

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Europese aanbesteding volgens de openbare procedure voor het tijdelijk ter beschikking stellen van ICT-Professionals op Detavast basis ten behoeve van de Ministeries van Defensie, het Ministerie van Volksgezondheid, Welzijn en Sport, het Ministerie van Sociale Zaken en Werkgelegenheid en het Ministerie van Buitenlandse Zaken.

Deelnemers ICT-organisatie en -landschap

v 1.0

Inhoud

1.	Het ministerie van Defensie	2
2.	Het ministerie van Volksgezondheid, Welzijn Sport	5
3.	Het ministerie van Buitenlandse zaken	6
4.	Het ministerie van Sociale Zaken en Werkgelegenheid	13

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

1. Het ministerie van Defensie

Visie op de IV/ICT-organisatie binnen Defensie

Ons Koninkrijk wordt dagelijks aangevallen in het cyber- en informatiedomein. Cruciale fysieke en digitale knooppunten worden vaker doelwit. Door beïnvloeding van verkiezingen en andere vitale processen willen tegenstanders landen moedwillig destabiliseren. Vroeger hadden we een gebrek aan informatie. Nu is er vaak te veel: we moeten constant filteren en zoeken in de hooiberg naar de spelden die waarheid zijn. We leven daarbij in een wereld vol verbindingen. We zijn een land van openheid en in onze open economie zullen er altijd onvermijdelijke afhankelijkheden bestaan. Dit maakt het beschermen van onze economische veiligheid extra belangrijk.

Oude dreigingen blijven bestaan en er komen nieuwe dreigingen bij. Ze komen tegelijkertijd en in vele vormen op ons af. Uit alle analyses blijkt dat er steeds vaker een beroep op de schaarse capaciteiten van Defensie zal worden gedaan. We moeten vaker en in meer verschillende situaties op (kunnen) treden. We moeten sneller terplekke kunnen zijn en er langer kunnen blijven.

Deze toenemende vraag naar Defensie inzet vergroot de kloof tussen taken enerzijds en middelen, voorraden en ondersteuning anderzijds. Het overwicht van de NAVO, waar we sterk op leunen, staat ondertussen onder druk. Eensgezind handelen is geen gegeven meer. Europa moet zelfstandiger kunnen optreden, maar kan dat momenteel niet. Defensie is onvoldoende toegerust voor het tegengaan van hybride dreigingen en optreden in de informatieomgeving. We hebben vaak een gebrek aan handelingsperspectief omdat we geen duidelijke dader kunnen aanwijzen. Daarnaast hebben we een personeelstekort voor hoe de organisatie nu is ingericht. De arbeidsmarkt zal in de toekomst geen oplossing bieden, dus die zullen we zelf moeten vinden.

Om de genoemde dreigingen en uitdagingen het hoofd te bieden zijn er tien inrichtingsprincipes (binnen drie sub thema's) opgesteld in de Defensie 2035 visie. De tien inrichtingsprincipes die het profiel van de defensieorganisatie worden, zijn:

1. Technologisch hoogwaardig
 - Unieke mensen en arbeidsextensieve capaciteiten
 - Flexibel optreden: snel inzetbaar, schaalbaar en zelfstandig
 - Sterk innoverend vermogen
 - Escalatiedominantie, met onze partners
2. Informatie gestuurd in organisatie en optreden
 - Gezaghebbende informatiepositie
 - Multidomein en geïntegreerd optreden
3. Betrouwbaar partner en beschermer
 - Transparant en zichtbaar in een betrokken samenleving
 - Inzetten op een sterker, zelfredzamer Europa
 - Inzetten op verdere specialisatie binnen de NAVO en de EU
 - Strategische capaciteiten voor diverse doeleinden

Verder moet de krijgsmacht doorlopend nieuwe manieren vinden om innovatief te zijn zonder de continuïteit van de bedrijfsvoering en de beveiliging van haar systemen en data in gevaar te brengen. Dit vereist ook flexibiliteit en adaptief vermogen in de bedrijfsvoering. De volgende ontwikkelingen onderstrepen het belang van deze zorgvuldige balans:

1. Wapensystemen in het digitale tijdperk. Wapensystemen bevatten steeds meer IT. Bijvoorbeeld het F-35 gevechtsvliegtuig. De missiecomputer koppelt alle sensoren (zoals CCTV, IR en radar) aan elkaar om een gecombineerde inschatting te maken van de dreiging. Hierdoor is de piloot op de hoogte van de actuele '360 graden dreiging' en weet hij/zij bovendien of de vijand hem/haar 'kan zien'. Dit systeem is uniek. Het systeem presenteert dit niet alleen aan de piloot, maar ook aan alle anderen (zowel in de lucht, op de grond als op zee) die gebruik moeten maken van deze informatie. Dit geïntegreerd optreden met behulp van Network Enabled Capabilities (NEC) staat voor het effectief gebruiken van informatie. Ofwel, een samenhangend geheel van militair operationele processen dat wordt ondersteund door moderne netwerk- en communicatietechnologieën. Dit brengt met zich mee dat grote hoeveelheden gegevens worden verzameld en verwerkt voor commandovoering, inlichtingenvergaring en wapeninzet. Zonder toereikende IT kan dat niet effectief plaatsvinden. IT kan ook ingezet worden als hoofdwapensysteem, zoals offensief optreden in het cyberdomein;

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

2. Informatiegestuurd Optreden (IGO). De Commandant der Strijdkrachten (CDS) hanteert Informatiegestuurd Optreden (IGO) als belangrijk uitgangspunt in het speerpunt 'Vernieuwing Operationeel Domein'. De focus ligt op informatiedominantie en een ononderbroken, en volledig gedeelde en gepersonaliseerde Situational Awareness (SA) en Situational Understanding (SU). Het huidige en toekomstige optreden van Defensie vereist dat essentiële functionaliteiten van Informatievoorziening en commandovoering flexibel, schaalbaar, adaptief en integraal over de hele keten van sensor naar effector kunnen worden uitgevoerd. Operaties in grote operatiegebieden met beperkte middelen dwingen tot gerichte effectieve inzet van militair vermogen. IGO vloeit voort uit het genetwerkt samenwerken en wordt gekenmerkt door adequate middelen, afgestemde procedures, een integraal netwerk van deelnemende eenheden en organisaties en van gevalideerde informatie en inlichtingen. IGO stelt de organisatie in staat om in de toekomst doelgericht haar capaciteiten in te zetten en haar taken, operationeel effectief, uit te voeren;

