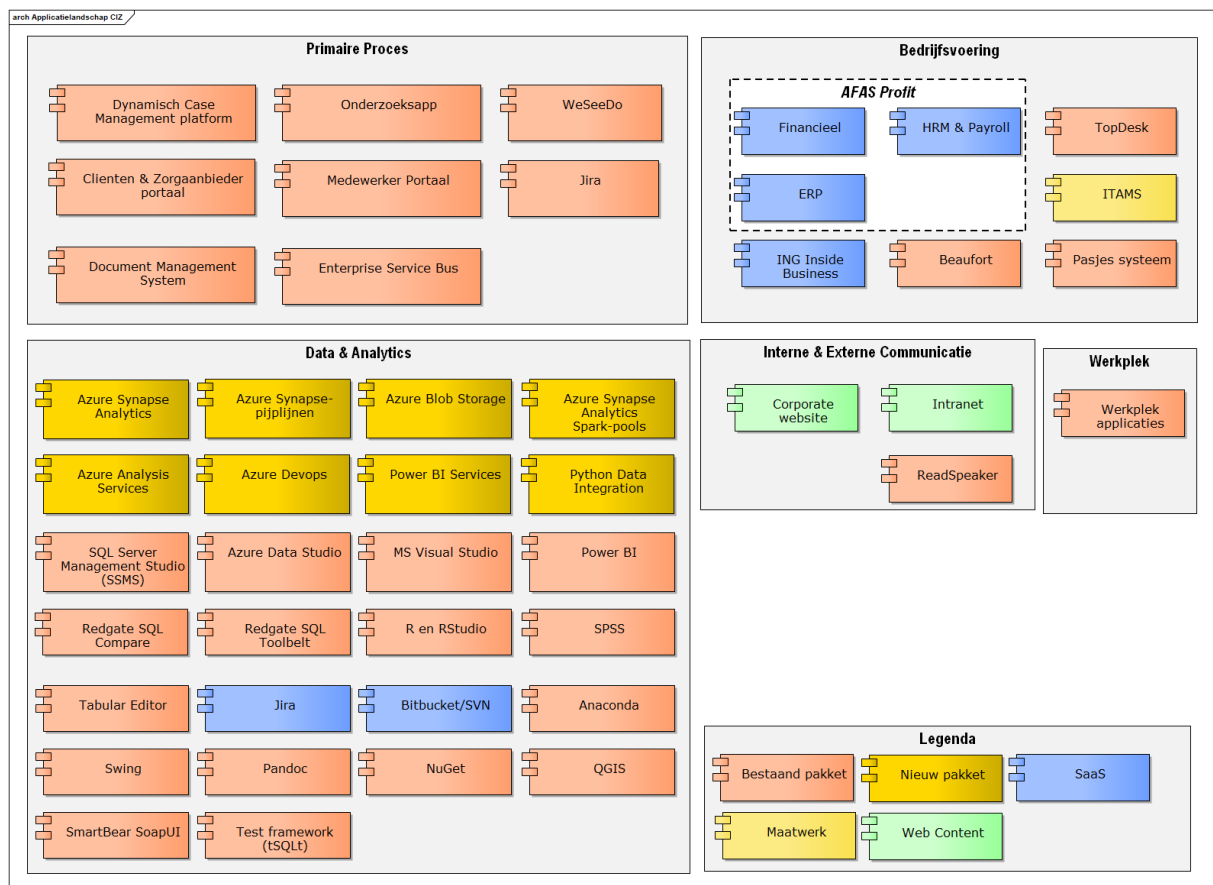
- Redgate SQL Toolbelt: bevat de industriestandaard producten voor de ontwikkeling, implementatie, back-up en monitoring van SQL Server.
- Redgate SQL Monitor: helpt teams die voor SQL-servers zorgen proactief te zijn. Met SQL Monitor kunnen bewakingsomgevingen die zijn aangepast aan de SQL-server van de gebruiker, problemen identificeren voordat ze van invloed zijn op gebruikers.
- Redgate SQL Compare: eenvoudige en gemakkelijke vergelijking van databaseschema's en gegevens.
- SQL Server Data Tools: wordt gebruikt om SQL Server Reporting Services rapporten, SQL Server Analysis Services kubus(sen) en SQL Server Integration Services packages te ontwikkelen, testen en debuggen.
- PowerDesigner: SAP PowerDesigner is een oplossing voor gegevensmodellering en transformatie waarmee ontwikkelaars bedrijfstransformaties kunnen visualiseren.
- Smart Data Factory: is een tool van Axians en op basis van het PowerDesigner model kan met behulp van de Smart Data Factory het model gegenereerd worden naar de gewenste oplossing.
- Power BI Desktop: met Power BI Desktop kan verbinding gemaakt worden met tal van gegevensbronnen en deze in een gegevensmodel combineren en modelleren.
- SPSS en R/R studio: helpt de organisatie bij het verzamelen, invoeren, lezen, bewerken en/of analyseren van gegevens.
- Azure Data Studio: is een Microsoft desктоptool, die kan worden gebruikt om SQL Server databases en Cloud gebaseerde Azure SQL database en Azure SQL Datawarehouse systemen te beheren.
- Tabular Editor: een tool die veelvuldig gebruikt wordt om modellen te ontwikkelen. In tegenstelling tot Visual Studio is deze tool erg gebruiksvriendelijk, makkelijk in gebruik en vooral erg snel. Tabular Editor kan ook worden gebruikt om Power BI Datasets te bewerken.
- Jenkins: is een Continuous Integration platform met name bedoeld voor het herhaaldelijk uitvoeren en monitoren van build-taken; het geautomatiseerd bouwen, testen en implementeren van applicaties.
- Octopus deploy: wordt gebruikt als configuratie en deployment management tool.
- Jira: teams gebruiken Jira voor allerlei doeleinden, van vereisten- en testcasebeheer tot agile softwareontwikkeling.
- Bitbucket/SVN: zijn bedoeld voor code collaboratie en versie beheer. Bitbucket is een tool om code te beveiligen, te bouwen en er samen aan te werken. De tool is geoptimaliseerd voor continuous Delivery en integreert met onder andere Jira.
- Anaconda: is bedoeld voor deployment en pakket management van Python en R programmeertalen.
- Swing: is een Self Service reporting omgeving voor publicatie via de website van het CIZ voor externe belanghebbenden en geïnteresseerden.
- Pandoc: is bedoeld voor omzetten van documenten formaten.
- NuGet: is package manager en bedoeld voor het delen van codes.
- QGIS: is een geografisch informatiesysteem.
- SmartBear SoapUI: is een desktop applicatie en kan gebruikt worden voor het testen, aanroepen, monitoren, simuleren of mocken van webservices.
- tSQLT: is een test framework voor SQL Server unit testing.

