Strategische I-agenda Rijksdienst 2017

Inleiding

De Strategische I-agenda[1] Rijksdienst, die bij brief d.d. 2 december 2016[2] aan de Kamer is aangeboden, wordt elk jaar geactualiseerd. Voor u ligt de I-agenda voor 2017, samengesteld door de CIO Rijk in nauwe samenwerking met de leden van het CIO-beraad en de CTO-raad.

Deze actualisering van de Strategische I-agenda Rijksdienst toont de voortgang van de ingezette acties en geeft een aantal nieuwe accenten
De voorgaande I-strategie liep van 2012 tot 2015. Sindsdien is veel gebeurd. We noemen maar de start en uitvoering van het programma Digitaal 2017, het onderzoek van de commissie-Elias en de kabinetsreactie daarop, en de oprichting van het Nationaal Cyber Security Centrum. Ook in de EU vinden ontwikkelingen plaats met implicaties voor de rijksdienst, bijvoorbeeld op het gebied van digitalisering, informatiebeveiliging en privacy. Tegelijk blijven de technische mogelijkheden toenemen.

Onder de oude I-strategie (2012-2015) is veel bereikt, zoals het consolideren van datacenters, het consolideren van het aanbod in digitale werkplekken en het introduceren van de Rijkspas. Echter, nieuwe accenten zijn nodig. Waar de vorige I-strategie zich vooral richtte op de bedrijfsvoering, liet de commissie-Elias zien dat meer aandacht nodig is voor het primaire proces: beleidsontwikkeling en uitvoering, inclusief toezicht. Dat primaire proces zit vooral bij de individuele departementen, uitvoeringsorganisaties en zelfstandige bestuursorganen (zbo's); anderzijds zijn er gemeenschappelijke elementen, die we in deze I-agenda benoemen. Uiteindelijk is het doel een betere en transparantere dienstverlening voor burgers, bedrijven en instellingen.

Deze Strategische I-agenda Rijksdienst beoogt echter niet om de departementale meerjarige I-plannen en de daarmee beoogde verbetering van primaire processen samen te vatten. Deze I-agenda gaat in brede zin over de gemeenschappelijke elementen. De Strategische I-agenda Rijksdienst beoogt dus vooral voorwaardenscheppend en kaderstellend te zijn voor de departementale I-plannen, en de agenda te bepalen voor het delen van kennis en ervaring binnen het Rijk.

We hebben de ontwikkelingen buiten en binnen de rijksdienst bekeken; deze komen terug in deel I. De impact daarvan op de rijksdienst is significant.

Dat ICT een steeds grotere rol speelt in onze maatschappij en ook in de dienstverlening van de rijksdienst is een cliché, maar daarom niet minder waar. Hoeveel eenvoudiger is het nu bijvoorbeeld om met de vooraf ingevulde aangifte (VIA) belastingaangifte te doen. De commissie-Elias heeft echter overtuigend laten zien dat goede inzet van ICT niet eenvoudig is.

---

[1] In deze Strategische I-agenda bedoelen we met "I" het geheel van (vraagstukken rond) Informatievoorziening, de technische ICT-systemen die deze verzorgen, alsmede de functie(s) en organisatieonderdelen die beleid hierover maken en dat beleid realiseren, zowel binnen de primaire processen als in de bedrijfsvoering.
[2] Kamerstuk 31490, nr. 221

Visie
De rijksdienst streeft ernaar om optimaal gebruik te maken van ICT om burgers en bedrijven optimaal en betrouwbaar te bedienen en de rijksambtenaren efficiënt en effectief te laten werken. We gaan hierbij verstandig om met informatiebeveiliging, verzekeren business continuïteit zoveel mogelijk en beschermen privacy. We blijven innoveren en verbeteren, maar wel op een pragmatische en gecontroleerde wijze. De drang om risico's bij I-trajecten te mijden staat overigens soms op gespannen voet met de noodzaak tot innovatie. Uitgangspunt is: risico's mijden als het moet, innoveren als het kan.

In de vorige versie van de I-agenda is uiteengezet dat wij bij voorkeur werken in kleine stappen die snel resultaat leveren. De Studiegroep Informatiesamenleving en Overheid[3] onderschrijft dat en stelt dat digitale toepassingen per definitie nooit af zijn en het principe 'first time right' overboord moet. Digitaal is volgens de Studiegroep 'permanent bèta', iteratief, experimenteren moet, en fouten zijn een opmaat naar een volgende release.

We kiezen bij kritische trajecten bij voorkeur voor gangbare en bewezen technologie; de rijksdienst is dan een trendvolger op gebied van ICT. We zetten interne en externe partijen hierbij optimaal in. Bij gelijke geschiktheid geven we de voorkeur aan open source oplossingen. We stimuleren innovatie om nieuwe vormen van dienstverlening te realiseren, en met kleinschalige en minder kritische trajecten. Innovatie, van fouten leren en trajecten stoppen horen immers bij elkaar. Sturing op samenhang en helderheid over te realiseren baten zijn ook daarbij aan de orde. Innoveren vraagt om nieuwe manieren van planning en control, niet om het volledig afschaffen daarvan. Ruimte voor experimenteren en fouten mag niet leiden tot minder vertrouwen in (de diensten van) het Rijk of in de stabiliteit van die diensten zelf. De verantwoordelijkheid voor de ontwikkeling van voorzieningen en het daarover verantwoording afleggen moeten daarom helder geregeld blijven.

De rijksdienst is een complexe organisatie, met veel onderdelen die specialist zijn in hun specifieke taak. Die diversiteit aan expertise op deelterreinen is een grote kracht van de rijksdienst. ICT moet deze onderdelen optimaal ondersteunen: wendbaar, efficiënt en optimaal berekend op hun taak.

Daarom is het uitgangspunt "managed diversity": departementen zijn verantwoordelijk voor het primaire proces met de daarbij behorende ondersteuning, waarbij voldaan moet worden aan een set van interoperabiliteits- en veiligheidskaders om samenwerking eenvoudig te maken. Beslissingen over de inrichting van gegevensstromen over departementen heen en over de ondersteunende rijksbrede ICT worden zoveel mogelijk in samenhang genomen. Wij kiezen, zoals ook de Studiegroep bepleit, voor focus op een samenhangende infrastructuur en dienstverlening. Standaardisatie en harmonisatie zijn daarmee middelen, geen doelen op zichzelf.

De vijf thema's
Op basis van de ontwikkelingen en de visie komen we tot vijf belangrijke thema's voor de I-agenda in deze planperiode:

1. **Versterking van de I-functie, "I in het hart van beleid"**: het belangrijkste thema om de visie te realiseren, als voortzetting op de kabinetsreactie op het

[3] Kamerstuk 26643, nr. 460

Eindrapport van de Tijdelijke commissie ICT-projecten Dit betekent dus ook het versterken van de positie van en aandacht voor "I" in het primaire proces, met name vroeg in de beleidscyclus en tegelijkertijd als gesprekspartner van de uitvoeringsorganisaties.

2. **Digitalisering van primaire processen:** deze I-agenda omvat heel "I", inclusief het primaire proces. Digitalisering van gegevensstromen in ketens met actoren binnen en buiten de overheid zet door. Met deze toename wordt het spanningsveld met bescherming van privacy ook een steeds grotere uitdaging. Departementen zullen hiertoe moeten samenwerken. De rijksdienst zal optimaal gebruik maken van de voorzieningen van de Generieke Digitale Infrastructuur (GDI).
3. **Eén concern, de rijksdienst als "connected enterprise"**: voortbouwen op het grondwerk van de compacte rijksdienst en SGO5[4] om samenhang en effectiviteit van de rijksdienst te versterken. Geen focus op verdere centralisatie van voorzieningen, maar wel aandacht voor regie op de interne ICT-dienstverleners, de kwaliteit en prijs van de dienstverlening en op samenhang en interoperabiliteit van systemen en processen. Aandacht voor ketens en architectuur.
4. **Verstandige aandacht voor informatiebeveiliging, continuïteit en privacy**: het vinden van de juiste balans tussen optimale bescherming van informatie van het Rijk, zeker stellen van continuïteit van dienstverlening, bescherming van de privacy van burgers, en ruimte voor de rijksdienst om haar taken goed en efficiënt uit te voeren.
5. **"Zaken voor elkaar krijgen" door optimale inzet van interne en externe leveranciers**: in het Regeerakkoord is afgesproken dat voortvarender dan voorheen beslist zal worden welke producten en diensten het Rijk zelf ontwikkelt en welke het door marktpartijen laat ontwikkelen. Wij zullen daarvoor een handreiking ontwikkelen.
   Wij zullen optimaal gebruik maken van marktpartijen, onder andere door een heldere en ten dele nieuwe handreiking voor het al dan niet inzetten van oplossingen, door versterking van het strategisch leveranciersmanagement, innovaties en infrastructuur van de markt; samenwerking met de markt die een goede balans vindt tussen open communicatie en van elkaar leren als het kan, en professioneel en hard zakendoen als het moet. Voor zover het Rijk taken in het I-domein zelf uitvoert streven wij naar een heldere organisatie en taakverdeling van interne dienstverleners, en verdere professionalisering.