3. Geïntegreerde bedrijfsvoering. Defensie werkt aan geïntegreerde bedrijfsprocessen. De invoering van Enterprise Resource Planning (ERP) is hiervan een voorbeeld. Hiermee kan de operationele footprint worden verkleind. Dit stelt hoge eisen aan de betrouwbaarheid van IT. Ook in de juridische, personele en medische processen is IT onmisbaar. Voorts maken eenheden in het operationele domein ook steeds meer gebruik van dit soort systemen. Daarmee vervaagt het onderscheid tussen IT voor de operationele taakuitvoering en voor de bedrijfsvoering. Vanuit de (operationele) behoefte moet dan ook heel bewust worden gekozen voor een beschikbaarheidsniveau van dit soort systemen;

4. Samenwerking. Defensie kiest voor samenwerking met strategische partners en marktpartijen (zoals NATO, interdepartementaal, veiligheidsketen, multi-agency of leveranciers) om capaciteiten te delen dan wel te poolen. Bij iedere vorm van samenwerking hoort het uitwisselen van informatie. Zonder adequate IT is dit niet meer mogelijk. Uit bijvoorbeeld de intensieve samenwerking met België (BENESAM) blijkt dat koppelingen tussen netwerken en toegang tot elkaars systemen steeds gangbaarder worden. Ook met internationale leveranciers van wapensystemen zijn beveiligde IT-verbindingen onmisbaar geworden in elke fase van ontwerp, ontwikkeling, productie, levering en gebruik;

5. Cyber defence en veiligheid. De technologische ontwikkelingen in de samenleving hebben grote invloed op onze veiligheid. Bedreigingen van buiten nemen toe. Ontwikkelingen zoals cyberaanvallen, virussen en malware leiden tot een wedloop tussen indringers en beveiligingsmaatregelen. De afhankelijkheid van digitale middelen leidt ook voor de krijgsmacht tot kwetsbaarheden die urgente aandacht behoeven. En het spreekt voor zich dat de impact op de samenleving van een grootschalige cyberaanval enorm kan zijn. De krijgsmacht wil ook in het digitale domein haar rol als 'zwaarmacht' naar behoren vervullen. Het voortdurend bewaken, monitoren en innoveren in IT is dan cruciaal. Het belang en de invloed van IT op zowel de bedrijfsvoering als de operationele inzet is groot. Het is een onmiskenbare enabler voor de gehele organisatie. Het fundament onder de doorontwikkeling van IT als integrale enabler rust op de volgende drie pijlers:

1. Continuïteit. De betrouwbaarheid van de IT is van wezenlijk belang. Zonder goed functionerende en betrouwbare IT geen inlichtingen, geen missies, geen bedrijfsvoering en dus geen goed functionerende krijgsmacht. Voor de inrichting van de continuïteit is een zorgvuldig vastgesteld risicoprofiel een vereiste;

2. Beveiliging. De aard van de krijgsmacht stelt hoge eisen aan de beveiliging. De beveiliging van IT-systemen en de integriteit van data moeten dan ook gegarandeerd zijn;

3. Innovatie. Met de ambitie om goed voorbereid te blijven op een scala aan inzetmogelijkheden is het noodzakelijk om slim gebruik te maken van nieuwe mogelijkheden. De krijgsmacht moet een wendbare (agile) organisatie zijn en blijven om 'anderen' een stap voor te zijn.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Doel en ambitie IV-organisatie

De CDS in zijn rol als behoeftesteller en corporate planner verantwoordelijk voor het 'wat'. Het Joint IV Commando (JIVC) is verantwoordelijk voor het 'hoe' en schrijft binnen opgelegde kaders de oplossingsrichting voor. Het JIVC is dé leverancier van IV-producten en diensten (inclusief ICT, documentaire IV trainers en simulatoren) voor Defensie (met inbegrip van de activiteiten die rechtstreeks zijn te relateren aan civiel-operationele samenwerking en de aan de Koninklijke Marechaussee opgedragen gezagstaken). Het JIVC zorgt voor tijdige beschikbaarheid van informatie in al zijn facetten met behulp van IV en ICT. Door de adviezen aan beleidsmakers, opdrachtgevers en klanten draagt JIVC bij aan realistische en haalbare IV-behoefte en opdrachten. De onvoorwaardelijke veilige toegang tot de juiste informatie en het delen daarvan is in toenemende mate bepalend voor de snelheid, flexibiliteit en effectiviteit van de defensieorganisatie bij het uitvoeren van alle hoofdtaken. De verantwoordelijkheid van het JIVC strekt zich uit over de gehele levenscyclus van de IV-dienstverlening. De (onderliggende) producten en diensten die het JIVC daartoe levert komen tot stand met behulp van eigen (Defensie) productiemiddelen en in toenemende mate in samenwerking met marktpartijen of die van militaire partners en militaire samenwerkingsverbanden (military/NATO off the shelf). In alle gevallen treedt het JIVC daarbij op als regisseur van de te leveren producten en diensten. Het uitgangspunt daarbij is dat de markt maximaal wordt benut. Afstemming met CDS vindt plaats in het kader van de opstelling van de nota Beleid-, Plannen- en Begrotingscyclus (BPB). Als de BPB-nota is vastgesteld, zal het JIVC binnen toegekende mandaten de BPB-nota uitvoeren. Buiten mandaat zal er dus afgestemd worden, met name met de CDS. De integratie tussen IV ten behoeve van operationele, bestuurlijke en ondersteunende processen wordt verstevigd op basis van één samenhangende IV-architectuur gebaseerd op BV(bedrijfsvoering)/IV-alignement. Bepalend voor de keuze zelf doen of de markt inschakelen zijn vooral de te ondersteunen activiteiten onder bijzondere gebruiksomstandigheden. Met het bepalen van de keuze wordt rekening gehouden met de criteria efficiënter en/of goedkoper. Het is de taak als Defensie te blijven draaien als al het andere faalt. Een eerste vereiste daarvoor is dat de IT stevig op orde is en daarvoor staat het JIVC vooraan om dit te realiseren.

De IV-organisatie

JIVC, het IT-bedrijf van Defensie, is dé leverancier van IV-producten en diensten, zowel voor operationele, bestuurlijke als ondersteunende processen en levert daarmee een substantiële bijdrage aan de waardeketen van Defensie. JIVC is tevens het kenniscentrum voor vorming van IV-beleid en bedrijfsvoering en geeft (dwingende) adviezen aan beleidsmakers, opdrachtgevers en klanten. Het JIVC draagt zo bij aan realistische en haalbare IV-behoefte en opdrachten.