6.2 Data & Analytics landschap (SOLL)

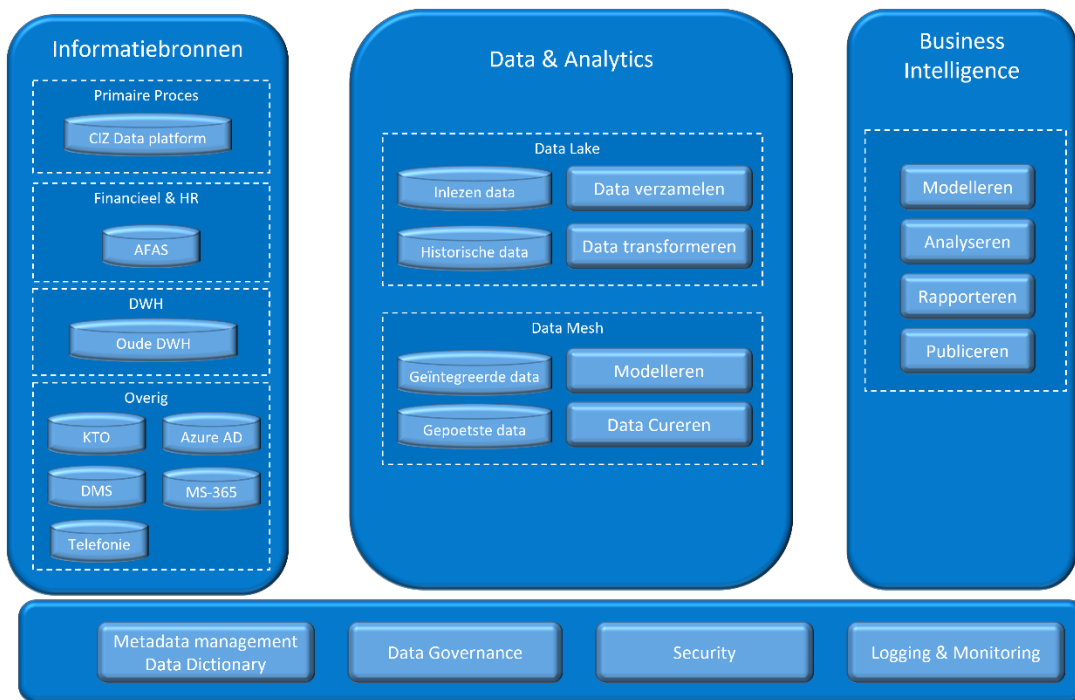
Het transformeren naar een nieuw applicatielandschap dat als een primaire bron dient, heeft een flinke impact op de architectuur van het huidige DWH. De DWH omgeving moet in de basis in staat zijn om nieuwe bronnen toe te voegen. Echter is het huidige DWH voornamelijk opgebouwd als een copy van het huidige applicatielandschap. De informatiemodellen en integratie-laag is redelijk specifiek voor het huidige applicatielandschap. Dit betekent dat een vervanging van het

applicatielandschap tezamen met een mogelijk gedeeltelijke transitie naar de Cloud een flinke impact gaan hebben op de architectuur van het DWH. Het CIZ heeft daarom besloten om gezamenlijk met de transformatie naar een nieuw applicatielandschap ook de DWH omgeving volledig opnieuw op te bouwen naar een Data & Analytics omgeving. Het nieuwe Data & Analytics platform heeft de volgende kenmerken:

- De nieuwe Data & Analytics architectuur wordt in Public Cloud gerealiseerd en geïmplementeerd.
- De nieuwe Data & Analytics architectuur wordt ontworpen en gerealiseerd op basis van Platform as a Service (PaaS) componenten.
- Het nieuwe Data & Analytics platform wordt ingericht op Microsoft Azure Cloud omgeving.



Hierna volgt een schematisch overzicht van onze oplossing. De nieuwe componenten zijn in de volgende paragrafen beschreven.



Hieronder wordt de functionaliteit per component kort beschreven:

CIZ data platform: Het CIZ data platform is een verzamelpunt voor gegevens die het CIZ ontvangt, verzamelt en genereert. Dit verzamelpunt kan worden omschreven als 'het geheugen van het CIZ voor de primaire processen'. Het geheugen heeft als doel opslag en reproductie van CIZ informatie vanuit het primair processysteem (historisch en actueel) en is onafhankelijk van huidige en toekomstige primaire proces applicaties. De gestructureerde data zal worden opgeslagen in terminologie van het CIZ. Kortom, alles wat in het zaakstelsel wordt vastgelegd wordt vertaald naar een CIZ gegevensmodel, opgeslagen op het data platform en in sync gehouden.

AFAS: Een ERP systeem, waarmee een groot aantal bedrijfsfuncties kunnen worden geautomatiseerd en bestaat uit CRM, Financieel, HRM en Payroll.

Oude DWH: In het nieuwe Data & Analytics platform worden de huidige DWH gegevens als informatiebron gebruikt.

KTO: klanttevredenheidonderzoek applicatie. KCM stuurt vragenlijsten uit naar de klanten van het CIZ. De informatie welke hierop terugkomt wordt aan de KCM kant verwerkt. De resultaten van onderzoek worden verder geanalyseerd in Data & Analytics.

Document Management System: Het CIZ werkt aan de digitalisering van haar werkprocessen. Het digitaliseren van het archief is in dit kader één van de belangrijkste ontwikkelingen. Het CIZ wil haar digitaal archief zoveel mogelijk vastleggen en onderhouden. Alle documenten van het zaakdossier worden opgeslagen in een Document Management Systeem (DMS).

MS-365: Microsoft Office-toepassingen zoals Exchange Online, SharePoint Online, cloudopslag en andere samenwerkings- en productiviteitstoepassingen.

Telefonie: Data van telefoongesprekken.

Azure AD: Azure Active Directory is een identiteits- en toegangsbeheerservice in de Cloud. Deze service helpt CIZ medewerkers toegang te krijgen tot interne en externe applicaties.

Data Lake: Hier wordt de data verzameld en bewaard binnen het Data & Analytics platform. Dit is de eerste, en meest eenvoudige stap, in de opbouw van het platform.

Data Mesh: Hier wordt de data omgezet tot bruikbare informatie. Met logica en business rules wordt data gemodelleerd (data verbinden en logica tussen data). Er is CIZ proceskennis nodig om te weten hoe data zich tot elkaar verhoudt en welke modellering wel/geen hout snijdt. Het modelleren en bouwen binnen de Data Mesh gebeurt door de BI ontwikkelaar.