De vijf thema's worden uitgebreid beschreven in deel II.

=====

Deze Strategische I-agenda Rijksdienst wordt uitgewerkt en geconcretiseerd in de I-strategieën en jaarplannen van de departementen en in de jaarplannen voor 2018 van het CIO-beraad en de CTO-raad. Hoewel de Strategische I-agenda vanaf 2017 een periode van 3 jaar bestrijkt hoeft u niet drie jaar te wachten op een nieuwe. I(CT) is dynamisch en we willen steeds snel in kunnen spelen op veranderingen, in kleine stappen ("agile"). Daarom

[4] SGO-5: Programma Herinrichting Governance Bedrijfsvoering Rijk

zullen we deze agenda in 2018 opnieuw actualiseren, in lijn met de cyclus van de departementale I-plannen.

Deel I: Ontwikkelingen

1. Ontwikkelingen buiten de Nederlandse overheid

Technologische en maatschappelijke trends en ontwikkelingen in de private sector en in de EU hebben directe impact op "I" binnen de Nederlandse overheid, inclusief de rijksdienst. Zowel op bedrijfsvoering als op het primaire proces. De rol van "I" verschuift van kostenpost steeds verder door naar motor van het primaire proces.

Technologische ontwikkelingen
Een aantal trends is rijksbreed relevant en blijft dit ook de komende planperiode (zie H2 en H3, deel II). Hieronder vallen bijvoorbeeld digitalisering van dienstverlening, mobiel werken en inzet van cloud-technologieën. Daarnaast komt steeds meer informatie vaak real-time voor steeds meer mensen beschikbaar. Dat heeft grote impact op de manier waarop we samenleven en werken. We zijn als samenleving, als overheid en als rijksdienst volop bezig om daar mee om te leren gaan.

Andere trends zijn zeker relevant voor individuele departementen, maar zult u in deze rijksbrede strategische I-agenda niet tegenkomen, zoals Internet-of-things, mesh of devices, blockchain technologieën, artificial intelligence, robotisering, self-driving cars, smart city.[5] Voor uitgebreide achtergrond over deze trends verwijzen wij naar beschikbare analyses uit de markt, zoals "The global forces breaking all the trends" (McKinsey, 2015), "Technology Vision 2016" (Accenture, 2016), "Top Ten Technology Trends for 2016" (Gartner, 2016). In I-plannen voor departementen zullen deze technologische ontwikkelingen daar waar relevant aan bod komen, zoals self-driving cars en Internet-of-Things bij het Ministerie van Infrastructuur en Milieu en blockchain bij het Ministerie van Financiën.

Maatschappelijke ontwikkelingen en dilemma's
De verwachtingen van de maatschappij ten aanzien van digitale dienstverlening zijn toegenomen. De overheid zet dan ook steeds verder in op digitalisering (zie volgend hoofdstuk en H2, deel II). De samenleving is echter niet homogeen. Voor de huidige jonge generatie is de mobiele toepassing van I in vele apparaten vanzelfsprekend. Echter, velen hechten ook aan niet-digitale dienstverlening. Laaggeletterden komen relatief op meer achterstand als geen rekening met hen wordt gehouden bij digitalisering. De groep van 65-plus groeit fors en vereist specifieke aandacht bij inzet van digitale middelen. Ook andere groepen vragen om dienstverlening via niet digitale kanalen of om een combinatie van kanalen. Daarnaast worden er regelmatig zorgen over privacy geuit, terwijl tegelijkertijd de vraag naar transparantie en open data groeit. Omgang met deze dilemma's komt deze planperiode dan ook aan de orde. Informatieveiligheid vraagt om steeds meer aandacht. Ransomware aanvallen zoals WannaCry zorgen wereldwijd voor grote problemen.

[5] Voor uitleg over deze begrippen verwijzen wij naar online artikelen, zoals een artikel van het World Economic Forum over Internet of Things, https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/, 27 november 2015

Ontwikkelingen private sector
De rijksdienst kan als trendvolger leren van ontwikkelingen in de markt en hier optimaal gebruik van maken. Dit is dan ook een thema voor deze planperiode. Enkele relevante ontwikkelingen zijn:

- Organisaties zoals Royal Dutch Shell zetten ICT heel bewust in om hun processen, mensen en ideeën met elkaar en met de buitenwereld te verbinden ("connected enterprise").
- Veel grote bedrijven kiezen ervoor om hun ICT-infrastructuur onder te brengen in de "clouds" van bedrijven als Amazon Web Services, Google en Microsoft.
  De markt voor cloud-infrastructuur ("IaaS") wordt sterk gedomineerd door Amerikaanse bedrijven. Dat is ook het geval, zij het in mindere mate, voor zogenoemde "SaaS", Software as a Service: software die als dienst wordt aangeboden en niet meer "draait" op de infrastructuur van de gebruiker.
- Het gebruik van SaaS-producten neemt nog steeds sterk toe, niet alleen in de consumentenmarkt, maar ook steeds meer in de zakelijke markt. Ook leveranciers van ERP-software als SAP en Oracle bieden hun producten steeds vaker aan als SaaS-oplossing.

Ontwikkelingen in de Europese Unie (EU)
In de EU zijn ook ontwikkelingen die impact hebben op overheidsbrede I-ontwikkelingen zoals genoemd in het volgende hoofdstuk en op digitalisering, informatiebeveiliging en privacy binnen de rijksdienst (zie deel II):

- De EU investeert sterk in innovatie. Horizon 2020 is bijvoorbeeld het grootste onderzoeks- en innovatieprogramma van de EU met bijna €80 miljard aan budget voor de komende zeven jaar. Tegelijk investeert de EU in de digitale economie via het programma Connecting Europe Facility (CEF) en met trans-Europese digitale services voor burgers, bedrijven en overheden. In april 2016 is het eGovernment Action Plan 2016-2020 gepubliceerd, met onder andere als doel om digitale barrières tussen EU-landen weg te nemen. Daarnaast wordt een Europese richtlijn voor toegankelijke overheidswebsites opgesteld: een standaard die moet worden gebruikt bij ontwikkeling en beheer van websites en mobiele applicaties, zodat ook mensen met een functionele of cognitieve beperking deze kunnen gebruiken. Deze richtlijn is van belang bij verdere digitalisering binnen de rijksdienst.
- In Europees verband wordt gewerkt aan vernieuwing van het European Interopability Framework (EIF). Van belang is dat Nederland goed aangesloten blijft en input levert op de ontwikkeling van Europese standaarden met het oog op verbetering van interoperabiliteit.
- In Europa neemt de zorg om de privacy van de burger toe. Per 25 mei 2018 vervangt de nieuwe European Data Protection Regulation, in Nederland de Algemene Verordening Gegevensbescherming (AVG), de Wet Bescherming Persoonsgegevens (WBP). Het onderwerp privacy komt dan ook aan de orde in deze planperiode.
- Aandacht voor cybersecurity neemt sterk toe. Deze ontwikkeling wordt versterkt door recente ontwikkelingen zoals de "hack" van informatie van meer dan 20 miljoen personen bij "The United States Office of Personnel Management" en het data-lek bij de Filipijnse verkiezingscommissie, waarbij gegevens van zo'n 55 miljoen Filipijnen gelekt zijn. De Europese Raad en het Europese Parlement hebben akkoord

gegeven op maatregelen om het niveau van cybersecurity in de EU te verhogen[6]. Dit heeft gevolgen voor cybersecurity binnen de rijksdienst (zie ook NCSC hierna).

2. Overheidsbrede ontwikkelingen in Nederland

Tijdens de planperiode van de vorige I-strategie (2012-2015) heeft een aantal overheidsbrede ontwikkelingen plaatsgevonden met invloed op "I" binnen de rijksdienst. Door decentralisatie van diensten naar gemeenten was het noodzakelijk om een aantal (keten-) processen te herzien. Ook heeft de overheid met "Digitaal 2017" een heldere ambitie uitgesproken om die processen versneld te digitaliseren. Met de Generieke Digitale Infrastructuur (GDI) beoogt de overheid digitalisering op een veilige manier verder te versnellen. Tenslotte is het Nationaal Cyber Security Centrum ingesteld, wat geleid heeft tot meer aandacht voor het onderwerp cybersecurity.

Decentralisaties
Met de decentralisatie van bijvoorbeeld Jeugdzorg en de WMO is een belangrijke verantwoordelijkheid van de rijksdienst naar gemeenten verplaatst. Door de decentralisaties zijn verantwoordelijkheden binnen ketens verschoven. Dit vergroot het belang van standaardkoppelvlakken met organisaties buiten de rijksdienst.

