Strategische I-agenda Rijksdienst

Inleiding

Voor u ligt de nieuwe Strategische I-agenda[1] Rijksdienst, samengesteld door de CIO Rijk in nauwe samenwerking met leden van het CIO-beraad en de CTO-raad. De voorgaande I-strategie liep van 2012 tot 2015. Sindsdien is veel gebeurd. We noemen maar de start van het programma Digitaal 2017, het onderzoek van de commissie-Elias en de kabinetsreactie daarop, en de opening van het Nationaal Cyber Security Centrum. Ook in de EU vinden ontwikkelingen plaats met implicaties voor de rijksdienst, bijvoorbeeld op gebied van digitalisering, informatiebeveiliging en privacy. Tegelijk blijven de technische mogelijkheden toenemen.

Onder de oude I-strategie 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), maar er zijn wel degelijk gemeenschappelijke elementen, die we in deze strategie zullen 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 op de rijksdienst is significant en we zijn dan ook gekomen tot een nieuwe visie.

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.

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

[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

continuïteit zoveel mogelijk en beschermen privacy. We blijven innoveren en verbeteren, maar wel op een pragmatische en gecontroleerde wijze. Wij doen dat bij voorkeur in kleine stappen die snel resultaat leveren. 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 – vooral door toepassingen van gangbare technologie die nieuw is voor de rijksdienst – om nieuwe vormen van dienstverlening te realiseren, maar dan bij kleinschalige en minder kritische trajecten. Innovatie, van fouten leren en trajecten stoppen horen immers bij elkaar.

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. Rijksbrede harmonisatie en standaardisatie kunnen helpen om de effectiviteit en/of efficiëntie van de rijksdienst te vergroten. 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-strategie 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 Eindrapport van de Tijdelijke commissie ICT-projecten, en daarmee een voorzetting (en ten dele uitbreiding) van het programma Operatie Informatiebestel Rijk (OIR). Dit betekent dus ook het versterken van de positie van “I” in het primaire proces, met name vroeg in de beleidscyclus en tegelijkertijd als gesprekspartner van de uitvoeringsorganisaties.
2. **Digitalisering van primaire processen:** deze strategie 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[2] om samenhang en effectiviteit van de rijksdienst te versterken. Wel met een accentverschuiving: geen focus op verdere centralisatie van voorzieningen, meer aandacht voor 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:** optimaal gebruik maken van marktpartijen, onder andere door een heldere en ten dele nieuwe handreiking voor het al dan niet inzetten van oplossingen, 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 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 2017 van het CIO-beraad en de CTO-raad. Hoewel deze Strategische I-agenda 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 gaan we dit plan jaarlijks actualiseren, in lijn met de cyclus van de departementale I-plannen.

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

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.[3] 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 voor 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.

[3] 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 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. De nieuwe *European Data Protection Regulation* of Algemene Verordening Gegevensbescherming (AVG) gaat dit jaar in en vervangt 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[4]. 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 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). Streven is dat het wetsvoorstel eind 2016 in consultatie gaat.

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 voert regie op de (door)ontwikkeling van de Generieke Digitale Infrastructuur. De ontwikkeling van GDI zelf is daarom 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)
Gezien de genoemde vergrote aandacht voor cybersecurity is in 2012 is het NCSC geopend, met als doel een veilig, betrouwbaar en veerkrachtig digitaal domein te realiseren. Het NCSC heeft een nationale scope. Het NCSC werkt inmiddels intensief samen met de ICT-dienstverleners binnen het Rijk.

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

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 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, als onderdeel van het programma Operatie Informatiebestel Rijk (OIR). Over dit programma wordt regelmatig aan de Kamer gerapporteerd[5].

Sommige maatregelen van zowel de vorige I-strategie als van de OIR zijn nog niet voltooid en lopen door in deze planperiode (zie Appendix B).

Tijdens de afgelopen planperiode is ook een aantal dilemma's duidelijker naar voren gekomen. Om er een paar te noemen: ambitie versus beheerste stappen; 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. De combinatie van de geschetste ontwikkelingen en dilemma's hebben geleid tot onze keuze voor de vijf thema's voor deze planperiode.

[5] Zie kabinetsreactie op het Eindrapport van de Tijdelijke commissie ICT-projecten, inclusief maatregelen zoals het versterken van I-interim

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)[6] als meest in het oog springende maatregel. Het geheel van maatregelen wordt ook wel aangeduid met de naam Operatie Informatiebestel Rijk (OIR). 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.