Het JIVC, met circa 3.500 medewerkers, wordt aangestuurd door een directeur, zijn plaatsvervanger en een aantal directieleden. JIVC bevindt zich in een ontwikkeltraject met een gefaseerde reorganisatietraject. Fase 1 van de reorganisatiefase is uitgevoerd. Op basis van deze reorganisatie wordt de directie ondersteund door de (staf)afdelingen Ondersteunende Staf, Plannen en Bedrijfsvoering, Architectuur en Programma Organisatie GrIT (grensverleggende IT). De volgende afdelingen zijn binnen JIVC ingericht:

1. Maritieme IT;
2. Landgebonden IT;
3. Luchtgebonden en Joint IT;
4. Civiel-Operationele Command en Control en Inlichtingen & Veiligheid IT;
5. Materieel logistieke en Financiële IT;
6. Personeel, Organisatie en Medische toepassingen IT;
7. Bestuurlijke en Overige Ondersteunende IT;
8. Generieke IT en Infrastructuur.

De eerste vier productieafdelingen vormen samen de Operationele IT (OIT) en de productieafdelingen 5 t/m 7 de Functionele IT (FIT). De afdeling Expertisecentrum is ingericht om de productieafdelingen en de andere organisatie-elementen van het JIVC te faciliteren. Verder maken de afdelingen Defensie Computer Emergency Response Team – Security Intelligence & Operations Center (DefCERT-SIOC), Informatiebeheer (IB), Kennis, Innovatie, Experimenten en Simulatie (KIXS) en IT Continuity Center (ITCC) deel uit van JIVC.

Fase 2 van de reorganisatie (in voorbereiding) is primair gericht op de aanpassingen om de samenwerking met het marktconsortium Athena (IBM, Atos en Unica) voor de grootschalige vernieuwing van de IT (Programma Grensverleggende IT, is GrIT) vorm te geven. In fase 2 vindt daarbij ook de doorontwikkeling van verschillende afdelingen plaats en worden ook nieuwe afdelingen

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

ingericht. Daarnaast vinden uitbreidingen plaats voor grote projecten en worden aanpassingen op basis van de evaluatie van fase 1 doorgevoerd.

Allemaal essentiële veranderingen om JIVC verder klaar te maken voor de toekomst. Het zorgt ervoor dat we nog beter kunnen leveren wat Defensie nodig heeft. Namelijk betrouwbare, veilige, toekomstbestendige en flexibele IT.

2. Het ministerie van Volksgezondheid, Welzijn Sport

Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is een divers ministerie met verschillende organisatieonderdelen. Naast het kerndepartement (beleidsdepartement) zijn er raden en commissies, agentschappen en een inspectie. Deze werken voor kantoorautomatisering veelal samen met Shared Service Organisaties van het Rijk. Dientengevolge maakt VWS gebruik van de rijksbrede dienstverlening en de hieraan verbonden applicaties. Indien dat niet mogelijk en/of doelmatig is, zoekt VWS naar standaardsoftware oplossingen die zo algemeen mogelijk binnen VWS worden ingezet. Voor de primaire taken van agentschappen en inspectie is meestal sprake van specifieke applicaties. VWS hanteert bij de inzet van alle soorten software de rijksbrede architectuurstandaarden (zie www.earonline.nl) en de Strategische I-agenda Rijksdienst.

De laatste jaren is het gebruik van SaaS-oplossingen, zowel voor webapplicaties als voor mobiele applicaties sterk in opmars. Belangrijk daarbij is dat gebruikers zo min mogelijk drempels ervaren bij een gebruikersvriendelijk, veilig en efficiënt gebruik van dit soort applicaties. Een goed werkende koppeling van en naar de door SSC-ICT beheerde ICT-omgeving is hierbij onontbeerlijk evenals de integratie met Office365 en MS-Teams, al dan niet via een rijkscloud-oplossing.

De komende jaren zal fors geïnvesteerd worden in het werken met data op basis van Microsoft Azure, het gebruik van analysetools zoals Python, R en R Studio en het gebruik van rapportagetools zoals Power BI. Voor informatievoorziening en verantwoording is ook de inzet van anonimiseer- en laktooling in opmars. Ten aanzien van de zaaksystemen op basis van IBM FileNet vindt er de komende periode bij VWS een herijking plaats, welke moet passen in de rijksbrede standaardisering en harmonisatie van DMS-systemen. Informatiebeveiliging (BIO), privacybescherming (AVG/GDPR), toegankelijkheid (WCAG), continuïteit en kwaliteit (ISO), open source en connectiviteit zijn uiteraard voor VWS van groot belang. Dit vraagt ex ante bewustzijn en toetsing bij ontwikkeling en gebruik van ict, maar ook tijdens het gebruik (zoals pentesten).

Het rijksbrede programma Open op Orde zal ook bij VWS intensivering van capaciteit en it-ontwikkeling vragen. Hierbij is ook de personele ontwikkeling, verbetering vakmanschap, een belangrijke pijler.

Voor algemene beschrijving zie: <https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport/inhoud/organisatie>

Hieronder volgt een nadere introductie van een aantal onder VWS ressorterende diensten en agentschappen die in het kader van deze Raamovereenkomst naar verwachting een grotere afnemer zullen zijn.

Het ministerie van VWS heeft naast het kerndepartement ook vele diensten en instellingen waarvan enkele verspreid zijn over Nederland. Toekomstige organisatiewijzigingen voorbehouden nemen de volgende VWS-onderdelen deel aan deze aanbesteding (in alfabetische volgorde):

- Bestuursdepartement, inclusief directoraten-generaal, directies en programmadirecties;
- CIBG;
- College ter Beoordeling van Geneesmiddelen (aCBG, inclusief agentschap);
- Centrale Commissie Mensgebonden Onderzoek (CCMO, inclusief secretariaat);
- Dienst Uitvoering Subsidies aan Instellingen (DUS-I);
- Eenheid Secretariaten Tuchtcolleges en Toetsingscommissies (ESTT);
- Gezondheidsraad (GR);
- Inspectie Gezondheidszorg en Jeugd (IGJ);
- Jeugdautoriteit (JA);
- Nederlandse Sportraad (NLSportraad);
- Raad voor Volksgezondheid en Samenleving (RVS);
- Rijksinstituut voor de Volksgezondheid en Milieu (RIVM);
- Sociaal en Cultureel Planbureau (SCP).

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Zelfstandige bestuursorganen met een eigen rechtspersoonlijkheid (zoals het NZa, CAK en ZonMw) nemen niet deel aan deze aanbesteding.