Digitaal 2017 en Generieke Digitale Infrastructuur
In 2013 is de visie-brief voor de digitale overheid in 2017 aan de Kamer gestuurd. De ambitie is: alle zaken met de overheid digitaal en de overheid opereert als één. Dit heeft significante impact op het primaire proces van departementen, met name in de uitvoering. Sindsdien is de Generieke Digitale Infrastructuur (GDI) gedefinieerd, met componenten als:

- Uitbreiding van authenticatie, bijvoorbeeld mogelijkheden voor burgers en bedrijven met behulp van eID en eHerkenning, maar ook blijvende aandacht voor Digid (12,2 miljoen actieve accounts eind 2015).
- Digitalisering van dienstverlening, zoals Overheid.nl, Digitaal ondernemersplein, Antwoord voor Bedrijven, Mijnoverheid, Berichtenbox burger en bedrijven, MijnOverheid voor Ondernemers, eFacturen.
- Standaardisatie van gegevens (de basisregistraties) en bevordering van interoperabiliteit overheidsbreed.
- Verbeterde interconnectiviteit en beveiliging, voortgezet met de Wet Generieke Digitale Infrastructuur (WGDI).

Daarnaast is in 2014 voor een periode van vier jaar de Digicommissaris benoemd, met als doel "het realiseren van een solide en toekomstbestendige digitale overheid". De Digicommissaris heeft zich met name gericht op de governance en financiering van de Generieke Digitale Infrastructuur.
De ontwikkeling van GDI zelf is geen onderdeel van deze strategische I-agenda. Echter, de verbinding met en aansluiting van de rijksdienst op de GDI wel. Het implementeren van Digitaal 2017 en de GDI is een forse operatie voor elk departement.

Nationaal Cyber Security Centrum (NCSC)
Het NCSC is opgericht met als doel een veilig, betrouwbaar en veerkrachtig digitaal domein te realiseren. Het NCSC heeft een nationale scope. Het NCSC werkt inmiddels intensief

[6] Zie "Network and Information Security (NIS) Directive", https://ec.europa.eu/

samen met de ICT-dienstverleners binnen het Rijk.

3. Ontwikkelingen en huidige situatie I binnen de rijksdienst

In 2011 is de I-strategie voor de planperiode 2012-2015 ontwikkeld. Deze I-strategie bestond, op basis van een drietal streefbeelden, uit zeven thema's en vijfentwintig maatregelen, waarover in de jaarrapportages bedrijfsvoering Rijk jaarlijks is gerapporteerd. De I-strategie was sterk gericht op de bedrijfsvoering en heeft de samenhang en efficiëntie van de rijksdienst ontegenzeggelijk vergroot.

Tijdens de planperiode heeft de commissie-Elias echter geconcludeerd dat de rijksoverheid haar ICT-projecten niet onder controle heeft. Met name tekortkomingen in de positie van de I-functie kwamen hierin naar voren, zoals het gebrek aan lerend vermogen en onprofessioneel contractmanagement. De commissie maakte duidelijk dat meer aandacht nodig is voor de "I" in het primaire proces. Op 30 januari 2015 heeft het kabinet een reactie gegeven op het Eindrapport van de Tijdelijke Commissie. Naar aanleiding hiervan is in 2015 het Bureau ICT-toetsing (BIT) opgezet. Bij brief d.d. 24 maart 2017[7] is de vierde en laatste rapportage over de uitvoering van de kabinetsreactie aan de Kamer aangeboden.
Zoals in deze rapportage gesteld zijn alle maatregelen uit de kabinetsreactie uitgevoerd, maar zal beheersing van ICT-projecten voortdurend aandacht blijven vergen. Daarom was en blijft de versterking van de I-functie een belangrijk onderdeel van de nieuwe Strategische I-agenda Rijksdienst.

In deze geactualiseerde I-agenda is de thematische indeling van de vorige versie, uit 2016, niet aangepast. De thema's en dilemma's uit de vorige I-agenda zijn nog steeds actueel: ambitie versus beheerste stappen; de arbeidsmarktproblematiek, innoveren versus minimaliseren van risico's; inzetten op data-analyse en verder digitaliseren van ketens versus privacy van burgers; centraliseren uit efficiëntie oogpunt versus decentraliseren uit flexibiliteitsoverwegingen; verscherpen van veiligheidseisen voor rijksambtenaren versus de factor mens; intern leveren van diensten versus externe inzet. In de volgende hoofdstukken is een aantal thema's verder uitgewerkt.

[7] Kamerstuk 26643, nr. 454

Deel II: De vijf thema's van deze strategische I-agenda

1. Versterking van de I-functie: "I in het hart van beleid"

De WRR schrijft in het rapport iOverheid van 2011: "Het 'technovertrouwen' van politiek en beleid vertaalt zich in grote ambities met ict, niet alleen in technische, maar zeker ook in beleidsinhoudelijke zin." Dit gaf toen al aan waarom versterking van de I-functie noodzakelijk is. In het eindrapport van de Tijdelijke commissie ICT (commissie Elias) is ook geconstateerd dat verdere stappen nodig zijn.

Het kabinet heeft in februari 2015 een groot aantal maatregelen in gang gezet om de ontwikkeling van ICT bij het Rijk beheersbaarder en transparanter te maken, met de oprichting van het Bureau ICT Toetsing (BIT)[8] als meest in het oog springende maatregel. Dit geheel van maatregelen wordt ook wel aangeduid met de naam Operatie Informatiebestel Rijk (OIR).

Deze planperiode zal er grote aandacht blijven voor het versterken van de I-functie zelf. Wij zullen de naam OIR hiervoor blijven gebruiken. Dit is een lange, meerjarige, operatie. Het gaat hierbij om de versterking van de positie van de departementale CIO's en hun offices, om het vergroten van bewustzijn van ICT-gerelateerde uitvoeringsvraagstukken bij beleidsmakers, en zeker ook om het werven en opleiden van goede mensen om de I-functie te versterken. Deze onderwerpen werken we hieronder nader uit.

Verstevigen van de positie van departementale CIO's en hun CIO-offices.
Traditioneel hebben CIO's bij de rijksdienst vooral een controlerende taak ("countervailing power"). Voor een beheerste ontwikkeling van "I" binnen een departement zullen zij de rol van gesprekspartner voor beleidsontwikkeling en -uitvoering moeten versterken, waartoe zij ook vertrouwen moeten winnen. Het is hiervoor nodig om hun kennis en vaardigheden te versterken, leidend tot verbetering van de impact van CIO-oordelen. Om als volwaardig gesprekspartner voor beleid en uitvoering te kunnen fungeren moeten de CIO's, ook die van de uitvoeringsorganisaties, de middelen hebben om te kunnen leren van ervaringen elders. Die kennis moet op een effectieve manier, en bovendien vroeg in de departementale besluitvormingsprocessen, kunnen worden ingebracht. Wij zullen een Kennisbank inrichten om documentatie, kennis en ervaringen uit ICT-projecten onderling te delen. De bij het BIT opgedane kennis maakt daar onderdeel van uit. Door versterking van de kennis en kunde en daarmee ook van de positie van de departementale CIO's en hun CIO-offices moet het BIT op termijn overbodig kunnen worden.

In de vorige versie van de I-agenda is aangekondigd dat wij zullen bezien of het zinvol is om de taken, verantwoordelijkheden en bevoegdheden van de departementale CIO en diens office te formaliseren in een besluit, zoals dat ook bestaat voor de departementale directeur FEZ. Hierbij moet wel bedacht worden dat de positie van de directeur FEZ niet één op één vergelijkbaar is met die van de departementale CIO. De positie van de directeur FEZ is immers verbonden aan de begrotingscyclus en de organisatie daarvan. De cyclus in het I-domein is vooralsnog minder concreet ingericht en kent een andere dynamiek en inhoud dan de begrotingscyclus.

[8] BIT toetst projecten en adviseert over deze projecten aan de departementen, die zelf verantwoordelijk zijn voor de goede beheersing ervan.

In de vorige versie van de Strategische I-agenda is vastgelegd dat de ministeries meerjarige I-plannen zullen ontwikkelen. Het CIO-beraad zal een proces inrichten waarin afspraken worden gemaakt over de inhoud van de departementale I-plannen en verantwoording daarover en zal bezien hoe deze plannen geïntegreerd kunnen worden in de departementale beleids- en begrotingscyclus. Daarbij zal worden aangesloten op de notie dat ontwikkeling in kleine stappen mogelijk is, en dat het principe “first-time right” zoveel mogelijk overboord wordt gezet. Dat doet ook recht aan de complexiteit van ICT en de invloed van ICT op de beleidsprocessen.

Versterken van I-bewustzijn en -vaardigheden bij beleidsmakers
Het versterken van I-bewustzijn bij beleidsmakers gaat om het vergroten van het besef van uitvoerings- en ICT-consequenties, om het leren stellen van de juiste vragen en om uitvoeringsorganisaties en “I” vroegtijdig te betrekken. Het gaat ook om het versterken van data-gedreven beleidsvorming en uitvoering, wat betekent dat extra kennis en vaardigheden nodig zijn. Dit betekent onder andere een voorzetting en uitbreiding van bestaande curricula voor beleidsmedewerkers, leidinggevenden en opdrachtgevers van projecten, waarbij onderzocht wordt of curricula verplicht gesteld kunnen worden. Voorzien wordt een aanpassing van de kernprofielen van topmanagers in de rijksdienst op kennis en begrip van digitale ontwikkelingen.
Een kwartiermaker is gestart met de uitvoering van de aanbeveling van de Studiegroep om een nieuwe ICT-opleidingsvoorziening in te richten, analoog aan de Rijksacademie voor Financiën en Bedrijfsvoering, met de werktitel RADIO (Rijksacademie voor Digitalisering en Informatisering Overheid).