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 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. Tevens zal onderzoek plaatsvinden om te bepalen of het zinvol is om de taken, verantwoordelijkheden en bevoegdheden van de departementale CIO en diens office verder te formaliseren in een besluit, zoals dat ook bestaat voor de departementale directeur FEZ, waardoor "I" aan tafel zit bij het begin van de beleidscyclus. Hieronder valt in ieder geval de taak van toetsing op uitvoerbaarheid van beleid. Ook wordt hierbij aandacht besteed aan andere rollen in de I-functie, zoals informatiemanagers en beheerders. Net als bij Comptabel Bestel is dit een lange operatie, niet een kortetermijnactie. Door versteviging van de departementale CIO's en hun CIO-offices moet het BIT op termijn overbodig worden.

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

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 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.

"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.

De rijksdienst streeft ernaar om ook 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.

Ontwikkelen van meerjarige I-plannen voor elk departement
Doel van het ontwikkelen van meerjarige I-plannen is onder andere het verkrijgen van vroegtijdig overzicht in ICT-consequenties van beleid, beslag op resources en mogelijke afhankelijkheden. In de meerjarige I-plannen (of: I-strategieën) van de departementen wordt het beleidsmatig gewenste en het haalbare duidelijk tegen elkaar afgewogen.

Vergroten van aandacht voor I-aspecten in formele processen
ICT-consequenties van voorstellen worden prominenter in beeld gebracht door deze expliciet mee te nemen in het Integraal Afwegingskader (IAK). Daarnaast wordt bezien welke aanvullende formele middelen geschikt zijn om I te verankeren in de sturingscyclus.

Versterken van de positie van het Rijk als ICT-werkgever
Het bovenstaande kan niet zonder goede mensen, zowel op de departementen, dicht bij de beleidsmakers, als in de uitvoering. Dit is ook in de eerdergenoemde kabinetsreactie van januari 2015 aangegeven. Echter, de bezetting van I-functies binnen de rijksdienst is een uitdaging, zowel door schaarste op de markt als door de vergrijzing bij de rijksdienst. Het gaat hierbij niet om alle ICT-posities: door automatisering, ook binnen de ICT zelf, vervallen posities in lagere schalen, terwijl juist bij een aantal andere rollen, zoals rollen met zowel een I als beleids-/uitvoerings-component en kennisintensieve rollen zoals veiligheidsexperts, data-analisten en architecten, schaarste is.

We gaan op zoek naar mogelijkheden om werving en ontwikkeling van talent te versterken. Hier wordt al hard aan gewerkt, bijvoorbeeld door verdubbeling van de pool van I-interim Rijk en introductie van het Rijks-ICT-Traineeprogramma (RITP). Er zijn veel aanvullende ideeën op dit vlak, zoals gerichte marketing en werving voor instroom en versimpeling van het proces van aanname, de mogelijkheid om ingehuurd ICT-talent in dienst te nemen, de mogelijkheid en wenselijkheid van arbeidsmarktoeslagen en andere financiële instrumenten en verbetering van doorstroming van ICT-talent binnen de rijksdienst. Wij moeten meer uitdragen dat het Rijk een uitdagende en zeer gevarieerde IT-werkgever is. Op korte termijn

is er echter geen snelle simpele oplossing voor de huidige tekorten (“no silver bullet”). Wij zullen een grondige analyse uitvoeren om te bepalen hoe we het best kunnen verbeteren op dit terrein. De meest veelbelovende maatregelen zullen we bundelen in een “aanvalsplan”, dat we in deze planperiode ook zullen invoeren.

=====

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), waarin ook Logius is ondergebracht.

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, drie uitvoeringsorganisaties en twee leden van de Manifestgroep.

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[7], aangevuld met enkele gezaghebbende CTO’s.

[7] Shared service organisaties

2. Digitalisering van primaire processen

Het programma Digitaal 2017 streeft ernaar dat burgers en bedrijven uiterlijk in 2017 zaken die ze met de overheid doen ook digitaal kunnen afhandelen. Het verder optimaliseren van deze processen zal ook na het jaar 2017 een belangrijk aandachtspunt blijven, zeker voor de rijksdienst. Waar tot op heden vaak bestaande traditionele processen worden gedigitaliseerd, zullen nieuwe processen en diensten steeds meer “meteen” als digitaal worden ontworpen en gerealiseerd, en wordt een eventueel papieren proces een afgeleide daarvan.[8]

In deze Strategische I-agenda is meer aandacht voor het primaire proces dan in de vorige I-strategie. Primaire processen verschillen 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. Als dit leidt tot breed toepasbare algemene inzichten: des te beter.