Voor de ICT-werkplekken en de bijbehorende kantoorautomatisering alsmede voor de hosting en housing van on-premise bedrijfsapplicaties maakt VWS gebruik van de dienstverlening van SSC-ICT van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en SSC Campus, gevestigd in Den Haag en Bilthoven. Voor specifieke bedrijfstoeepassingen wordt ook gebruik gemaakt van de dienstverlening van DICTU, gevestigd in Den Haag, Assen en Zwolle en van cloud-leveranciers (SaaS/PaaS e.d.).

3. Het ministerie van Buitenlandse zaken

Het ministerie van Buitenlandse Zaken (BZ) werkt in binnen- en buitenland voor de belangen van Nederland en Nederlanders. Door het leggen en onderhouden van de juiste verbindingen tussen mensen, informatie, overheden en organisaties leveren wij een bijdrage aan de veiligheid, welvaart en vrijheid in Nederland, in Europa en in de wereld. Met een compacte en moderne organisatie streven wij ernaar om de Nederlandse belangen optimaal te bedienen en flexibel in te spelen op de Nederlandse en mondiale ontwikkelingen. Wij opereren zowel vanuit het departement in Den Haag als vanuit ruim 150 ambassades, permanente vertegenwoordigingen, beroepsconsulaten en andere vertegenwoordigingen verspreid over de hele wereld (posten).

Het is de missie van het ministerie van Buitenlandse Zaken (BZ) om het Koninkrijk der Nederlanden veiliger en welvarender te maken en Nederlanders in het buitenland te steunen. Samen met onze partners zetten wij ons in voor een rechtvaardige wereld. Kernwaarden van het Ministerie zijn samenwerken, verantwoordelijkheid nemen en het behalen van resultaten.

Nederland is nauw verbonden met het buitenland. Daar hebben wij baat bij, onder meer in economisch opzicht. Echter, deze verbondenheid brengt ook risico's met zich mee, want wat ver weg gebeurt, raakt ons vaak ook dichtbij. Denk bijvoorbeeld aan terrorisme, vluchtelingenstromen en klimaatverandering. Door internationale samenwerking kunnen we zowel deze problemen aanpakken, als ook onze economie versterken.

Nederlandse overheidsinstellingen zijn doelwit van omvangrijke en hardnekkige digitale aanvallen. Deze aanvallen hebben spionage, beïnvloeding, sabotage of terrorisme als oogmerk. Zij vormen een omvangrijke en toenemende bedreiging voor de integriteit en de vertrouwelijkheid van de Nederlandse overheid. Ook digitale (spionage)aanvallen met een economisch motief zijn een bron van zorg. Dergelijke aanvallen vormen een bedreiging voor ons economisch verdienvermogen en het ongehinderd functioneren van het publieke leven en de vitale sectoren. De bovengenoemde internationale verbondenheid en plotselinge gebeurtenissen verhogen de noodzaak tot intensievere communicatie, hetgeen resulteert in een toenemende afhankelijkheid van de ICT-dienstverlening.

De *ambitie van BZ* is om toonaangevend te zijn in de diplomatie: een flexibele netwerkorganisatie, waarmee iedereen graag samenwerkt. Bijbehorende kernkwaliteiten zijn:

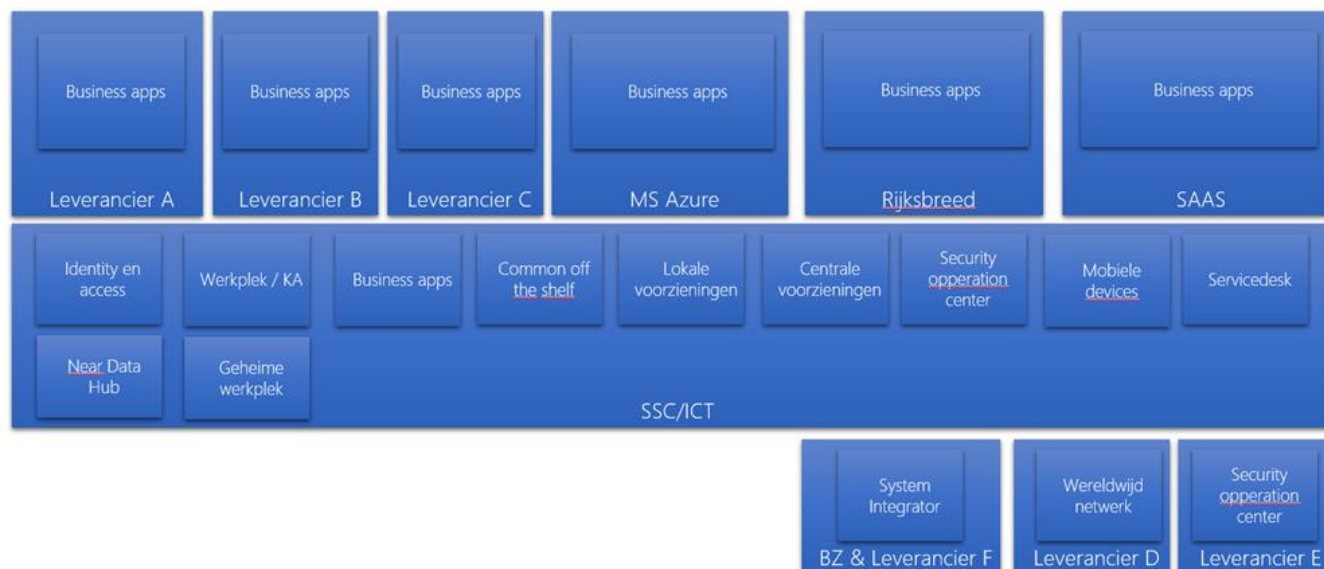
- Samenwerken: verbinden en dienstverlenend;
- Verantwoordelijkheid nemen: ondernemend en vernieuwend, integer en transparant;
- Resultaten behalen: kwaliteitsgericht, onderscheidend en zichtbaar.