6.3 Applicatie architectuur principes

De belangrijke principes voor de Applicatie Architectuur (AA) binnen Data & Analytics worden in deze paragraaf geschreven. Deze principes zijn samengesteld uit de uitgangsdOCUMENTEN genoemd in hoofdstuk 3.

AA01	
Principe	Scheiding van data en proces: Door in de applicatielaag van informatiebronnen af te bakenen op een scheiding van data en proces wordt afhankelijkheden van verbonden businessprocessen en data voorkomen en een flexibele modulaire opbouw verkregen.
Motivatie	De applicatie architectuur bestaat uit meerdere lagen en typische functionele domeinen die ondersteunend zijn aan één of meerdere bedrijfsfuncties. De minimaal te onderscheiden lagen zijn: • Applicatie processen • Integratie • Data

AA02	
Principe	Bedrijfsregels in informatiebronnen zijn ontkoppeld van processen en systemen: Door regels als (micro)services te beschouwen kunnen deze breder worden toegepast dan alleen in de bijhorende applicatie.
Motivatie	Service oriëntatie vergroot de modulariteit en herbruikbaarheid van het applicatielandschap. Regels kunnen sneller en eenvoudiger worden geïmplementeerd en samenwerking tussen organisaties en organisatieonderdelen wordt vereenvoudigd. Veranderende functionele behoeftes kunnen sneller worden ingevuld, de ondersteuning van de functionele behoefte kan meer op maat worden toegesneden.

AA03	
Principe	Gebruik van standaard applicaties: Functionaliteiten worden ingevuld met op de markt verkrijgbare standaard applicaties. Applicaties en functionaliteiten maken gebruik van open standaarden en standaard gegevensdefinities.
Motivatie	Gebruik van standaard pakketten biedt directe beschikbaarheid van functionaliteit en leidt tot lagere kosten door minder zelf te ontwikkelen en te beheren. Standaard applicaties voorkomen problemen bij upgrades naar nieuwe versies. Voor een aantal standaarden geldt het hanteren van de standaard als een wettelijke plicht, zoals bij de Basisregistraties. Het hanteren van standaard applicaties maakt de organisatie voorspelbaar, zowel intern als naar de buitenwereld. Daarnaast wordt de kennis over functionaliteiten vergroot, de uitwisselbaarheid van services en personeel bevordert en worden single points of failure weggenomen.

AA04	
Principe	Applicaties gekoppeld middels integratielaag: Applicaties worden aan elkaar gekoppeld middels een integratielaag. De integratielaag biedt gestandaardiseerde functionaliteit om gegevens tussen applicaties uit te wisselen.
Motivatie	Integratielaag biedt: • standaardmethodes voor het uitwisselen van gegevens.

	• hergebruik voor nieuwe koppelingen. • zowel kernregistraties (lokaal) als basisregistraties (landelijk) zijn relatief eenvoudig te koppelen met daarvoor geschikte applicaties. • maakt automatiseren van routinematige gegevensuitwisseling mogelijk en geeft ruimte voor nieuwe initiatieven en verbeterlagen. • Leidt tot betere procesbesturing en minder fouten bij gegevensoverdracht.
--	---

AA05	
Principe	Cloud, PaaS en SaaS: Applicaties worden aangeboden vanuit de Cloud middels Platform as a Service (PaaS) of Software as a Service (SaaS).
Motivatie	• Applicaties en gegevens zijn overal beschikbaar voor de CIZ medewerkers • Altijd werken met de laatste versie en minder afhankelijk van eigen ICT-beheer • Minder ICT-beheer, zowel software en hardware als databases

AA06	
Principe	Ondersteuning foutsituaties: Processen houden expliciet rekening met foutsituaties.
Motivatie	In de praktijk treden er allerlei functionele uitzonderingssituaties op in processen binnen Data & Analytics (denk aan inladen van gegevens). Als deze uitzonderingen leiden tot technische fouten die door specialisten worden afgehandeld dan kan hier in de processen niet meer op worden gestuurd. Hierdoor is er een reële kans dat tijdslijnen worden overschreden en er zelfs business verloren kan gaan.

AA07	
Principe	Centrale identiteit opslag: Data en Analytics platform wordt aangesloten op een centrale identiteit opslag.
Motivatie	Er wordt gebruik gemaakt van een services voor identiteits- en toegangsbeheer in de Cloud (Azure AD). Deze centrale identiteit opslag biedt veilige verificatie- en autorisatieoplossingen, zodat CIZ medewerkers toegang hebben tot de toepassingen die ze nodig hebben.

AA08	
Principe	Publiceren wijzigingen: Gewijzigde gegevens worden gecommuniceerd middels publish/subscribe.
Motivatie	Het verspreiden van gewijzigde gegevens is anders van aard; de herbruikbaarheid en het initiatief van de communicatie ligt daar juist bij het systeem dat de gegevens beheert.

AA09	
Principe	Scheiding rapportage en analyse: Rapportage en analyse is gescheiden van de operationele omgeving.
Motivatie	Rapportage vanuit een gescheiden omgeving voorkomt onderbrekingen en vertragingen in de operationele omgeving. Rapporten hebben veelal gegevens nodig die zijn verspreid over meerdere applicaties. Analytische applicaties vragen eigen gegevens om performance problemen op bronapplicaties te voorkomen, zoals

	onderbrekingen en vertragingen in de bronsystemen als gevolg van dataloads van het Data & Analytics platform.
--	---

AA10	
Principe	Historische data volgt bron: De historische opslag de bron te laten volgen in plaats van geïntegreerde en bewerkte data historisch op te slaan.
Motivatie	De historische opslag de bron te laten volgen in plaats van geïntegreerde en bewerkte data historisch op te slaan. Bronsystemen zijn stabiel en de interpretatie van de data en zijn verbanden betekenen. Indien de informatiebron geen voorzieningen voor historische opslag heeft, wordt gebruik gemaakt van het Data & Analytics platform voor historische opslag.