Wij verwachten de volgende drie onderwerpen de agenda zullen domineren: inzetten van de Generieke Digitale Infrastructuur (GDI), inzetten van data-analyse en ontwikkelen van ketenprocessen en ketenstandaarden.

Inzetten van GDI bij rijksdienst
De rijksdienst zal bij de digitalisering van zijn (primaire) processen uiteraard waar nuttig (of verplicht) gebruik maken van de GDI, die onder regie van de Digicommissaris wordt ontwikkeld. Het CIO-beraad zal zich vooral buigen over de elementen 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 de gemeenschappelijke basisadministraties (GBA’s) 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 de plannen van de Digicommissaris.

Inzetten van data-analyse
Met de toename van gegevensuitwisseling, neemt ook de mogelijkheid voor verdere data-analyse toe, tegenwoordig vaak aangeduid met de term “big data”. 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 graag inzet voor hun marketing, bijvoorbeeld door “profiling” om het koopgedrag van een potentiele klant te beïnvloeden, past dit veel minder goed bij de taken en verantwoordelijkheden van de rijksdienst. Het bepalen van juiste toepassingsgebieden is dan ook een van de uitdagingen voor de komende tijd.

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[9] van

[8] Principe is dat burgers ook niet digitaal zaken kunnen blijven doen met de overheid
[9] Wetenschappelijke Raad voor het Regeringsbeleid, “Big data in een vrije en veilige samenleving”, 2016

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. Zeker in die gevallen waarbij de overheid gegevens als open data beschikbaar wil stellen, bijvoorbeeld ten dienste van onderzoek, is aandacht voor de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens belangrijk.[10]

Met deze twee uitdagingen (bepalen van toepassingsgebieden en de extra aandacht voor privacy) gaan wij de komende tijd in het CIO-beraad aan de slag. Op dit moment zijn die meer aan de orde dan de technische kant van data-analyse.

Open Data
De overheid beschikt over veel databestanden. Uitgangspunt van het kabinet is dat deze bestanden zoveel mogelijk deze bestanden 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 ketenprocessen en ketenstandaarden
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 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.

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

[10] Zie hierover ook de Nationale Open Data Agenda (NODA) 2016, kamerbrief van 30 november 2015

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 op de gemaakte afspraken op te nemen in de Enterprise Architectuur Rijk, of althans referenties naar de gemaakte afspraken daarin op te nemen.

=====

Overige overwegingen: “legacy”

Bij digitaliseren van bestaande processen moeten departementen regelmatig bestaande oudere software 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” probleem. Op zichzelf hoeft de leeftijd van een systeem geen probleem te zijn, maar als het systeem niet meer goed is aan te passen aan de eisen van vandaag of kwetsbaar is voor cyberaanvallen, dan is het wel een probleem. Departementen en sectoren zijn verantwoordelijk voor hun eigen systemen en dus ook voor hun “legacy”. Vervangingsprojecten moeten gedegen zijn, met voldoende tijd en 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. Er is veel werk verzet aan de “één concern gedachte”. Ook in deze planperiode werken we verder aan deze gedachte, maar leggen daarbij wel andere accenten. Minder dan het verleden zullen we werken aan verdere centralisatie van systemen, maar meer dan in het verleden aan interoperabiliteit van afzonderlijke systemen. Anders geformuleerd, we werken aan 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.

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 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.

Invoeren van een interoperabiliteitskader voor digitale werkomgevingen in de rijksdienst
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 IDWOR (Interoperabiliteitskader voor Digitale Werkomgevingen in de Rijksdienst) gaat hier een bijdrage aan leveren. Het IDWOR regelt bijvoorbeeld dat alle ambtenaren agenda’s kunnen delen, overal automatisch wifi hebben, overal eenvoudig kunnen printen en scannen, met elkaar kunnen video-conferencen, een gezamenlijk adressenboek. Het IDWOR zal deze planperiode stapsgewijs worden ingevoerd.