“Agile” manier van werken
Bij het versterken van I-bewustzijn en -vaardigheden hoort ook een manier van werken, met “I” projecten die meer uitgaat van kleine stappen (‘agile’). Meer kleinere en kortdurende projecten met heldere doelen en kleine teams, en minder grote meerjarige projecten.

Wij streven er daarmee naar om meer en meer over te gaan op kort-cyclisch ontwikkelen van diensten en systemen, zodat deze sneller beschikbaar komen voor burgers en bedrijven en ook sneller in de praktijk kunnen worden getoetst. Bij innovatie wordt gewerkt met een mix van experts, inclusief een beleidsmaker. Dit vergroot wendbaarheid en innovatiekracht. We weten immers niet precies wat technologie ons over vijf tot tien jaar brengt, noch hoe behoeften van burgers en bedrijven zich ontwikkelen.
De traditionele manier van planning en control sluit niet goed aan bij de noodzaak om op een iteratieve manier te kunnen werken. Echter een zeker mate van P&C blijft nodig om te kunnen sturen op samenhang en helderheid te kunnen bieden over te realiseren baten. Innoveren en ‘agile’ werken moeten niet gepaard gaan met het volledig weglaten van planning en control. Ruimte voor experimenteren en het maken van fouten mogen niet tot minder vertrouwen leiden in (de diensten van) het Rijk of in de stabiliteit van die diensten zelf. De verantwoordelijkheid voor en het verantwoording afleggen over de ontwikkeling van voorzieningen moeten daarom helder geregeld blijven. We zullen actief ruimte zoeken voor innovatie en experiment, en tegelijkertijd werken aan een control-framework dat zowel recht doet aan een ‘agile’ manier van werken als aan de behoefte aan planning en control.

Vergroten van aandacht voor I-aspecten in formele processen
Het Integraal Afwegingskader (IAK) is aangepast, zodat ICT-consequenties van voorstellen

prominenter en expliciet in beeld worden gebracht. De effectieve inzet van het IAK zal worden gestimuleerd.

Versterken van de positie van het Rijk als ICT-werkgever
Het bovenstaande kan niet zonder goede mensen, zowel op de ministeries, dicht bij de beleidsmakers, als in de uitvoering. Dit is ook in de eerdergenoemde kabinetsreactie van januari 2015 op het Eindrapport van de Tijdelijke commissie ICT aangegeven. Echter, de bezetting van I-functies binnen de rijksdienst is een uitdaging, zowel vanwege schaarste op de markt als vanwege de vergrijzing bij de rijksdienst.
De urgentie voor het versterken van de positie van het Rijk als ICT-werkgever is groot.
De belangrijkste aanleiding hiervoor zijn de (geprognosticeerde) tekorten aan eigen ICT-personeel bij het Rijk (met name op hbo- en wo-niveau) en de afhankelijkheid van externe inhuur. Deze tekorten zijn in algemene zin het grootst voor ontwikkelaars, ICT inkopers, data-analisten en IT security specialisten, maar over de gehele linie bestaat een krappe arbeidsmarkt.

De tekorten staan niet op zichzelf. Het Rijk opereert in een overspannen vraagmarkt, waarin de concurrentieslag voor ICT'ers in volle gang is en verder wordt versterkt door:

- Toenemende vervlechting van ICT en toenemende relevantie van ICT-competenties in het primaire proces van het Rijk. Dit vraagt om een nadrukkelijker inspanning en betrokkenheid van de CIO-offices op het terrein van (meerjarige) personeelsplanning van ICT'ers.
- Het Rijk heeft te maken met een tamelijk vergrijsde (ICT) populatie, zeker in vergelijking met het landelijke beeld. Er zullen dus niet alleen ervaren ICT'ers moeten worden aangetrokken om aan de verwachte vervangingsvraag te kunnen voldoen, maar ook voldoende aan de starterskant worden gerekruteerd om de vervanging vanwege interne doorstroom van ICT'ers aan te vullen en tegemoet te komen aan de uitbreidingsvraag van specifieke disciplines als bijvoorbeeld data science en IT security. Het in 2016 gestarte Rijks ICT Traineeprogramma (RITP) en het onderzoeken van de mogelijkheden om een rijksbreed Data Science traineeship op te zetten, dragen hieraan bij.
- .

Niet alleen het aantrekken van voldoende I-personeel, maar ook het bieden van een adequaat ontwikkelperspectief voor ICT 'ers wordt belangrijker, met daarin mogelijkheden voor continue (bij)scholing van relevante ICT-kennis en kunde.

We gaan op zoek naar mogelijkheden om werving en ontwikkeling van ICT-talent te versterken. Hieraan wordt al gewerkt, bijvoorbeeld door verdubbeling van de pool van I-interim Rijk.
Om tot rijksbrede en structurele oplossingen te komen en te kunnen anticiperen en acteren op (toekomstige) knelpunten is het belangrijk om een informatiepositie op te bouwen. In 2017 is een interdepartementaal onderzoek naar (toekomstige) tekorten en knelpunten omtrent werving en ontwikkeling van ICT-personeel afgerond. Dit onderzoek levert de kennis op om tot meer gerichte en daarmee effectievere en meer efficiënte (beleids)interventies te komen in een aanvalsplan voor de langere termijn. Een plan, gericht op de versterking van de positie van het Rijk als ICT-werkgever zal eind 2017 gereed zijn. Tegelijkertijd wordt ook op korte termijn aan rijksbrede initiatieven gewerkt zoals het rijksbreed delen van CV's van potentiële ICT-werknemers, het opzetten van een ICT-

stagebureau en een herijking van en een meer coherente arbeidsmarktcommunicatie gericht op ICT'ers.

=====

Overige overwegingen: sturing en besluitvorming
Ook op centraal niveau is versterking van de I-functie nodig. Mede hierom is in 2015/2016 een reorganisatie bij het ministerie van Binnenlandse Zaken (BZK) uitgevoerd waarbij de omvang en takenpakket van de directie CIO Rijk (voorheen Directie Informatiseringsbeleid Rijk) is uitgebreid. Ook zijn de verantwoordelijkheden voor ICT in het Rijk (directie CIO Rijk) en de verantwoordelijkheid voor overheidsbreed I-beleid (Directie Informatiesamenleving Overheid) nu samengebracht in één directoraat-generaal (DG Overheidsorganisatie, DGOO).

In 2015 is besloten om de rol van de interdepartementale commissie van CIO's van departementen (ICCIO) uit te breiden. Deze verandering is ook gemarkeerd door een nieuwe naam: het CIO-beraad. Het CIO-beraad zal zich naast de bedrijfsvoering ook steeds meer richten op de digitalisering van het het primaire proces. Dit laatste zal veelal gebeuren in de vorm van kennisuitwisseling, zie ook het volgende hoofdstuk. Het CIO-beraad blijft onverminderd verantwoordelijk voor rijksbrede kaders, jaarplannen en beleid op het gebied van I. Het CIO-beraad staat onder voorzitterschap van de CIO Rijk en bestaat uit CIO's van departementen en vijf uitvoeringsorganisaties.

Beslissingen met belangrijke nieuwe financiële consequenties worden over het algemeen genomen door de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR); voor dit type beslissingen treedt het CIO-beraad dus als adviseur op. Onderwerpen die doorgeleid worden naar de ministerraad lopen van de ICBR naar het overleg van secretarissen-generaal (SGO).

Het CIO-beraad wordt zelf geadviseerd door een eigen vooroverleg, door de CTO-raad en door de subcommissie informatiebeveiliging (SIB). Alle rijksbrede vraagstukken met een technisch karakter, zoals optimaliseren van het netwerk, worden in principe voorgelegd aan de CTO-raad. Deelnemers van de CTO-raad zijn directeuren van ICT-uitvoeringsorganisaties/SSO's[9], aangevuld met enkele gezaghebbende CTO's.

[9] Shared service organisaties

2. Digitalisering van primaire processen

In de vorige versie van de Strategische I-agenda (2016) was er meer aandacht voor het primaire proces en niet alleen voor de beheersing van ICT-projecten, zoals in de I-strategie uit 2012. Primaire processen en de uitvoering bij agentschappen en ZBO's verschillen echter sterk per sector en per departement.
Daarom ligt de focus in dit hoofdstuk minder op het ontwikkelen van rijksbreed beleid en centrale voorzieningen, maar meer op het delen van kennis en ervaring, bijvoorbeeld in het CIO-beraad, en het bevorderen van het gebruik van bestaande bouwstenen.
Het programma Digitaal 2017 streeft ernaar dat burgers en bedrijven uiterlijk in 2017 overheidsbrede diensten digitaal beschikbaar zijn. Inmiddels is 90% van de overheidsbrede diensten digitaal beschikbaar. Het verder optimaliseren van processen zal ook na het jaar 2017 een belangrijk aandachtspunt blijven.