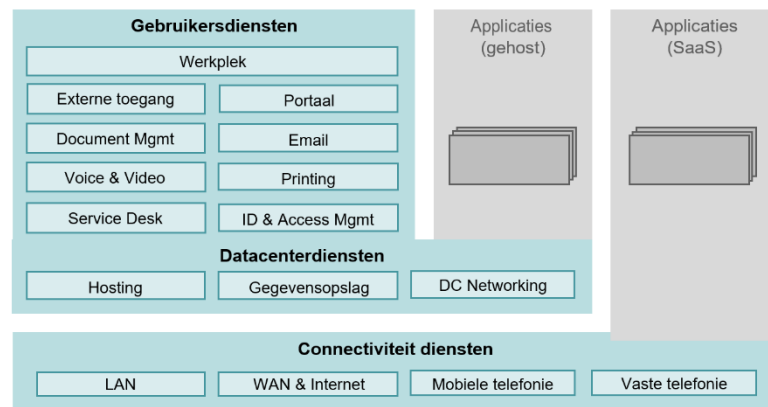
7 Technische architectuur

De Technische architectuur beschrijft de samenhang tussen de hardware, netwerkcomponenten en de software die nodig is om informatie tussen applicaties te kunnen delen die binnen de informatievoorziening van het CIZ worden gebruikt. De infrastructuur dient eigenlijk als het fundament om de informatievoorziening op te bouwen. In de praktijk zijn de verantwoordelijkheden voor de hosting en het technische beheer van de infrastructuur voor de primaire proces applicaties en Data & Analytics van het CIZ belegd bij een externe leverancier.

7.1 Technische architectuur componenten (IST)

In de volgende view wordt een overzicht gegeven van de infrastructuurcomponenten die door de huidige leverancier worden ingezet om de huidige applicaties van het CIZ op een robuuste, betrouwbare en veilige manier te ondersteunen. Het betreft hier alleen de infrastructuurcomponenten die worden ingezet voor de exploitatie van de primaire procesapplicaties en Data & Analytics binnen het CIZ.

Onderstaande figuur geeft een overzicht van de verschillende diensten binnen de CIZ infrastructuur. De diensten zijn ondergebracht in de volgende categorieën:



- **Gebruikersdiensten**

Voorzien de medewerkers van de standaardmiddelen en -functies om voor hun taakuitvoering te kunnen werken met documenten, te kunnen communiceren en samenwerken, en toegang te krijgen tot bedrijfsapplicaties.

- **Datacenterdiensten**

Bieden voorzieningen om op centrale locaties (datacenters) softwarecode te kunnen uitvoeren en digitale gegevens te kunnen opslaan. Datacenter diensten kunnen zowel worden ingezet voor gebruikersdiensten als voor bedrijfsapplicaties die worden gehost binnen de eigen infrastructuur. Bedrijfsapplicaties die worden afgenomen als dienst (Software-as-a-Service) maken daarentegen geen gebruik van de datacenterdiensten.

- **Connectivitediensten**

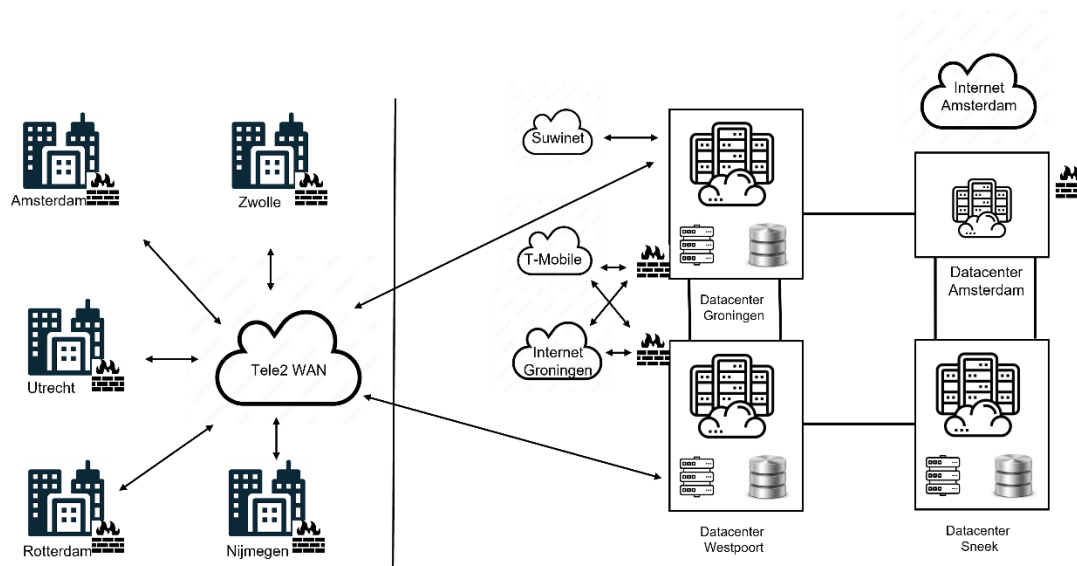
Zorgen voor het transporteren van digitale gegevens tussen en met de verschillende apparaten en componenten binnen de informatievoorziening.

Datacenterdiensten

Datacenterdiensten zijn voorzieningen voor het op een centrale locatie (datacenter) bewerken en opslaan van digitale gegevens.

Datacenterdiensten worden door externe leverancier geleverd onder de overeenkomst ICT-dienstverlening.

De ICT-dienstverlener maakt voor de dienstverlening aan het CIZ gebruik van meerdere datacenters, die onderling en met externe omgevingen zijn verbonden via redundante netwerkverbindingen. Een en ander is schematisch weergegeven in onderstaande figuur.

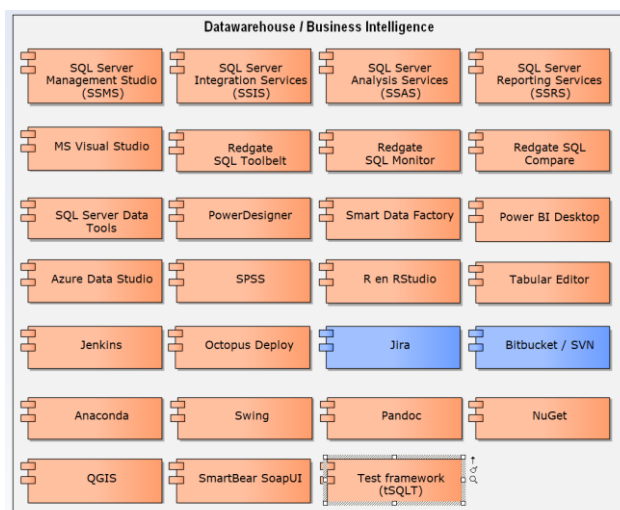


Op de verschillende locaties worden de volgende voorzieningen gerealiseerd:

- Datacenter Groningen: primaire locatie voor het CIZ, hier zijn alle applicaties en diensten ondergebracht en bevinden zich de primaire externe netwerkkoppelingen naar het CIZ Wide Area Network, het internet, Diginetwerk (via Suwinet en via RINIS) en de openbare telefonieomgeving.
- Datacenter Westpoort: uitwijklocatie voor het CIZ. Hier worden de systemen gehuisvest die bij uitval van de primaire locatie de hostingfuncties voor de meeste applicaties en diensten overnemen en/of in stand houden. Tevens zijn hier de redundante netwerkkoppelingen naar het Wide Area Network, het internet en openbare telefonie ondergebracht.
- Datacenter Sneek en Amsterdam : hier worden de off-site back-ups bewaard.