Invoeren afspraken Rijks Identity Management (RidM)
Medewerkers van de rijksdienst (ambtenaren, maar ook uitzendkrachten, bewakers en andere 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. Een voorbeeld hiervan is het toepassen van het RIN in de rijksadresgids (RAG), waarmee de gegevens van een medewerker overzichtelijk bij elkaar worden gebracht en de 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.

Stapsgewijs verbeteren van informatiehuishouding (Rijk aan Informatie)
Tijdens de planperiode (tot eind 2018) ontwikkelen we principes en standaarden om de informatiehuishouding van de rijksdienst stapsgewijs te verbeteren. Dit programma is een coproductie van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en het ministerie van Binnenlandse Zaken (BZK). Het programma bestaat voortdurend uit twee tot vier deelprojecten, die elk gericht zijn op een concreet resultaat of op het oplossen van een concreet probleem. Voor 2016 zijn de deelprojecten: bewaren en archiveren van email en samenwerken in documenten. Deze deelprojecten worden ondersteund door een doorlopend deelproject dat de wensen en prioriteiten van medewerkers in kaart brengt en interventies ontwerpt om verbeteringen effectief bekend te maken en te implementeren.

Het programma zal ook stapsgewijs werken aan een visie op de toekomst van ondersteunende systemen (bijvoorbeeld Document Management Systemen) en bepalen welke systemen het beste centraal aangeboden kunnen worden en welke beter per departement kunnen worden georganiseerd.

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 meer 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. Dit gebeurt uiteraard in samenhang met de overheidsbrede initiatieven van de Digicommissaris 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 zullen ernaar streven 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, naast het geven van informatie over mogelijke invulling van die regels, verwachte toekomstige ontwikkelingen, etc.

Behalve aan bovengenoemde onderwerpen zal tijdens de planperiode aandacht gegeven worden 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 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 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.

[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. Tegelijkertijd bevatten die systemen steeds meer kwetsbare informatie, wat de zorg om de vertrouwelijkheid en integriteit van gegevens vergroot, evenals de noodzaak om correct met die gegevens om te gaan in het licht van de nieuwe Europese privacywetgeving.

Drie belangrijke activiteiten staan op de rol: het ontwikkelen van de nieuwe Baseline Informatiebeveiliging Rijksdienst (BIR), het versterken van de operationele samenwerking, en het implementeren van de Algemene Verordening Gegevensbescherming (AVG) binnen de rijksdienst.

Ontwikkelen van een nieuwe Baseline Informatiebeveiliging (“BIR 2.0”)
In 2012 is de Baseline Informatiebeveiliging Rijksdienst (BIR) vastgesteld. De BIR is gebaseerd op de internationale ISO-standaard (ISO-27002) en harmoniseerde en verving de bestaande regelingen binnen de departementen. Dankzij de BIR is de aandacht voor en effectiviteit van informatiebeveiliging[12] sterk toegenomen. In 2015 is de BIR aangevuld met een standaard “In Control Verklaring”, die jaarlijks door de secretaris-generaal van elk departement wordt afgegeven.

Inmiddels is ook een aantal nadelen van de BIR naar boven gekomen. De BIR (en de verantwoordingsprocessen daaromheen) bergt door zijn omvang het gevaar in zich dat deze gebruikt wordt als “afvinklijst” in plaats van als leidraad om de informatiebeveiliging te verbeteren. Ook blijkt de huidige toepassing van de BIR niet toereikend in situaties waar partijen in ketens met elkaar samenwerken of samen gebruik maken van een Shared Service Organisatie (SSO) binnen het Rijk. Soms lijkt het erop dat nog te weinig aandacht wordt besteed aan de “factor mens”. De BIR lijkt soms aanleiding te geven tot maatregelen die als dermate onpraktische worden ervaren dat de individuele gebruiker zich welhaast gedwongen voelt om er een weg omheen te vinden. Beveiliging die zo strikt is dat iedereen er omheen werkt, is schijnbeveiliging.

In de planperiode willen we daarom de Baseline Informatiebeveiliging (BIR) gaan herzien alsmede de bijbehorende verantwoordingsprocessen, met als werktitel “BIR 2.0”. Met de BIR 2.0 willen we bovengenoemde nadelen aanpakken en streven naar een document[13] dat niet alleen kaderstellend is, maar ook een handreiking voor departementen, die helpt om de (administratieve) werklast te verlagen en toch een grotere bijdrage te leveren aan de feitelijke informatiebeveiliging (risicomanagement).