Overheden zijn geneigd om aan digitale toepassingen de eis te stellen dat ze bij aanvang perfect werken en toegankelijk zijn voor alle burgers. Dit heeft tot gevolg dat vaak voor maatwerk wordt gekozen en goedkopere standaardoplossingen weinig wordt ingezet. Dat vraagt om meer aandacht en als dit leidt tot breed toepasbare algemene inzichten: des te beter.

Wij verwachten dat de volgende onderwerpen de agenda voor de rijksdienst zullen domineren: inzetten van de Generieke Digitale Infrastructuur (GDI), verantwoorde inzet van data-analyse, ontwikkelen van bestendige ketenstandaarden en gegevensstromen, en vernieuwen van legacy-systemen. Ook projecten als het Digitaal Stelsel Omgevingswet (DSO) raken meerdere ministeries.

Inzetten van GDI-bouwstenen bij de rijksdienst
De huidige GDI is onder regie van de Digicommissaris ontwikkeld voor algemeen gebruik in de gehele publieke sector. In de praktijk is daarvan echter tot nu toe nog slechts beperkt sprake, maar de verwachting is, dat mede door de recente financieringsafspraken, het gebruik sterk zal toenemen. De rijksdienst zal bij de digitalisering van zijn (primaire) processen uiteraard waar nuttig (of verplicht) gebruik maken van de GDI-bouwstenen. Het CIO-beraad zal zich vooral buigen over de bouwstenen van de GDI die voor de rijksdienst de meeste voordelen opleveren in het primaire proces en voor bedrijfsvoering, zoals inzet van authenticatiemiddelen die in het kader van het programma eID worden ontwikkeld, gebruik van het stelsel van basisregistraties en inzet van open standaarden. Omgekeerd zal het CIO-beraad waar nuttig en wenselijk een standpunt namens de rijksdienst formuleren, als input voor de ontwikkeling van nieuwe GDI-bouwstenen.

Verantwoorde inzet van data-analyse
Door de digitalisering ontstaat een explosieve toename van allerlei data; hierdoor neemt ook de mogelijkheid voor verdere data-analyse toe, tegenwoordig vaak aangeduid met de term "big data analytics". Ook de rijksdienst streeft ernaar data optimaal in te zetten bij de uitvoering van haar taken, bijvoorbeeld voor het verbeteren van gezondheidszorg, misdaad- en fraudebestrijding, bestrijding van ziekten, optimalisatie van dienstverlening, HR-analytics en optimalisatie van huisvesting.

Er is overigens wel een verschil met het bedrijfsleven: waar het bedrijfsleven data-analyse ook graag inzet voor hun marketing, bijvoorbeeld door "profiling" om het koopgedrag van een potentiële klant te beïnvloeden, past dit veel minder goed bij de taken en

verantwoordelijkheden van de rijksdienst. Het bepalen van juiste toepassingsgebieden en het beschikken over voldoende talent (data-scientists) om het daadwerkelijk te realiseren is dan ook een van de uitdagingen voor de komende tijd. We bezien de mogelijkheid om een specifiek traineeproject voor data-scientists te starten.

De andere uitdaging is het enerzijds optimaal uitoefenen van de taken van de rijksdienst en anderzijds beschermen van de privacy van de burger. De WRR geeft in haar rapport[10] van april 2016 aan: "Tegelijkertijd ontstaan er nieuwe risico's voor burgers op het gebied van privacy, voor discriminatie, en door foutmeldingen en schijnverbanden."
Het wordt een steeds grotere uitdaging om zeker te stellen dat deze gegevensstromen blijven voldoen aan de privacywetgeving en dat tegelijkertijd het nationaal belang (nationale veiligheid) wordt gediend.
Met deze twee uitdagingen ten aanzien van het gebruik van data (bepalen van toepassingsgebieden en de extra aandacht voor privacy) gaan wij de komende tijd in het CIO-beraad aan de slag. Zie ook hoofdstuk 4 wat betreft privacy.

Open Data
De overheid beschikt over veel databestanden. Uitgangspunt is dat deze bestanden zoveel mogelijk voor iedereen toegankelijk en beschikbaar zijn. Zorgvuldigheid omtrent privacy en accuratesse van de data worden hierbij vanzelfsprekend in acht genomen. Door open data wordt data-analyse buiten de overheid mogelijk gemaakt en kunnen organisaties buiten de rijksdienst verder innoveren.
Daardoor kunnen service en dienstverlening aan burgers en bedrijven ook door partijen buiten de rijksdienst verbeterd worden.

Ontwikkelen van bestendige ketenstandaarden en gegevensstromen
In veel primaire processen spelen vaak verschillende overheidspartijen een rol: gemeenten, provincies, waterschappen, ZBO's en (agentschappen van) departementen; en soms ook partijen buiten de overheid, zoals onderwijsinstellingen en zorgverleners en -verzekeraars. De taakverdeling tussen deze partijen wordt veelal door het kabinet, al of niet bij wet, vastgesteld. I-aspecten spelen idealiter bij deze beslissingen een rol, maar zijn zeker niet de enige overweging. In deel I is gememoreerd dat in de afgelopen jaren een aantal taken is verlegd van het Rijk naar medeoverheden, meestal gemeenten. In de praktijk worden taken niet zelden gespreid over meerdere partijen die (dus) goed samen moeten kunnen werken. Een voorbeeld is de gegevensstroom in de inkomensketen: de vooraf ingevulde aangifte (VIA) voor de inkomstenbelasting, die wordt samengesteld door gebruik te maken van meerdere ketenpartners binnen en buiten de overheid.

Nadat de taakverdeling is vastgesteld is het zaak om de dienstverlening voor burgers en bedrijven te optimaliseren. Kernpunt daarbij is vaak het ontwikkelen van de interoperabiliteit: definiëren van koppelvlakken, protocollen en veiligheidseisen om gegevens tussen partijen uit te wisselen en te zorgen dat processen soepel en foutloos verlopen. De I-functie heeft hierin een belangrijke rol. Wij verwachten dat departementen in hun I-strategieën (zie vorige hoofdstuk) ruime aandacht geven aan de ontwikkeling van de gegevensstromen in de sector(en) en ketens waar zij verantwoordelijk voor zijn.

[10] Wetenschappelijke Raad voor het Regeringsbeleid, "Big data in een vrije en veilige samenleving", 2016

Ook in het CIO-beraad zullen wij hierover regelmatig inzichten uitwisselen. Dat kan gaan over concrete plannen om gegevensstromen te structureren en te verbeteren, maar ook over de inrichting van besluitvorming om tot betere gegevensstromen te komen (vaak aangeduid met 'ketenregie'). Bijzondere aandacht zullen we daarbij geven aan situaties waarin agentschappen of ZBO's die "vallen" onder departement x een bijdrage leveren aan een proces waarin departement y eindverantwoordelijk is, bijvoorbeeld de PGB-keten (persoonsgebonden budget), waarvoor het ministerie van Volksgezondheid, Welzijn en Sport ketenverantwoordelijkheid draagt, maar waarin ook de Sociale Verzekeringsbank, die onder het ministerie van Sociale Zaken en Werkgelegenheid valt, een belangrijke rol speelt.

Hoewel het ontwerp van de gegevensstromen en koppelvlakken dus vaak binnen sectoren gebeurt, streven we ernaar om de gemaakte afspraken op te nemen in de Enterprise Architectuur Rijk, of althans referenties naar de gemaakte afspraken daarin op te nemen.

Vernieuwen legacy-systemen

Bij het digitaliseren van bestaande processen moeten departementen regelmatig bestaande oudere systemen aanpassen. Dat is soms niet eenvoudig en wanneer het systeem niet meer onderhoudbaar is of niet langer ondersteund wordt door leveranciers spreekt men van een "legacy-systeem". Op zichzelf hoeft de leeftijd van een systeem geen probleem te zijn. Legacy-systemen zijn immers over het algemeen systemen die al vele jaren operationeel zijn en stabiel werken. Legacy-systemen kunnen echter problematisch zijn indien deze niet meer goed aan te passen zijn aan de eisen van vandaag of kwetsbaar zijn voor cyberaanvallen. Departementen en sectoren zijn verantwoordelijk voor hun eigen systemen en dus ook voor hun "legacy". Vervangingsprojecten zijn risicovol en moeten daarom gedegen zijn, met voldoende tijd en een behapbare scope. Liefst opgedeeld in kleine projecten om het beheersbaar te houden. Hierbij worden oude applicaties eerst architectonisch verdeeld in stukken en modules. Het is belangrijk kennis en ervaringen hierover uit te wisselen. Bij tijd en wijle zullen we daarom in het CIO-beraad en in de CTO-raad aandacht besteden aan deze problematiek.

3. Eén concern, de rijksdienst als “connected enterprise”

Het belang van samenwerking binnen de rijksdienst is groot. De rijksdienst moet zoveel mogelijk kunnen werken als één samenhangend, efficiënt geheel, met inachtneming van het feit dat internationale samenwerkingsverbanden van ministeries ook eigen eisen kunnen stellen aan die samenwerking. We werken verder aan deze één concerngedachte, met daarbij andere accenten. Geen verdere centralisatie van systemen, maar interoperabiliteit van afzonderlijke systemen en samenwerking tussen diverse onderdelen van de rijksdienst als “connected enterprise”. Dat betekent niet noodzakelijk alle voorzieningen gemeenschappelijk voor alle departementen – dat is vaak onmogelijk –, maar de diversiteit managen en verbinden: “managed diversity”. Dat gaat met name om samenhang en interoperabiliteit van systemen en processen die hergebruik van (bron)gegevens mogelijk maken.