Aansluitend op de Strategische iAgenda Rijksdienst 2019-2021 ondersteunt de Digitaliseringsvisie voor BZ 2019-2022 de primaire doelen en strategieën van BZ, waarin de prioritaire beleidsthema's zijn: veiligheid, welvaart, eerlijke en duurzame wereld, alsmede Nederlanders in het buitenland. Uitgangspunt is dat wij ons verder professionaliseren, de kansen van digitalisering optimaal benutten, de risico's ervan adequaat managen en daarbij ook aandacht hebben voor de ethische aspecten van digitalisering. Wij werken op digitaal gebied zoveel mogelijk samen met andere Rijksorganisaties en maakt waar mogelijk gebruik van Rijksbrede ICT-voorzieningen. Ook blijven wij de Rijksbrede I(CT)-ontwikkelingen voeden en meebesturen vanuit onze brugfunctie naar de internationale wereld.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Het ICT-landschap

De volledige ICT-uitvoering van BZ is uitbesteed. Globaal is dit onder te verdelen in de componenten genoemd in onderstaand figuur. Het applicatielandschap bestaat uit uiteenlopende oplossingen zoals volledige maatwerk oplossingen (veelal gebaseerd op de Microsoft stack), standaard pakketoplossingen, SaaS diensten en diensten die binnen de overheid generiek worden aangeboden. Dit alles is belegd bij meerdere commerciële en publieke partijen. Werkplekbeheer, inclusief aanverwante producten en diensten, is interdepartementaal ondergebracht bij het rijks shared service centrum SSC-ICT.



Ontwikkelingen op I(CT)-gebied zullen zich de komende jaren voornamelijk afspelen rond thema's als: digitale innovatie, e-dienstverlening, digitalisering van processen, plaats-, tijd- en apparaat onafhankelijk werken, digitaal samenwerken, clouddiensten en social media, informatiehuishouding, big data analyse en open data. De insteek daarbij is voornamelijk een functionele uitvraag van diensten en oplossingen. Bij al deze thema's dient rekening gehouden te worden met een internationaal speelveld en een 24/7-dienstverlening.

Onderstaande tabel geeft een nadere invulling van enkele bovenstaande thema's en de betrokken rollen.

Scope/ Organisatie onderdeel	Type werk	Type functionarissen*	Ontwikkelingen BZ
Centraal departementaal	Centrale I(CT)-regie	I-beleidsadviseurs, I-architecten, Business consultants, Portfoliomanagers, Service-integratie managers, Contractmanagers	Centrale I-organisatie BZ heeft een vaste kern met een flexibele schil. Na reorganisatie zal komend jaar het grootste deel van resterende vacatures worden vervuld met vast personeel. Flexibele schil is voor: tijdelijke taken, bijzondere / ontbrekende expertises, opvang van capaciteitsproblemen.
	Centrale I(CT)dienstverlening aan dienstonderdelen en posten	Functioneel beheerders, Businessanalisten, Informatieanalisten, Risicoanalisten, BI-consultants, Data scientists, Productowners, Data-engineers	Er is een klein intern team voor deze taken, naar behoefte aangevuld met externe inhuur voor aanvulling, vervanging, etc. Het verzorgingsgebied en de inzet van deze functionarissen is zich geleidelijk aan het uitbreiden.
	ICT- projectenportfolio BZ	Portfoliomanagers	BZ heeft jaarlijks een ICT- projectenportfolio van gemiddeld 50 projecten. Er is een klein intern team

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

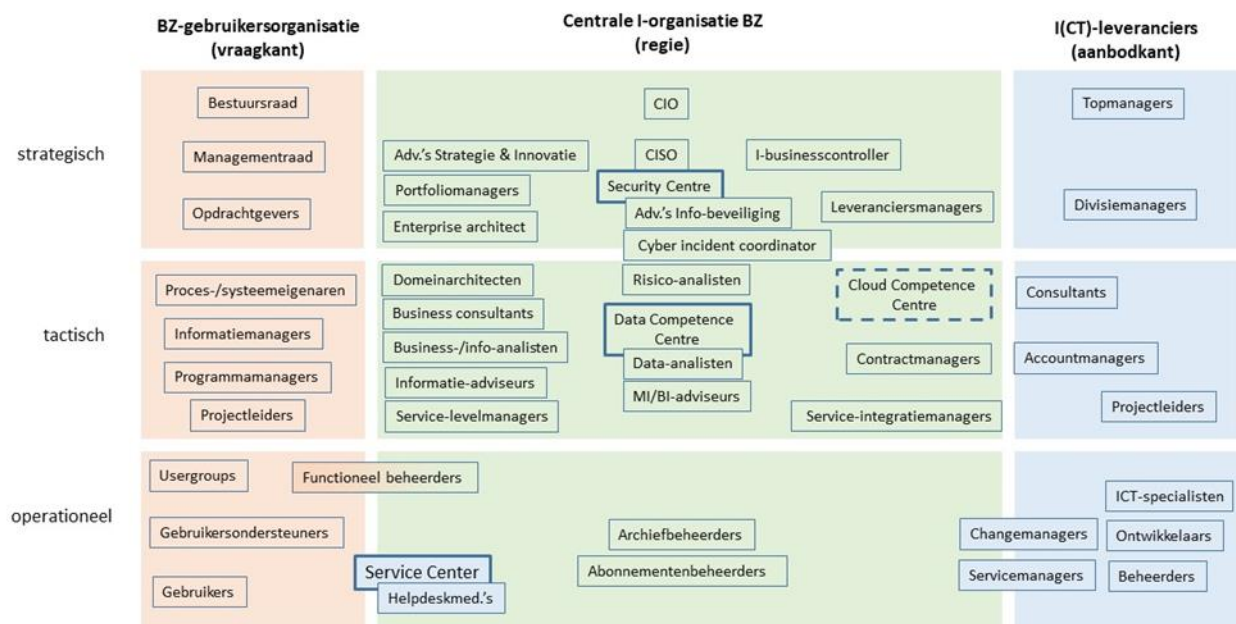
Scope/ Organisatie onderdeel	Type werk	Type functionarissen*	Ontwikkelingen BZ
		Projectleiders, Projectmedewerkers, Projectsecretarissen	van projectleiders. Overig projectmanagement wordt in beginsel vervuld met externe inhuur, de andere taken incidenteel.
	Ondersteuning van de corporate informatiehuishouding	I-adviseurs, Recordsmanagers, Architecten	De ondersteuning van de corporate informatiehuishouding, digitalisering van de informatiehuishouding en borging van de wettelijke verplichtingen rond de informatiehuishouding (archiefbeheer, transparantie van overheidsinformatie) is belegd bij een interne unit.
Decentraal bij dienstonderdelen	Ondersteuning van decentraal informatie-beleid en informatie-management	I-adviseurs, Business-analisten, Business- en informatiearchitect, Productowners, Functioneel beheerders	De business van BZ is zich aan het ontwikkelen naar formulering van decentraal informatiebeleid, professionalisering van informatiemanagement en vraagsturing op I(CT)-diensten. Er is een geleidelijke toename van initiatieven en activiteiten op dit gebied bij directies en posten in buitenland.
			Ondersteuning daarbij komt deels vanuit de centrale I-organisatie BZ, deels van externe inhuur.
	Uitvoering van projecten met een I(CT)component	Programma managers, Projectleiders, Projectmedewerkers, Projectsecretarissen	De I(CT)-afhankelijkheid in primaire BZ-processen wordt steeds groter. Een toenemend aantal directies en posten neemt zelf initiatieven tot decentrale projecten met een I(CT)component, zoals op gebied van e-diensten, kunstmatige intelligentie, data analyse, open data, CRM. Ondersteuning daarbij komt deels vanuit de centrale I-organisatie BZ, deels van externe inhuur.
Rijksbreed	Uitvoering van rijksbrede ICT-dienstverlening buitenland	n.n.b.	Sinds enkele jaren is shared service centrum 3W operationeel als aanbieder van rijksbrede generieke bedrijfsvoering diensten m.b.t. het buitenland, waaronder een aantal ICT-diensten. 3W is zich gaandeweg aan het professionaliseren. Het dienstenpakket groeit geleidelijk.