7.2 Tool stack (IST)

De gebruikte applicaties en tools zijn hieronder weergegeven:



7.3 Technische architectuur componenten (SOLL)

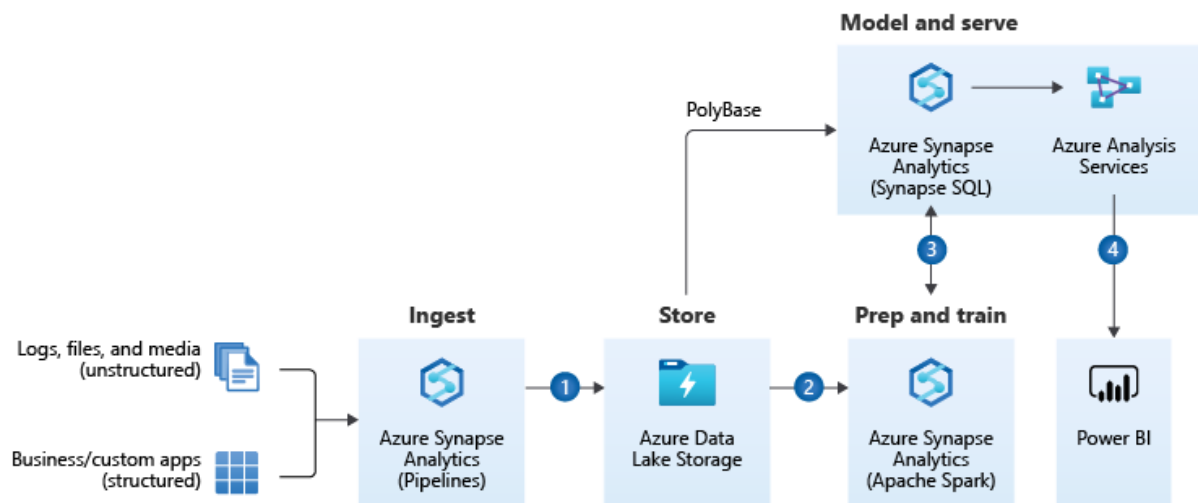
De Cloud technologie zal de komende jaren een grotere rol in gaan nemen. Hierdoor is het eenvoudiger om infrastructuur op te zetten en op te schalen. Daarnaast zijn er in de Cloud aanzienlijk meer functionaliteiten en toepassingen mogelijk. De transformatie naar de Cloud is in de Data & Analytics dienstverlening bijna onomkeerbaar en kan versnelling en meer mogelijkheden bieden in het realiseren van de ambities van het CIZ. De integratie en interoperabiliteit van Cloud omgevingen onderling is de afgelopen jaren aanzienlijk verbeterd. Dit helpt het CIZ in de ambities om met meerdere externe bronnen te koppelen. CIZ wil voorzieningen als een proeftuinomgeving voor het datalab team gebruiken en Cloud zal al snel veel voordelen bieden.

De conclusie van het CIZ is dat het hosten van de Data & Analytics omgeving in de publieke Cloud wat betreft toekomstige mogelijkheden meer te bieden heeft dan dat een on-premise omgeving, zeker op technische ontwikkelingen. Daarnaast blijkt het ook qua kosten effectiever te zijn door het op- en af kunnen schalen van resources en tijdelijk gebruik kunnen maken van tools of extra functionaliteiten zonder grote investeringen. Van belang hierbij is wel dat er goed beheer op plaatsvindt, zodat als extra capaciteit of functionaliteit niet meer nodig is, hier ook op geacteerd wordt. Ook is er bij Cloud beter inzicht in de kosten. Cloud geeft ook een goede mogelijkheid om in zeer korte tijd databases neer te zetten en te configureren.

Vanuit technisch en functioneel perspectief is er een duidelijke voorkeur van het CIZ om Data & Analytics hosten in de Cloud. Het hosten van Data & Analytics in de Cloud dient echter wel te gebeuren binnen de kaders en de richtlijnen van het Cloud beleid CIZ.

7.4 Tool stack (SOLL)

Het CIZ heeft haar uitgangspunten, huidige situatie, ambities in een marktconsultatie met drie leveranciers besproken. De leveranciers hebben het Azure platform geadviseerd. De benoemde applicaties en tools in Azure Enterprise Datawarehouse omgeving zijn hieronder weergegeven:



Bovenstaande is een aanzet van Microsoft voor een Enterprise Datawarehouse binnen Azure Cloud omgeving. Hierboven genoemde producten zijn resources welke binnen de Azure omgeving afgenomen kunnen worden. Hieronder een korte beschrijving van deze diensten:

Azure Synapse Analytics is het snelle, flexibele en vertrouwde Cloud datawarehouse waarmee elastisch en onafhankelijk geschaald kan worden. Maar ook berekenen en opslaan, met een massively parallel verwerkingsarchitectuur.

Azure Synapse-pijplijnen is er voor om ETL-/ELT-werkstromen te maken, te plannen en te beheren.

Azure Blob Storage is oplossing voor de opslag van objecten in de cloud. Blob Storage is geoptimaliseerd voor het opslaan van enorme hoeveelheden niet-structureerde gegevens. Ongestructureerde gegevens zijn gegevens die niet voldoen aan een bepaald gegevensmodel of bepaalde definitie, zoals tekst of binaire gegevens.

Azure Synapse Analytics Spark-pools is een framework voor parallele verwerking dat ondersteuning biedt voor in-memory verwerking om de prestaties van toepassingen voor de analyse van big data te verbeteren.

Azure Analysis Services is kubussen in de Cloud.

Power BI is een suite met hulpprogramma's voor bedrijfsanalyse die inzichten bieden in de CIZ organisatie. Verbinding maken honderden gegevensbronnen, vereenvoudigde gegevensvoorbereiding en ad-hocanalyse mogelijk.

7.5 Technische architectuur principes

De belangrijke principes voor de Technische Architectuur (TA) worden in deze paragraaf geschreven. Deze principes zijn samengesteld uit de uitgangsdOCUMENTEN genoemd in hoofdstuk 3.

TA01	
Principe	Beschikbaar: Op basis van business requirements bepaalt CIZ de mate van beschikbaarheid van verschillende soorten gegevens.
Motivatie	De beschikbaarheid van applicaties en gegevens is een essentieel onderdeel binnen het CIZ. ICT diensten moeten altijd beschikbaar zijn, op ieder moment, overal. Een CIZ medewerker moet overal, vanaf iedere plek, bij zijn of haar gegevens kunnen.