In het vorige hoofdstuk is al gesproken over ketenprocessen als eerste voorbeeld voor de “connected enterprise”. In dit hoofdstuk komen aanvullende onderwerpen die ondersteunende processen en gegevensstromen betreffen en daardoor niet beperkt zijn tot één sector of departement, maar veelal relevant zijn voor de hele rijksdienst. Veel van onderstaande onderwerpen zijn – soms in een andere vorm – al in gang gezet onder de vorige I-strategie uit 2012.

Invoeren van een interoperabiliteitskader voor digitale werkomgevingen en rijkskantoren
Op dit moment zijn binnen het Rijk (de kerndepartementen, agentschappen en shared service organisaties) nog 14 met name interne leveranciers van werkplekken actief. Dit aantal kan nog naar beneden, maar het is niet ons plan om de werkplekken bij één interne aanbieder te concentreren.

Het is van belang dat ambtenaren rijksbreed goed samen kunnen werken, ook als zij niet dezelfde ICT-dienstverlener hebben of op dezelfde locatie zitten. Het programma IDWOR (Interoperabiliteitskader voor Digitale Werkomgevingen en rijkskantoren) levert hier een bijdrage aan. IDWOR beschrijft kaders voor de volgende onderwerpen: toegang tot internet, overal eenvoudig printen en scannen, connectiviteit naar de digitale werkomgeving, met elkaar kunnen video conferencen, het delen van de digitale agenda tussen rijksmedewerkers en een gezamenlijk adressenboek. Daarnaast realiseert IDWOR een rijksbrede producten- en dienstencatalogus voor ICT dienstverlening in de rijkskantoren. Het IDWOR zal verder stapsgewijs worden ingevoerd.

Invoeren afspraken Rijks Identity Management (RidM)
Medewerkers van de rijksdienst (ambtenaren, maar ook uitzendkrachten, bewakers en externen) maken gebruik van departementale en sectorale voorzieningen en applicaties, maar ook van rijksbrede voorzieningen en applicaties. Het programma Rijks Identity Management beoogt de rijksbrede (toegangs-)processen zo eenvoudig en makkelijk mogelijk in te richten, vanuit het oogpunt van gebruiksgemak, betrouwbaarheid en veiligheid, en kosten. Bij gebruiksgemak gaat het er bijvoorbeeld om dat een medewerker één exemplaar van een rijksbrede voorziening – zoals een Rijkspas – bij meerdere werkrelaties (bijvoorbeeld in geval van detachering) kan gebruiken, en dat een medewerker zijn rijksbrede voorzieningen kan behouden bij een overplaatsing binnen het Rijk. Bij betrouwbaarheid en veiligheid gaat het er onder andere om dat gegevens goed worden vastgelegd, zodat ze voor meerdere voorzieningen kunnen worden gebruikt, en dat iemand bij uitdiensttreding volledig wordt afgesloten van rijksvoorzieningen. Dit verlicht de taak van

de zogenaamde Identity Management Systemen en processen van de departementen, maar stelt omgekeerd ook eisen aan deze systemen en bijbehorende processen. De ondersteuning van P-Direkt bij de HR-processen van de departementen is hiermee vergelijkbaar.

Een goed werkend Rijks Identificerend Nummer (RIN) is hierbij essentieel. Het RIN zal in deze periode verder worden ingezet als “koppelnummer” om voorzieningen medewerker-specifiek te maken, processen te verbeteren en daar waar mogelijk kosten te verlagen. Het RIN wordt inmiddels in de rijksadresgids (RAG) toegepast, waarmee de gegevens van medewerkers overzichtelijk bij elkaar worden gebracht en hun bereikbaarheid wordt vergroot.

Interoperabel maken van cloudontwikkelingen binnen het Rijk (Rijkscloud)
Veel van de interne dienstverleners werken aan het virtualiseren en optimaliseren van hun datacenters. Het programma rijkscloud is een vervolg op de I-strategie van 2011 en loopt door tot en met 2017. Het programma heeft drie componenten: consolidatie van datacenters (PCDC), optimalisatie van het rijksoverheid netwerk (RON) en verbeteren van de samenwerking van ICT-dienstverleners, zodat hun clouddiensten interoperabel worden en ze tezamen rijksbrede clouddiensten kunnen leveren. Het programma rijkscloud eindigt in 2017. De interne dienstverleners werken ook daarna verder aan hun voorzieningen en delen hun kennis.

Informatiehuishouding
Het Programma Rijk aan Informatie (RAI) werkt aan stapsgewijze verbetering van de informatiehuishouding van de rijksdienst. Het programma is een coproductie van het ministerie van OCW en het ministerie van BZK. Het programma bestaat voortdurend uit drie tot vijf deelprojecten, die bijdragen aan een toekomstbestendige en duurzame informatiehuishouding. Op dit moment zijn dat onder andere webarchivering en het bewaren en archiveren van email. De deelprojecten worden vanuit het perspectief van de medewerker en ‘by design’ ingevuld met steeds een sponsor op hoog ambtelijk niveau vanuit de Rijksoverheid. Het programma werkt ook aan een visie op de toekomst van ondersteunende systemen (zoals Document Management Systemen).

Verder optimaliseren van onze netwerken
Een goed kosteneffectief netwerk is van levensbelang voor een “connected enterprise”. Meerdere initiatieven vinden plaats en hebben plaatsgevonden ter verbetering van het netwerk van de rijksoverheid. Toch bestaat de indruk dat de flexibiliteit van onze netwerken nog omhoog kan en de kosten omlaag, bijvoorbeeld door verdere samenvoeging van (fysieke) verbindingen en door passend gebruik te maken van de reeds bestaande eigen netwerken. In deze planperiode zal gewerkt worden aan verdere optimalisatie en implementatie van de netwerken van de rijksdienst met oog voor informatiebeveiliging. Dit gebeurt uiteraard in samenhang met bestaande overheidsbrede initiatieven en binnen de kaders van overheidsbrede afspraken. Een voorbeeld hiervan is het DigiNetwerk afsprakenstelsel, dat beschrijft hoe besloten netwerken van overheidsorganisaties betrouwbaar gegevens uit kunnen wisselen.

Vastlegging in Enterprise Architectuur Rijk (EAR)
De Enterprise Architectuur Rijk zal in deze planperiode opnieuw worden ingericht. De EAR zal niet alleen gaan over bedrijfsvoering, maar ook over (verwijzingen naar) architectuurafspraken in de primaire processen van specifieke sectoren, en naar de NORA[11]. Wij streven ernaar om de EAR relevanter te maken voor organisaties binnen de rijksdienst door duidelijker en compacter te beschrijven wat de regels (kaders) zijn waaraan zij zich hebben te houden, met voorbeelden over de mogelijke invulling van die regels, verwachte toekomstige ontwikkelingen, etc.

Behalve aan bovengenoemde onderwerpen zullen wij aandacht geven aan de vraag op welke aanvullende punten het helpt om in gezamenlijkheid te werken, rekening houdend met de verschillen tussen de departementen.

Overige overwegingen: standaardisatie
Bij bovenstaande onderwerpen zullen wij regelmatig de vraag beantwoorden of wij een proces dat op veel plaatsen voorkomt gaan ondersteunen met één en dezelfde applicatie, of dat de keuze aan departementen blijft. Processen binnen departementen kunnen specifiek zijn voor het takenpakket van dat departement, of generiek, in de zin dat vergelijkbare processen bij alle departementen plaatsvinden. Het lijkt voor de hand te liggen ernaar te streven dat departementen voor generieke processen hetzelfde systeem gebruiken, of althans (kopieën van) dezelfde applicatie. In de praktijk blijkt dit echter soms niet of slechts met onevenredig grote inspanning te realiseren. Ook is het vaak moeilijk of onmogelijk om eenzelfde applicatie verplicht te gebruiken als niet eerst de achterliggende processen zijn gestandaardiseerd. Daarom hanteren we de volgende criteria bij het nadenken over standaardisatie:

- Een business case heeft overtuigend aangetoond dat de te boeken kostenbesparing en/of de waarde van de kwaliteitswinst van de standaardisatie opwegen tegen verlies aan flexibiliteit bij departementen en de te maken projectkosten.
- Er is een organisatie binnen de rijksdienst die namens alle gebruikers opdrachtgever zal zijn voor beheer, onderhoud en verdere doorontwikkeling van het systeem na de initiële oplevering. Bij voorkeur is dit een organisatie die ook een verantwoordelijkheid heeft ten aanzien van de processen die door het systeem worden ondersteund.
- Dit standaardisatieproject heeft voldoende prioriteit binnen de rijksdienst om hiervoor capaciteit vrij te maken, technische en projectcapaciteit, maar ook voldoende ruimte op de agenda van betrokken bestuurders, i.c. vaak het CIO-beraad en de ICBR.