Opdrachtgever merkt op dat bovenstaande beschrijving een momentopname is en een inhuurbehoefte van deelnemende dienst op andere gebieden nadrukkelijk niet is uitgesloten.

Als aanvulling op bovenstaand geeft onderstaande plaatje een beeld van hoe vraag, regie en aanbod is georganiseerd binnen BZ.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Organisatie van de informatievoorziening BZ (I-governance BZ)



Als wereldwijd opererende organisatie is BZ sterk afhankelijk van goede informatievoorziening, communicatie en bijbehorende I(CT)-dienstverlening. In de ontwikkeling naar een moderne Nederlandse diplomatie is betrouwbare, transparante en duurzaam toegankelijke digitale informatievoorziening en -beheer onmisbaar.

Actuele thema's op dat gebied zijn:

- digitale innovatie
- open overheid
- e-dienstverlening
- optimalisering informatiehuishouding
- digitalisering van processen en informatie
- digitalisering in beleid
- plaats-, tijd- en apparaatonaafhankelijk werken
- digitaal samenwerken
- informatiegestuurd werken
- clouddiensten
- social media
- big data analyse
- open data.

Bovenstaande thema's komen bij BZ ook terug in de I(CT) strategie en digitaliseringsvisie. In onderstaande afbeelding wordt daarvan een overzicht gegeven.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

I(CT)-STRATEGIE BZ 2020-2022

Kennis verbreden en verdiepen/ Buitenlandbeleid is digitaal alert

- Kennis van nieuwe technologieën en digitalisering in het buitenlandbeleid

Digitale innovatie BZ

- Data Competence Center in huis
- Cloud experimentterruimte met minimale kaders
- Scheiding beheer en ontwikkel leveranciers
- Samenwerking met hoger onderwijs, onderzoeksinstituten

Modernisering van het ICT-fundament

- snelle wereldwijde netwerkverbindingen
- Cloud first met standaard cloudplatforms (workflow, case)
- beheerbaar applicatielandschap
- extra beveiligde werkplek voor staatsgeheim

ICT waar BZ-ers blij van worden

- Unified communications
- platform voor veilig digitaal samenwerken met externe partners
- Uitbreiding mobiele applicaties
- meertalige ICT-diensten
- ICT-diensten arbeidsbeperken

Beter zoeken en vinden

- zoekvaardige BZ-medewerkers
- BZ-zoekmachine

Open tenzij informatievoorziening

- integrale visie op informatiebeheer
- geclassificeerde BZ-informatie
- Geleidelijk aanpassing BZ-applicaties, starten met Office

Informatiehuishouding

- upgrade Sharepointplatform BZ
- 24/7 Fox vervangen
- automatische archivering
- archivering BZ-websites en e-mailverkeer
- duurzame toegankelijkheid 'by design'
- stimuleren van actieve openbaarmaking



Datascience BZ

- DataLab BZ bij het Data Competence Center BZ
- DataLake en datacatalogus voor hergebruik data
- data-ethiek 'by design'
- datavaardige BZ-medewerkers

Digitale zelfredzaamheid

- I-bevuste en digitaal vaardige BZ-medewerkers
- adequaat risicomanagement bij directies en posten
- Ingericht Securitylab BZ

Veilig over de digitale snelweg

- GRC (Governance, Risk, Compliance) tooling voor betere verantwoording
- weerbare ICT BZ door 'veilig by design'
- informatiebeveiliging op data-niveau
- gecompartmenteerde 'trust zones': vertrouwelijke info-on premise
- Scheiding EU-NATO: restricted informatie van NL-vertrouwelijke data

Robuuste en stabiele ICT middelen

- Gebruik standaarden uit de markt (Office 365)
- Verbeteren regie door monitoren katen

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)



Principes, normen en standaarden

De algemeen van toepassing zijnde principes, normen en standaarden zijn hieronder opgesomd en onderverdeeld in "wetten en regelgeving", "normen en standaarden" en "principes en richtlijnen". Deze vormen de basis voor het compliance beleid.

Wetten en regelgeving:

- AVG;
- Archiefwet;
- VIR;
- VIR-BI.
- ABBZ voor Applicatiediensten

Normen en standaarden:

- Baseline Informatiebeveiliging Overheid BIO
- Baseline informatiebeveiliging BZ 2018 (grotendeels gebaseerd is op de ISO 27001);
- Normenkader DigiD;
- Normenkader DigiNetwerk;
- NORA/EAR;
- (open) Overheidsstandaarden (Comply or Explain, <https://www.forumstandaardisatie.nl>).

Principes en richtlijnen:

- BZ Enterprise architectuur principes
- Werken onder architectuur.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Hard-/software en technologieën

Voor het huidige landschap worden onder andere onderstaande producten, hard- en software en technologieën ingezet:

De gebruikte ICT middelen

Categorie	Onderdeel
OS Platformen	Microsoft Windows
	Citrix
	RedHat Enterprise Linux
	Microsoft Active Directory / Azure AD
Applicatie platformen	Liferay Portal
	Microsoft Sharepoint Portal
	MS Dynamics
	MS SQL (Azure) Server
	SSP
	MZ Azure IaaS / PaaS componenten
Ontwikkelmethodieken	Agile/SCRUM/DevSecOps
	Waterval
Architectuur-, Test- en Beheer- methodieken/principes	ITIL, Togaf, Otap
Ontwikkeltools	Azure DevOps
	Visual studio
Overige tools	MS Office incl Visio & Project
	MAVIM Rules
	Planon
	SAP
	BlueDolphin
Programmeertalen	MS .NET-FRAMEWORK
	Xamarin
	Angular
	PHP, Java
	Datalab (Databricks, Python, MS-Flow, Data factory, Datalake)
	Management Informatie (Blob storage, Data factory, Datalake ,Tableau)
E-mail	Microsoft Exchange
	BlackBerry

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

4. Het ministerie van Sociale Zaken en Werkgelegenheid

Werk en bestaanszekerheid voor iedereen: samen werken voor samen leven. Het ministerie van Sociale Zaken en Werkgelegenheid (hierna te noemen: het ministerie van SZW) werkt aan eerlijk, gezond en veilig werk in Nederland. Iedereen moet de kans krijgen om mee te doen en zich te ontwikkelen. Mensen moeten zelf kunnen bijdragen aan hun eigen toekomst. Als het tegenzit zorgen we voor een vangnet, en als je met pensioen gaat voor een inkomen. Dat kan alleen in een land waar mensen er voor elkaar zijn.