TA02	
------	--

Principe	Taal los van transport: We maken onderscheid tussen taal en transport en koppelen dat los van elkaar.
Motivatie	Taal, het vocabulaire dat gesproken wordt, en het transport zijn verschillende onderdelen. Het vocabulaire en de semantiek van de gegevens wordt gedefinieerd in de data architectuur en resulteert in uitwisselingsformaten. Het transport wordt gedefinieerd in de technologische architectuur inclusief de gegevens die voor het realiseren van het transport noodzakelijk zijn. Het transport van gegevens moet via verschillende kanalen van transport kunnen plaatsvinden.

TA03	
Principe	De infrastructuur is beveiligd conform het organisatie beveiligingsbeleid: Applicaties, functionaliteiten en infrastructuur voldoen aan de behoeften op het gebied van beveiliging die worden gesteld en voldoen aan het interne beveiligingsbeleid binnen het CIZ en de wettelijke eisen en plichten op dat gebied. Toegangsbeveiligingsbeheer is gericht op interne en externe rollen.
Motivatie	Binnen de applicaties en functionaliteiten moet autorisatie kunnen worden toegepast op het benodigde niveau, voor zowel de functionaliteiten als de gegevens.

TA04	
Principe	Medewerkers kunnen hun werk apparaat onafhankelijk uitvoeren: Functionaliteit is op elke werkplek, locatie (verbonden met internet) en tijdstip te gebruiken. De fysieke werkplek is niet meer van één specifieke gebruiker, maar iedere gebruiker is in staat om op een plek met een device met een browser te werken, onafhankelijk van de locatie waar de gebruiker zich bevindt conform CIZ beleid en richtlijnen (qua werkplek, device en browser).
Motivatie	De behoefte aan flexibel werken wordt steeds groter. Niet alleen zullen gebruikers steeds meer op verschillende fysieke locaties gaan werken, zowel binnen als buiten de organisatie, ook zullen zij vaker binnen de organisatie en over afdelingen heen met flexwerkplekken te maken krijgen (mede in het kader van procesgericht werken). De gebruiker moet in staat zijn zich op iedere willekeurige plek waar een (draadloze) internetverbinding beschikbaar is aan te melden op de systemen. De gebruiker heeft dan de beschikking over en toegang tot alle applicaties en informatie waar hij conform zijn gebruikersprofiel (rol) recht op heeft. Deze benadering vermindert ook de beheerlast op de infrastructuur bij verhuizingen en organisatiewijzigingen.

TA05	
Principe	De infrastructuur is flexibel: De infrastructuur kenmerkt zich door het vermogen componenten te wijzigen zonder grote continuïteitsrisico's, zonder veel kosten en binnen acceptabele doorlooptijden. De infrastructuur is voorbereid op het kunnen ondersteunen van nieuwe functionaliteit en kan snel inspelen op veranderingen in de vraag naar ICT diensten en veranderingen in de bedrijfsvoering. De infrastructuur is voldoende schaalbaar om bij toe- of afname van het gebruik geen ingrijpende aanpassingen aan de inrichting door te hoeven voeren.
Motivatie	Op deze wijze kan de ICT infrastructuur op een optimale manier inspelen op de behoeften die ontstaan vanuit het CIZ. De dimensies van waaruit het begrip flexibiliteit kan worden benaderd, zijn werkwijzen, schaalbaarheid, presentatie, onafhankelijkheid, partitionering, integratie, hergebruik en implementatiesnelheid.

TA06	
-------------	--

Principe	De infrastructuur bestaat uit open standaarden en is gericht op integratie: De ICT infrastructuur bestaat uit verschillende systemen en technologieën. In plaats van een streven naar eenvormigheid, wordt gestreefd naar een open architectuur, gericht op integratie van systemen en functionaliteiten.
Motivatie	Door gebruik te maken van open standaarden wordt bevorderd dat de verschillende infrastructurele componenten onderling op elkaar kunnen aansluiten en onderling uitwisselbaar zijn, dat de afhankelijkheid van bepaalde producten en leveranciers kleiner wordt, dat de infrastructuur flexibeler en opener wordt en dat de continuïteit op langere termijn verzekerd is. Het gebruik van een service bus reduceert de complexiteit van koppelingen en realiseert een betere applicatie integratie. Het streven is een generieke service bus voorziening waarop alle applicaties zijn aangesloten.

TA07	
Principe	Behoud van informatie: Wanneer een deel van de informatiebehoefte naar de Cloud wordt verhuisd, is het natuurlijk belangrijk dat bestaande gegevens behouden blijven.
Motivatie	Bij afname van Cloud diensten worden de eigen servers vertaald naar virtuele servers bij de Cloud provider. Elke Cloudleverancier biedt wel een mogelijkheid om fysieke servers te vertalen naar virtuele machines. Het is daarbij goed om zo veel mogelijk gebruik te maken van open standaarden, zoals het Open Virtualisation Format (OVF). De migratie van data zal in dat geval, mits goed voorbereid, relatief eenvoudig kunnen gebeuren. Bij afname van een SaaS-dienst wordt een eigen applicatie vervangen door een standaard Cloud-applicatie en het eigen dataformat dient in dat geval te worden gemigreerd naar een format dat ondersteund wordt door de Cloudapplicatie.

TA08	
Principe	Applicatiekoppelingen met juiste webservices: Koppelingen met applicaties binnen de eigen omgeving of zelfs met andere Cloudapplicaties moet gebaseerd zijn op open standaarden.
Motivatie	Voor meeste koppelingen binnen Cloud worden veelvuldig webservices gebruikt, die wel of niet gebaseerd zijn op open standaarden. Bij de selectie van een SaaS-provider dient er rekening mee gehouden te worden dat deze voor de desbetreffende Cloudapplicatie de juiste webservices ondersteund op basis van de juiste koppelvlakken.

TA09	
Principe	Cloud en Life Cycle Management: Het Data Analytics platform biedt de volledige functionaliteiten en diensten in de Cloud omgeving.
Motivatie	Het Data & Analytics platform heeft belangrijke voordelen, voordelen die gelden bij het gebruik van clouddiensten. Dat zijn onder andere: • Eénmalig inrichten van hoge schaalbaarheid en beschikbaar voor alle subscriptions • Alle componenten redundant uitgevoerd • Monitoring en schaalbaarheid éénmalig ingeregeld voor alle subscriptions • Infrastructuur voor continuous deployment gedeeld (CI/CD) • Releases zonder productieonderbreking • Resources optimaal gebruikt • Snel beschikbaar voor nieuwe tenants (geen infrastructuur uitrol) • Life Cycle Management van het platform uniform.