Wanneer niet wordt gekozen voor algehele standaardisatie voor een bepaald proces, dan zullen departementen uiteraard in voorkomende gevallen wel onderzoeken of een binnen de rijksdienst goedwerkende bestaande applicatie hergebruikt kan worden. De eisen die worden gesteld aan de kwaliteit van de gewenste dienstverlening worden meegenomen in deze overweging.

[11] Nederlandse Overheid ReferentieArchitectuur

4. Verstandige aandacht voor informatiebeveiliging en privacy

ICT-ontwikkeling is niet mogelijk zonder blijvende aandacht voor de “donkere” kanten ervan. Door toenemende digitalisering worden we in onze dagelijkse operatie steeds afhankelijker van ICT-systemen. Deze systemen bevatten steeds meer kwetsbare informatie. De combinatie met steeds toenemende en veranderende dreigingen vergroot de zorg over de beveiliging, de vertrouwelijkheid en de integriteit van gegevens, evenals de noodzaak om correct met die gegevens om te gaan in het licht van de nieuwe Europese privacyverordening (AVG).
Het op orde hebben van de informatiebeveiliging vormt een randvoorwaarde voor een succesvolle verdergaande digitalisering van overheidsorganisaties. De Algemene Rekenkamer constateert in de Staat van de Rijksverantwoording dat informatiebeveiliging bij de ministeries nog tekortkomingen vertoont; de noodzaak voor extra aandacht is daarmee evident.

Verhogen bewustwording en digitale vaardigheden
Aan de basis van informatieveiligheid moet de wil staan om veilig te handelen; daarvoor is het noodzakelijk dat men zich bewust is van de digitale dreigingen, de eigen rol en mogelijke consequenties/risico’s van het eigen handelen en de daarmee samenhangende (bedrijfs)risico’s. Het treffen van beveiligingsmaatregelen heeft geen zin als mensen er (onbewust onbekwaam) omheen werken omdat dat makkelijker is.

Het merendeel van de ambtenarenpopulatie is niet opgegroeid met ICT en heeft digitale vaardigheden gaandeweg op eigen kracht verkregen. Zelfs nu worden digitale vaardigheden niet vanzelfsprekend in het basis- en voortgezet onderwijs aangeboden. Het geïsoleerd focussen op het ICT-veiligheidsbewustzijn is daarmee vergelijkbaar met een verkeersveiligheidcampagne voor automobilisten die zonder rijlessen en rijbewijs aan het verkeer deelnemen. Het vergroten van ICT-veiligheidsbewustzijn is daarom onderdeel van het vergroten van algemene digitale vaardigheden. Een positief bijeffect is dat bestaande ICT beter en efficiënter wordt benut.
Via iBewustzijnRijk wordt reeds geïnvesteerd in het verhogen van ICT vaardigheden en bewustzijn bij ambtenaren van de rijksdienst en de medeoverheden

Implementeren van de nieuwe Baseline Informatiebeveiliging (BIR 2017)
De Baseline Informatiebeveiliging Rijksdienst alsmede de bijbehorende verantwoordingsprocessen is in 2017 herzien; het resultaat daarvan is de BIR 2017. In de planperiode wordt de implementatie van de nieuwe BIR gemonitord en waar nodig begeleid. Deze begeleiding krijgt vorm door de ontwikkeling van interdepartementaal bruikbare best practices (handreikingen).
Het streven is dat de BIR 2017 als basis zal dienen voor het BIO-stelsel (Baseline Informatiebeveiliging Overheid) dat voor alle overheden zal gaan gelden.

Verder is in het kader van de BIR een systematiek van In Control Verklaringen (ICV) opgezet. Dit zal waar nuttig en nodig ook worden aangepast aan de nieuwe BIR 2017.

Informatiebeveiligingsvoorschriften
In 2007 is het Voorschrift Informatiebeveiliging Rijksdienst herzien. In 2013 is het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie herzien. Een aantal ontwikkelingen maakt het noodzakelijk te bezien in hoeverre deze voorschriften bijstelling behoeven, met name doordat de rijksdienst anders is georganiseerd dan in 2007.

Daarnaast wordt de BIR-2017 nog verder uitgebreid met een BBN3-niveau waarin expliciet weerstand tegen statelijke actoren is opgenomen, op basis van NAVO regelgeving.

Versterken operationele samenwerking
In de afgelopen jaren is een duidelijke operationele samenwerking ten aanzien van informatiebeveiliging tot stand gekomen tussen ICT-dienstverleners binnen het Rijk, alsook tussen deze dienstverleners en het NCSC. Dit heeft onder andere geleid tot een beschrijving en formalisering van deze samenwerking (ook wel aangeduid met de term Joint SOC's), en een pilot van het Nationale Detectie Netwerk (NDN). In deze planperiode zal deze samenwerking verder worden uitgebouwd. De CTO-raad zal hierin samen met het NCSC het voortouw nemen, om effectiviteit van preventie te vergroten en snelheid bij het oplossen van veiligheidsproblemen te verhogen. Naast de samenwerking op operationeel niveau zal ook bekeken worden hoe de interdepartementale samenwerking op informatiebeveiliging beter gestroomlijnd kan worden met een duidelijke taakverdeling tussen de verschillende strategische en tactische overleggen.

Implementeren van de AVG
De rijksdienst heeft bij uitstek een verantwoordelijkheid om gegevensstromen en gegevensopslag altijd te laten voldoen aan privacywetgeving. Deze wetgeving is op dit moment in beweging. In mei 2018 wordt de AVG van kracht en vervangt op dat moment de Wet Bescherming Persoonsgegevens (WBP).

In 2017 is er een basis gelegd voor de introductie van de AVG binnen het Rijk. Op basis van een verkenning van de huidige behoeftes bij de CIO-offices en de opgebouwde privacy kennis binnen de CIO Offices (o.a. met betrekking tot PIA's) wordt er verder gewerkt aan de implementatie van de AVG.
Samen met de CIO Offices zullen hiertoe voorstellen worden gemaakt. CIO Rijk zal zich inzetten voor het verbeteren van de governance van rijksbrede voorzieningen, het ondersteunen van de besluitvorming rondom rijksbrede privacyproducten zoals het Rijksmodel PIA (gegevensbeschermingseffectbeoordeling), het stimuleren van het gebruik van best practices, en het verbeteren van de informatievoorziening rond privacy.

.

5. “Zaken voor elkaar krijgen” door optimale inzet van interne en externe leveranciers

Uiteindelijk moet alle beleid na de zorgvuldige besluitvorming (zie H1, deel II) en na aandacht voor de risico’s (zie H4, deel II) uitgevoerd worden. Het Rijk maakt gebruik van de markt als dat kan, maar doet zaken zelf als het moet of gewoon beter is.

We streven ernaar om optimaal gebruik te maken van de markt, onder andere door heldere en ten dele nieuwe instructies voor het al dan niet inzetten van oplossingen en infrastructuur van de markt en door met de markt samen te werken op een manier die een goede balans vindt tussen open communicatie en van elkaar leren als het kan, en professioneel en hard zakendoen als het moet. De markt wordt dan ook in een vroeg stadium betrokken. Voor zover het Rijk taken in het I-domein zelf uitvoert streeft het naar een heldere organisatie en taakverdeling van interne dienstverleners, en verdere professionalisering. Het gaat dus om een optimale inzet van zowel de externe als de interne leveranciers. Hoe dit eruit ziet, werken we hieronder uit.

Maken van handreiking voor interne versus externe inzet
De rijksdienst wil optimaal gebruik maken van de expertise en mogelijkheden van marktpartijen. Er wordt gewerkt aan een handreiking (“sourcingstrategie”) waarmee in een specifiek geval kan worden afgewogen of een externe vorm van dienstverlening een passende en kosteneffectieve oplossing is, of dat een dienstverlener binnen de rijksdienst beter is. Bij de afweging spelen verder criteria een rol als (functionele) kwaliteit van software, privacy (AVG), kosten, eisen aan de informatieveiligheid (BIR)[12], continuïteit van de dienstverlening en het risico van afhankelijkheid van één leverancier. Externe dienstverlening kan bijvoorbeeld zijn: “hosting” door een marktpartij, SaaS (Software as a Service), IaaS (Infrastructure as a Service) of PaaS (Platform as a Service) diensten. Bij dit type dienstverlening wordt overheidsdata opgeslagen in een datacenter van de leverancier. De genoemde afweging zal bij open overheidsdata uiteraard tot andere uitkomsten leiden dan bij gegevens die gerubriceerd zijn als staatsgeheim.

Uiteraard moeten dienstverleners voldoen aan alle wetten en regels (voor zover relevant voor hun dienstverlening), zoals de Baseline Informatiebeveiliging (BIR), de Wet bescherming persoonsgegevens (Wbp) tot mei 2018 en de Algemene verordening gegevensbescherming (Avg) vanaf mei 2018. De te stellen voorwaarden worden altijd vastgelegd in verifieerbare contracten. Aan het besluit om een externe partij in te zetten (dan wel om een dienst aan te besteden) gaat in beginsel een risicoanalyse vooraf, en indien van toepassing een privacy impact assessment. Het risico van afhankelijkheid van één leverancier (“vendor lock-in”) wordt altijd zo klein mogelijk gemaakt, bijvoorbeeld door inzet van open source software[13], en door consequent gebruik van vastgestelde open standaarden.