De bewindslieden zijn onder meer verantwoordelijk voor het arbeidsmarktbeleid, inclusief migratie en vrij verkeer van werknemers, uitkeringen en re-integratie, inkomensbeleid, het combineren van arbeid en zorg, arbeidsomstandighedenbeleid en inspectie daarop.

Er werken ongeveer 3000 medewerkers bij het ministerie van SZW. Het ministerie bestaat uit stafdirecties, beleidsdirecties en uitvoerende onderdelen.

Deelnemende onderdelen

De deelnemende onderdelen zijn de onder het kerndepartement vallende organisatieonderdelen waaronder de Directie Organisatie, Bedrijfsvoering en Personeel (OBP), Directie Dienstverlening, Samenwerkingsverbanden en Uitvoering (DSU) en de Nederlandse Arbeidsinspectie (NLA). OBP verzorgt als centrale stafdirectie de ondersteuning van SZW op de terreinen personeel en organisatie, ICT, documentaire informatievoorziening, inkoop, facilitaire zaken en huisvesting. DSU is dé dienstverleningsdirectie van SZW en voert als opdrachtnemer diensten, opdrachten en regelingen uit voor inmiddels zeven departementen. Te denken valt aan de uitvoering van de coronasteunmaatregelen, zoals de tijdelijke Noodmaatregel Overbrugging Werkgelegenheid (NOW) en de Zorgbonus.

De NLA werkt aan eerlijk, gezond en veilig werk en bestaanszekerheid voor iedereen. Ze doet dit op basis van meldingen, risico- en omgevingsanalyses. Ze zet toezicht en opsporing in waar de meest hardnekkige problemen zitten en het effect het grootst is en werkt risicogericht en programma gestuurd.

Uitvoeringsinstanties als de Sociale Verzekeringsbank (SVB) en het Uitvoeringsinstituut Werknemersverzekeringen (UWV) zijn geen deelnemers in deze aanbesteding.

ICT

Het ministerie SZW en de Nederlandse Arbeidsinspectie sluiten zoveel mogelijk aan bij rijksbrede dienstverlening en hieraan verbonden applicaties (zoals P-Direkt), rijksbrede standaarden (zie www.earonline.nl) en de Strategische I-agenda Rijksdienst. Hiernaast maakt SZW gebruik van eigen applicaties (maatwerk/standaardsoftware). SZW maakt gebruik van de dienstverlening van SSC-ICT: een goede aansluiting op hieraan verbonden processen is van belang. Betrouwbaarheid en continuïteit vormt de basis voor onze informatievoorziening, prioriteiten voor de komende periode zitten o.a. op het gebied van sturen op ketens van uitvoerders, omgang met data en algoritmen, informatiebeveiliging en privacy en I-awareness.

Het ICT-landschap bij SZW is in de basis opgezet conform het DWR-concept van SSC-ICT. SSC-ICT host ook alle t/m DepV geclassificeerde applicaties die bij SZW in gebruik zijn.

Nederlandse Arbeidsinspectie

Vanuit een visie op informatie gestuurd werken wordt de informatievoorziening binnen de Nederlandse Arbeidsinspectie doorlopend doorontwikkeld en vernieuwd waar nodig. Daarnaast wordt steeds meer gebruik gemaakt van app's voor zowel de eigen medewerkers als voor de onder toezicht staande organisaties in Nederland.

De Nederlandse Arbeidsinspectie is een informatie intensieve organisatie. Dat begint bij het bepalen waar wij inspecteren. En als de inspecteur of rechercheur op locatie is, moet hij kunnen beschikken over de benodigde informatie of toegang tot bronnen waar deze informatie staat. En moeten gegevens eenvoudig geregistreerd en verwerkt kunnen worden om zo te komen tot een compleet dossier.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)

Verantwoordelijk voor het goed functioneren van de ICT-voorzieningen en de informatiebeveiliging is de afdeling Informatiemanagement en -voorziening (IMV) die bestaat uit ongeveer 42 medewerkers. De taakgebieden van IMV zijn.

- a. Beheer en rapportage over de ICT-projecten uit de IMV-portfolio en beheer/exploitatie van inspectie-specifieke systemen, inclusief budgetbeheer;
- b. Beheer en doorontwikkeling van bestaande systemen;
- c. Regie op leveranciers, externe partners en relatiemanagement Shared Services organisaties binnen de Overheid;
- d. Coördinatie op procesmanagement;
- e. Business Intelligence (BI): adviseren, ophalen, bewerken en presenteren van en over informatie voor stuur- en verantwoordingprocessen. En het leveren van data aan derden voor risico gestuurde processen;
- f. Service Desk: eerste aanspreekpunt voor eindgebruikers bij problemen met geautomatiseerde systemen van Inspectie SZW;
- g. Tactische advisering op het domein integrale veiligheid en privacy (AVG, WPG, VIR, VIR-BI, BIO, NKBR), uitvoering van de PDCA-cyclus en liaisonfunctie richting het kerndepartement.
- h. Concretiseren van (latente) functionele behoeften van organisatieonderdelen tot adviezen en oplossingen binnen de informatie- en applicatiearchitectuur;
- i. Adviseren van de vraagzijde van de informatievoorziening binnen de Nederlandse Arbeidsinspectie;
- j. Verzorgen van de verbinding tussen vraag en aanbod op operationeel en tactisch niveau.

De informatievoorziening bij de Nederlandse Arbeidsinspectie ondersteunt de primaire processen binnen Toezicht met twee maatwerk zaaksystemen (.net C#) aangevuld met services en standaardproducten voor het opstellen van bijvoorbeeld modelcorrespondentie en het koppelen van andere informatiesystemen en bronnen waaronder de basisregisters.