8 Informatiebeveiliging en Privacy

Informatiebeveiliging en beheer is gericht op het waarborgen van de kwaliteitsaspecten Beschikbaarheid, Vertrouwelijkheid, Integriteit en Controleerbaarheid. Het waarborgen van de aspecten Integriteit en Vertrouwelijkheid hebben dezelfde functionaliteit nodig.

Alle zorgvuldigheid volgens principes van doelbinding, proportionaliteit, beveiligingsklasse van gegevens en dergelijke is immers gebonden aan de aard van de gegevens en moeten door de applicatiecomponenten geïmplementeerd worden. Eventueel nieuw in te regelen autorisaties op de gemigreerde componenten en/of datasets zijn rol gebaseerd en worden vastgelegd in het autorisatie beheer tool (lees: Azure Active Directory).

8.1 Normenkaders voor informatiebeveiliging

Vanuit de overheid worden verschillende normenkaders aangereikt voor het beveiligen van informatie en informatiesystemen. Deze normenkaders kunnen bindend of richtinggevend zijn. De voor het CIZ toepasselijke normenkaders worden hieronder kort besproken.

8.1.1 Voorschrift Informatiebeveiliging Rijksdienst (VIR)

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR) is een oorspronkelijk in 1995 van kracht geworden en in 2007 vernieuwd besluit dat algemene eisen stelt aan de beveiliging van de informatievoorziening en de informatiesystemen binnen de rijksoverheid, ongeacht de toegepaste technologie en het karakter van de informatie. Het gaat daarbij met name om het identificeren en toekennen van de verantwoordelijkheden in de organisatie. In het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) uit 2013 worden aanvullende maatregelen gespecificeerd voor de behandeling van vertrouwelijke informatie bij de rijksdienst en wordt hier ook een rubricering voor gedefinieerd.

8.1.2 Baseline Informatiebeveiliging Overheid (BIO)

Waar het VIR en het VIR-BI de algemene eisen beschrijven waaraan de beveiliging van de informatiesystemen moet voldoen, wordt in de Baseline Informatiebeveiliging Overheid (BIO) een gemeenschappelijk normenkader aangereikt voor de maatregelen die moeten worden genomen om aan de beveiligingseisen te voldoen. De BIO vervangt sinds 1 januari 2019 de specifieke baselines voor Rijk, Gemeenten en Provincies en daarmee hanteert de overheid dus één basisniveau voor informatiebeveiliging.

De BIO is gebaseerd op de internationale normen voor informatiebeveiliging NEN-ISO/IEC 27001:2017 en 27002:2017 en beschrijft de invulling daarvan voor de overheid. De BIO bestaat voor het grootste deel uit de ISO normen, maar voegt daar een aantal specifieke maatregelen aan toe die van toepassing zijn op de situatie van de overheid.

Bovendien hanteert de BIO een indeling op basis van zogenoemde BasisBeveiligingsniveau's (BBN's) om risicomanagement hanteerbaar en efficiënt te houden. Door te kijken naar de betrouwbaarheidseisen (beschikbaarheid, integriteit en vertrouwelijkheid) die gesteld worden aan de informatie die beveiligd moet worden en de dreigingen die er zijn, wordt bepaald welke set aan maatregelen relevant is voor een adequate beveiliging van die informatie:

- Bij BBN1 gaat het om wat er minimaal verwacht mag worden van de overheid voor de bescherming van informatie. We hebben hier te maken met een laag betrouwbaarheidsniveau en daarom blijven complexe eisen hier achterwege. Het gaat puur om een minimale basis.

- Bij BBN2 komen we op het niveau waar de meeste informatie van de overheid in valt. Het gaat hier om goed huisvaderschap voor informatie. BBN2 is het standaardniveau. BBN2 is het minimale niveau waarop met persoonsgegevens gewerkt wordt. BBN2 ligt qua zwaarte op hetzelfde niveau als de oude baselines. Bij BBN2 ligt voor statelijke actoren en vergelijkbare dreigers de nadruk op 'detectie'.
- BBN3 vergt aanvullende maatregelen om weerstand te kunnen bieden tegen statelijke actoren of criminele organisaties (of gelijksoortige actoren) of waar informatie wordt verwerkt die door de bronhouder een bepaalde classificatie (boven BBN2) heeft mee gekregen. De BIO schrijft voor BBN3 geen standaard maatregelen voor, aangezien op dit niveau vanwege de hoge complexiteit veelal maatwerk is vereist. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van NAVO en EU-normen.

De meest gevoelige data/informatie binnen het CIZ zijn de cliëntengegevens (met name medische gegevens en BSN), justitiële gegevens, personeelsgegevens. Het overgrote deel van de gegevens die het CIZ verwerkt vallen onder beveiligingsniveau BBN2. De overige gegevens binnen het CIZ vallen onder het lagere BBN1 niveau. Voor deze twee niveaus staat VWS het gebruik van cloud toe.

8.1.3 Algemene verordening gegevensbescherming (AVG)

AVG is een privacywet die geldt in de hele Europese Unie (EU). Het principe van 'Data protection by design and by default' worden daadwerkelijk ingevuld. Er wordt de impact van de implementatie van passende maatregelen om de persoonsgegevens te beschermen inzichtelijk. Onder de AVG gelden er nieuwe:

Informatieverplichtingen. Cliënten hebben van tevoren recht op heldere informatie over wat het CIZ met hun persoonsgegevens gaat doen en waarom.

Regels voor het werken met toestemming van de client. Het CIZ moet kunnen aantonen dat CIZ daadwerkelijk toestemming van zijn client heeft gekregen.

8.1.4 Forum Standaardisatie

Het Forum Standaardisatie is een adviescommissie, benoemd door het Ministerie van Binnenlandse Zaken, die open standaarden toetst en voorschrijft aan publieke organisaties. Het Forum Standaardisatie beheert twee lijsten van open standaarden. Voor de standaarden op de lijst "Verplichte standaarden" geldt het "Pas toe of Leg uit" principe. Dit houdt in dat de standaard verplicht moet worden gebruikt (Pas toe), tenzij de betreffende dienst of het betreffende product in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert of er sprake is van een andere reden van bijzonder gewicht. De afwijking en de reden daarvan moeten beschreven worden in de bedrijfsvoeringparagraaf van het jaarverslag (Leg uit). Voor de standaarden op de lijst "Aanbevolen standaarden" geldt het "Pas toe of Leg uit" principe niet.

De Verplichte standaarden hebben niet alleen betrekking op informatiebeveiliging, maar ook op interoperabiliteit (koppelvlakken en uitwisselformaten).