Voor wat betreft *externe leveranciers* zijn we het volgende van plan:

Versterken van inkoop

[12] Hieronder valt ook nationale en economische veiligheid
[13] Bij keuze van software maken we bedrijfseconomische afwegingen. Bij gelijke geschiktheid kiezen we voor open source.

In de afgelopen jaren is binnen de rijksdienst een grote mate van samenwerking op het gebied van inkoop gerealiseerd. Zo is een inkoopstelsel tot stand gebracht waarin rijksbrede inkoopcategorieën voor de generieke dienstverlening zijn gevormd. Deze inkoopcategorieën zijn verdeeld over departementen: elk departement is verantwoordelijk voor de rijksbrede inkoop van de aan hem toebedeelde inkoopcategorieën. Het inkoopstelsel kent zeven ICT-inkoopcategorieën, zoals werkplekken en netwerken. Ook is voor een vijftal ICT-leveranciers strategisch leveranciersmanagement (SLM) ingericht. Met de kabinetsreactie op het rapport van de commissie Elias in februari 2015 is een intensivering van dit beleid in gang gezet.

ICT Categoriemanagement
Het ICT categoriemanagement is geconcentreerd binnen zes van de in totaal twintig inkoopuitvoeringscentra: IUC Noord (Datacenters), IUC V&J (standaardpakketsoftware), IUC EZ (Inhuur ICT), IUC Haagse Inkoop Samenwerking (Werkplekgerelateerde ICT), IUC Rijkswaterstaat (Dataverbindingen) en IUC Belastingdienst (Enterprise business applicaties, Totaaloplossingen). In 2016 zijn diverse generieke ICT aanbestedingen, met een rijksbreed karakter of voor een cluster van organisaties, uitgevoerd vanuit het rijksbrede categoriemanagement.
Daarnaast worden aanbestedingen van specifieke beleidsprojecten met een substantiële ICT-component uitgevoerd en ondersteund door verschillende IUC's

Uitbreiding strategisch leveranciersmanagement
Met de ontwikkeling van rijksbreed strategisch leveranciersmanagement is ervaring opgedaan met de leveranciers SAP, Microsoft en Oracle, die een vitale rol spelen in de ICT infrastructuur van de rijksoverheid. Deze ervaring leert dat de opzet van strategisch leveranciersmanagement rijksbreed inzicht en overzicht ten aanzien van deze leveranciers oplevert en dat daarmee de positie van het Rijk als opdrachtgever versterkt wordt. De belangrijkste doelstellingen van rijksbreed strategisch leveranciersmanagement zijn het verbeteren van de aansturing van de ICT leveranciers, het creëren van meer toegevoegde waarde voor de organisatie en het reduceren van kosten door het beter organiseren van de vraag vanuit het Rijk aan de markt.

Eind 2016 is besloten tot de uitbreiding van het rijksbrede strategisch leveranciersmanagement ICT met de leveranciers KPN en IBM. Hiervan wordt toegevoegde waarde voor de rijksoverheid verwacht. Bij deze keuze is onder meer gekeken naar de uitgaven van het Rijk aan deze leveranciers, hun betrokkenheid bij belangrijke processen binnen de rijksoverheid en de verwachte toegevoegde waarde van de inrichting van strategisch leveranciersmanagement. In 2017 worden hiervoor verdere plannen uitgewerkt. Ook zal voor de uitvoering per leverancier een rijksbrede leveranciermanager worden benoemd, die namens het Rijk richting deze leveranciers zal opereren.

Software Asset Management
Ten behoeve van versterking van het rijksbrede Strategische Leveranciersmanagement wordt gewerkt aan de ontwikkeling van Software Asset Management (SAM) binnen de rijksoverheid. Dit geeft inzicht in de software die binnen de rijksoverheid in gebruik is. Een rijksbreed programma ondersteunt de ministeries in de ontwikkeling van hun SAM, met als doel dit rijksbreed inzichtelijk te maken.
In 2016 zijn de volgende resultaten gerealiseerd:

- een SAM toolkit is ontwikkeld met daarin: o.a. een SAM self assesment gebaseerd op ISO 19770 waarmee rijksoverheidsorganisaties hun SAM volwassenheid kunnen meten;

- er is een SAM Rijk Portal ingericht als digitale ontmoetingsplaats en kennisbank voor SAM professionals binnen de rijksoverheid; - er is een aanpak opgesteld voor het consolideren van de SAM data van de verschillende ministeries.
- In 2017 worden de ministeries verder ondersteund in hun SAM activiteiten.

Gebleken is dat veel bestaande contracten clausules bevatten die het onmogelijk maken om licenties rijksbreed in te zetten. Inmiddels is in de CTO-raad afgesproken dat dit soort beperkingen in nieuwe licentieovereenkomsten niet meer mogen voorkomen, tenzij met instemming van de CTO-raad. De formele uitwerking hiervan wordt verder onderzocht.

Werken aan een professionele omgangsvorm met de markt
Het rapport van de commissie Elias en ook recente publicaties hebben – terecht – geleid tot een grotere aandacht voor integriteit en rechtmatigheid bij externe inkoop. Voorkomen moet echter worden dat dit doorslaat in verkramping – bij een professionele relatie met de markt horen ook ontspannen omgangsvormen. De markt is voor de rijksdienst een belangrijke bron van kennis en innovatie. Het is belangrijk dat de uitwisseling van informatie, kennis en ideeën in stand blijft. Daarom zal ook gezocht worden naar maatregelen om een integere en rechtmatige maar ook ontspannen omgang met de markt mogelijk te maken. Bijvoorbeeld door niet alleen te definiëren wat niet mag, maar vooral ook wat wel mag. Ook zullen we meer aandacht besteden aan bijeenkomsten waarin ambtenaren en medewerkers van marktpartijen elkaar kunnen ontmoeten en informatie kunnen uitwisselen. Herintroductie van het CIO-café – een bijeenkomst tussen marktpartijen en overheidsmedewerkers – is hier een voorbeeld van.

Zoals eerder aangegeven, stimuleren we innovatie om nieuwe vormen van dienstverlening te realiseren, met name bij kleinschalige en minder kritische trajecten. Als rijksdienst zijn we op het gebied van ICT-innovatie bij voorkeur een trendvolger en geen trendsetter. Bij innovatieve trajecten van het Rijk speelt de markt dan ook een belangrijke rol. Daarbij wordt als partners op basis van vertrouwen samengewerkt, naast formele besturing op basis van contracten.

Voor wat betreft onze *interne leveranciers / shared services centers* zien we de volgende prioriteiten:

Maken van afspraken over taakverdeling
Afspraken worden gemaakt over hoe de interne markt tussen leveranciers wordt verdeeld. Hoewel ook voor interne leveranciers geen principieel bezwaar bestaat tegen een zekere marktwerking en concurrentie, is toch ook een expliciete taakverdeling (bijvoorbeeld naar soorten dienstverlening of verzorgingsgebied) en regievoering nodig. In deze planperiode zal deze taakverdeling verder vorm krijgen. Het meest urgent is hierbij de taakverdeling tussen interne leveranciers in “Rijkskantoren”, met name in die gevallen waarin onderdelen van verschillende ministeries met verschillende dienstverleners worden ondergebracht. Dit is van groot belang voor een efficiënte en effectieve rijksbrede bedrijfsvoering.

ICT-dienstverleners binnen het Rijk maken voor de huisvesting van hun eigen hardware (“housing”) altijd gebruik van een van de vier overheidsdatacenters (ODC’s). De uitvoering van het in 2010 vastgestelde programma consolidatie datacenters, vastgelegd in de zogenaamde “plot”, loopt nog steeds en wordt in beginsel onverkort uitgevoerd, hoewel veranderende omstandigheden en/of voortschrijdend inzicht tot aanpassingen kunnen

leiden. Aanpassingen van de “plot” hebben altijd de instemming nodig van de CIO Rijk en het CIO-beraad.

Benchmarken van interne leveranciers met elkaar en met de buitenwereld
Interne leveranciers, meestal shared service centers, moeten de uitvoering van hun taken op orde hebben: goede up-to-date voorzieningen tegen een marktconforme prijs. In deze planperiode wordt gewerkt aan een systeem van benchmarking waarin de prijs (kosten) van diensten van interne ICT-dienstverleners worden vergeleken, met elkaar, en met vergelijkbare diensten “op de markt”, rekening houdend met de verschillen in regelgeving.

Zaken voor elkaar krijgen door “agile” te werken
Zowel met externe als interne leveranciers zal meer kort cyclisch gewerkt worden. Projecten worden kleiner en duren bij voorkeur maximaal een jaar. Teams worden ook steeds kleiner, maar wel met de juiste mix van mensen, zowel beleid, operatie als techniek, zodat bijsturing ook snel kan plaatsvinden.