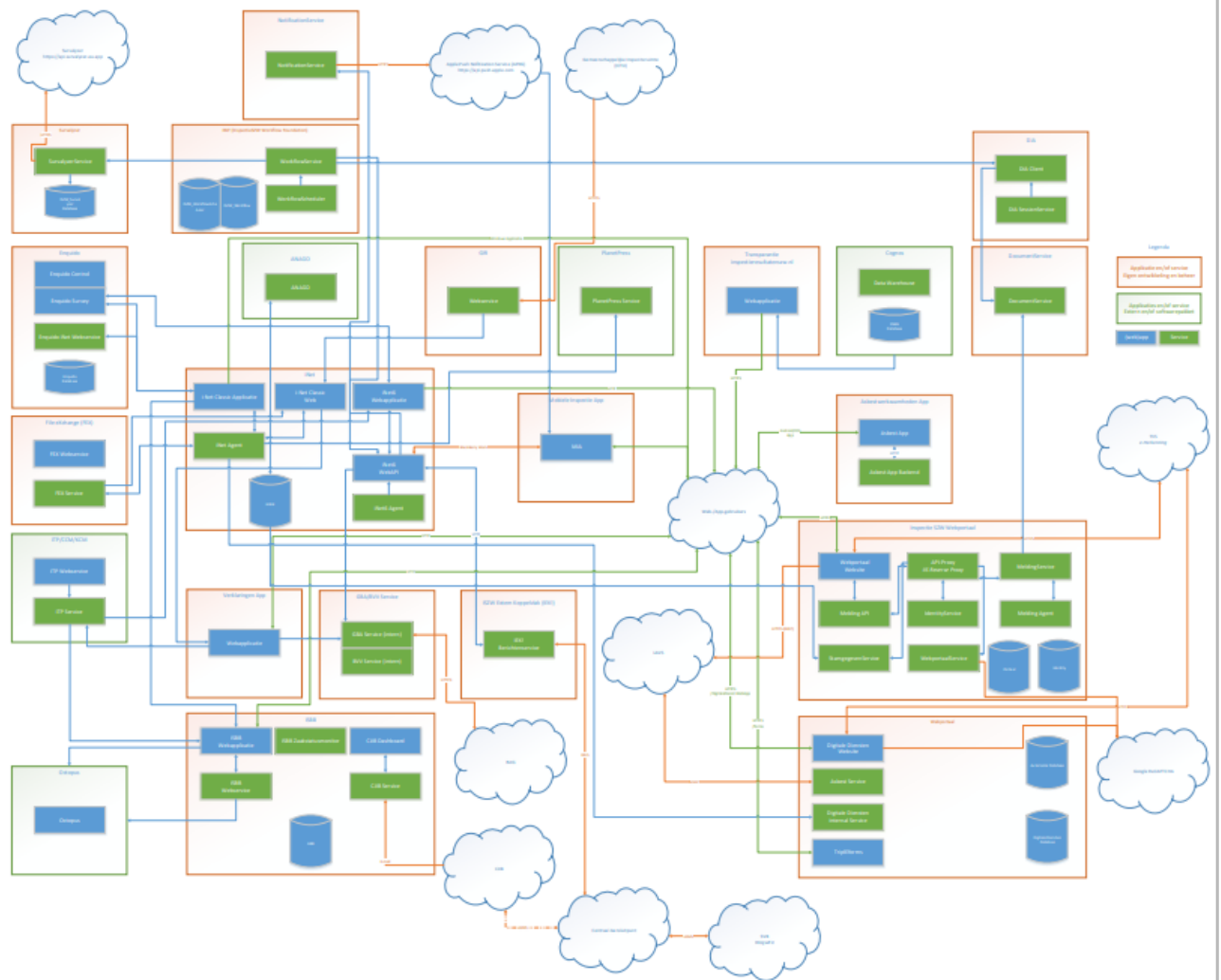
Binnen de directie Opsporing (recherche) wordt gebruik gemaakt van het zaakstelsel Summ-IT.

Een BI-omgeving (MS SQL DWH en Cognos BI) zorgt voor stuur- en verantwoordingsinformatie. Voor analyse wordt gebruikt gemaakt van standaardanalyse/ datascience producten als R-studio en SPSS, alsmede specialistische forensische software als i2 iBase SQL.

MS SharePoint wordt gebruikt als DMS / samenwerkingsruimte en voor onze kennisbank met gevalideerde informatie ondersteunend aan de processen. Procesbeschrijving zelf zijn vastgelegd in Mavim.

Ondersteuning aan gebruikers wordt geleverd door de servicedesk die gebruik maakt van Topdesk als service management systeem. In de bijgaande tekening is het applicatielandschap binnen Toezicht weergegeven.

Bijlage 3 Beschrijving ICT-organisatie en -landschap (Deelnemers)



Onze ambities voor 2022 en volgende jaren:

1. Uitvoering geven aan het ICT- beheer en –ontwikkelprogramma conform de goedgekeurde investeringsbegroting waaronder het aanpassen van het ICT landschap aan verandering in wet en regelgeving;
2. Participatie in de verschillende verbeterprogramma's bijvoorbeeld met betrekking tot meer werken onder architectuur en het implementeren van de e-overheid bouwstenen;
3. Verhogen van de wendbaarheid binnen het informatielandschap, het team en onze partners bijvoorbeeld het tijdig vervangen van verouderde (beperkende) techniek en aannemen en opleiden van nieuwe medewerkers.

Directie Dienstverlening, Samenwerkingsverbanden en Uitvoering

Onder DSU vallen het Leer- en Ontwikkelplein (LOP), het Financieel Dienstencentrum (FDC) en Uitvoering van Beleid (UVB; het voormalig Agentschap SZW). Het FDC voert de financiële administratie en het beheer van het financiële SAP 3F-systeem uit voor de ministeries van BZK, Financiën, OCW, SZW en VWS. Uitvoering Van Beleid (UVB) ondersteunt als uitvoeringsexpert binnen het sociaal domein beleidsdirecties bij het ontwikkelen, opzetten en uitvoeren van complexe opdrachten met politiek-bestuurlijke gevoeligheid, vooral op het terrein van werk, inkomen en migratie. UVB voert nationale en Europese regelingen en andere opdrachten uit voor met name het ministerie van SZW, maar ook voor het ministerie van JenV. Het Leer- en Ontwikkelplein is een samenwerking tussen OCW, SZW en VWS gericht op alle medewerkers van deze drie ministeries. Het leer- en ontwikkelaanbod is flexibel en voortdurend vernieuwend.

Voor algemene beschrijving zie: <https://www.rijksoverheid.nl/ministeries/ministerie-van-sociale-zaken-en-werkafelegenheid>