8.1.5 NEN 7510-7513

NEN-7510 is een door het Nederlands Normalisatie-Instituut ontwikkelde en beheerde norm voor informatiebeveiliging in de zorg. De norm is van toepassing op alle organisaties werkzaam in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. De verplichting is opgenomen in de "Regeling gebruik burgerservicenummer in de zorg" bij de Wbsn-z.

NEN-7510 geeft aan wat een organisatie moet doen om informatie te beveiligen, maar bevat geen expliciete aanwijzingen voor specifieke technische maatregelen.

NEN-7510 bestaat uit twee delen. NEN-7510-1 stelt eisen aan het informatiebeveiliging managementsysteem en NEN-7510-2 geeft richtlijnen voor beheersmaatregelen. Daarnaast kent NEN 7510 nog de volgende aanvullende normen:

- NEN-7512: Vertrouwensbasis voor gegevensuitwisseling
- NEN-7513: Eisen aan instellingen die audits t.b.v. certificatie van informatiebeveiliging managementsystemen in de zorg uitvoeren
- NTA-7516: Eisen voor veilige e-mail en chatapplicaties

De norm kan worden gehanteerd in verschillende bij de zorg betrokken organisaties, zoals individuele zorgverleners, zorginstellingen, netwerkorganisaties, verzekeraars, certificerende organisaties. Hoewel NEN 7510 niet direct van toepassing is op het CIZ, moet het CIZ hier wel rekening mee houden voor wat betreft de gegevensuitwisselingen met zorgaanbieders en cliënten.

8.2 Informatiebeveiliging principes

IBP01	
Principe	<i>Toegang tot de CIZ informatievoorziening</i> Gebruikers wordt toegang tot diensten verleend, waarvoor ze specifiek bevoegd zijn en zijn identificeerbaar met een persoonlijk, uniek en voor de medewerker herkenbaar account.
Motivatie	Hier wordt invulling aangegeven doordat Single Sign On ondersteund wordt.

IBP02	
Principe	<i>Aansluiting op Active Directory</i> De gegevens – inclusief accountgegevens, waaronder het wachtwoord - die bepalen welke gebruikersrechten zijn toegekend, worden vastgelegd in de centrale CIZ directory Services (Active Directory).
Motivatie	Hiervan moet het toekomstige systeem gebruik maken.

IBP03	
Principe	<i>Doelbinding</i> De term doelbinding staat voor het gestructureerd en gecontroleerd ontsluiten van informatie (documenten en gegevens) aan slechts die medewerkers die dit direct nodig hebben voor het uitvoeren van hun taak. Voorwaarden voor de ontsluiting zijn: • Toegangsbevoegdheid. Het bevoegd zijn om de informatie te mogen inzien. • Behandelrelatie. Het hebben van een relatie tussen medewerker en het object van aanvraag.
Motivatie	Dit principe moet ondersteund worden door de concepten van het toekomstige systeem.

8.3 Logging & monitoring

Logging: Het proces van registreren van informatie (voor Informatie Beveiliging & Privacy (IB&P) analyse en bewakingsdoelstellingen) over menselijke- en systeemactiviteiten binnen systemen en op netwerken van het CIZ en het vastleggen daarvan in logrecords.

Monitoring: Het gebruiken van gelogde informatie om de digitale veiligheid van de organisatie en de privacy van de cliënten te waarborgen.

IBP05	
-------	--

Principe	Een logregel bevat de vereiste gegevens (zoals: de gebeurtenis, herleidbaarheid tot een medewerker, identiteit van het werkstation of de locatie, handelingen, datum en tijdstip).
Motivatie	Met zekerheid kunnen detecteren van eventuele schendingen van functionele of beveiligingseisen en om achteraf de juistheid van uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

IBP06	
Principe	Een logregel bevat in geen geval gegevens die de beveiliging kunnen doorbreken van de beveiliging kunnen leiden (zoals: wachtwoorden, inbelnummers enz.).
Motivatie	Zorg dragen dat het mogelijk blijft om (achteraf) met zekerheid eventuele schendingen van functionele en beveiligingseisen te detecteren en aantonen.

IBP07	
Principe	De informatieverwerkende omgeving wordt door detectievoorzieningen bewaakt met behulp van een Security Information and Event Management (SIEM) en/of Security Operations Centre (SOC), die wordt ingezet op basis van een risico-inschatting en van de aard van de te beschermen gegevens en informatiesystemen zodat aanvallen kunnen worden gedetecteerd.
Motivatie	CIZ verwacht voor alle nieuwe systemen één centrale SIEM en SOC implementatie.

IBP08	
Principe	Nieuw ontdekte dreigingen (aanvallen) worden binnen de geldende juridische kaders gedeeld binnen de overheid door (geautomatiseerde) threat-intelligence-sharing mechanismen.
Motivatie	Bij ontdekte nieuwe dreigingen worden deze, rekening houdend met geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het Nationaal Cyber Security Centrum (NCSC) door geautomatiseerde mechanismen.

IBP09	
Principe	Bij het verwerken van persoonsgegevens wordt, conform het gestelde in de Algemene Verordening Gegevensbescherming (AVG), een verwerkingsactiviteiten register bijgehouden.
Motivatie	Het register van verwerkingsactiviteiten (verwerkingsregister) bevat informatie over de persoonsgegevens die CIZ verwerkt. AVG schrijft voor welke informatie CIZ als verantwoordelijke of verwerker in het verwerkingsregister moet zetten.

IBP10	
Principe	De log-bestanden worden gedurende een overeengekomen periode bewaard voor toekomstig onderzoek en toegangscontrole.
Motivatie	Onrechtmatige pogingen om persoonsgegevens in te zien of te wijzigen worden tijdig gedetecteerd en vastgelegd, zodat via de logregistratie de oorzaak van een datalek kan worden achterhaald of daar een bijdrage aan kan leveren en dat onrechtmatige pogingen worden ontmoedigd of zelfs voorkomen.

IBP11	
Principe	IT middelen (Infrastructuur, waaronder ook netwerken, middleware en applicaties) behoren adequaat te worden gemonitord om ze te beschermen tegen bedreigingen en om beveiliging te handhaven.
Motivatie	De inrichting van de IT-middelen en de gehanteerde protocollen dienen aanvallen/dreigingen te detecteren om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

IBP12	
Principe	De logging- en detectie informatie (registraties en alarmeringen) en de condities van de beveiliging van IT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
Motivatie	Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de IT-diensten en de status van de componenten waarmee deze worden voortgebracht.



CIZ
Orteliuslaan 1000
3528 BD Utrecht
Postbus 2690
3500 GR Utrecht

T: 088 789 1000
F: 088 789 1011
E: info@ciz.nl
www.ciz.nl