[12] Binnen de rijksdienst wordt de term “informatiebeveiliging” gebruikt om drie aspecten aan te duiden: vertrouwelijkheid, d.w.z. voorkomen dat deze in verkeerde handen komt; integriteit, d.w.z. zorgen dat informatie tijdig juist en volledig is; en continuïteit, d.w.z. zorgen dat (ICT-)systemen en de daarin vervatte gegevens bij calamiteiten beschikbaar blijven of hersteld kunnen worden, voor zover nodig.
[13] Of set van documenten

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.

Implementeren van de AVG en uitvoeren van de meldplicht Datalekken 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. Op 1 januari is de Wet Meldplicht Datalekken[14] van kracht geworden. Een dergelijke meldplicht is ook onderdeel van de reeds genoemde AVG, die de Nederlandse Wet Bescherming Persoonsgegevens (WBP) gaat vervangen.

De CIO Rijk zal onderzoeken wat hiervoor binnen de rijksdienst nodig is. De stelselverantwoordelijkheid is bij de Minister van VenJ belegd. De uitvoerende verantwoordelijkheid blijft uiteraard binnen departementen liggen. Tijdens de planperiode wordt bepaald welk rijksbreed beleid nodig is. Hierbij zal de CIO Rijk onder andere ook kijken naar de vraag hoe privacy verantwoordelijkheden (bijvoorbeeld databewerker versus dataverantwoordelijke) moeten worden verdeeld tussen SSO's en hun klanten.

[14] Staatsblad 281, "Besluit inwerkingstredingsbesluit Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp"

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. Wij zullen werken 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 (EPV), kosten, eisen aan de informatieveiligheid (BIR)[15], 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 (Wpb) tot mei 2018 en de Algemene verordening gegevensbescherming (Avg) vanaf mei 2018[16]. 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 altijd 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[17], en door consequent gebruik van vastgestelde open standaarden.

[15] Hieronder valt ook nationale en economische veiligheid
[16] De Avg is op 4 mei 2016 gepubliceerd in het Publicatieblad van de EU. Deze treedt 20 dagen later in werking, waarbij lidstaten twee jaar de tijd hebben om wetgeving aan te passen om te voldoen aan de nieuwe regels.
[17] Bij keuze van software maken we bedrijfseconomische afwegingen. Bij gelijke geschiktheid kiezen we voor open source.

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

Versterken van inkoop
In de afgelopen jaren is 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 drietal 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.

Momenteel wordt onderzocht of het aantal leveranciers waarvoor SLM is ingericht, kan worden uitgebreid. Ook zal SLM voor softwareleveranciers worden versterkt met rijksbrede gegevens over gekochte en in gebruik zijnde licenties door middel van rijksbreed “Software Asset Management”. In de eerste inventarisatie is al gebleken 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 op dit moment onderzocht. Dit is een voorbeeld van een maatregel die flexibiliteit vergroot en afhankelijkheid van leveranciers verkleint.

Ook zal verbetering van aanbestedingen van grote projecten van het Rijk doorgezet worden, zowel op gebied van rechtmatigheid als doelmatigheid van deze aanbestedingen.

Werken aan een professionele omgangsvorm met de markt
Het rapport van de commissie Elias en ook recente publicaties en rapportages op televisie 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 zal worden 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.

APPENDIX A: Financiële paragraaf

Alle ministeries dragen de eigen kosten die voortvloeien uit deze strategische I-agenda. Planning en financiering zullen interdepartementaal worden afgestemd. Voor de gezamenlijke elementen en de ontwikkeling van de I-agenda is er een aantal structurele geldstromen:

- De door BZK beschikbaar gestelde formatie[18], met name binnen de directie CIO Rijk.
- ICBR-bijdrage van jaarlijks €2,5 miljoen ten behoeve van de jaarlijks vast te stellen jaarplannen van het CIO-beraad en ter dekking van de uitgaven voor onder andere extra "ICBR-plekken" in de door BZK vastgestelde formatie.
- Beschikbaar gestelde middelen voor de uitvoering van kabinetsreactie op het rapport van de commissie Elias (zie tabel).
- Een bijdrage van de departementen aan de kosten voor beheer, onderhoud en doorontwikkeling van rijksbrede ICT-voorzieningen, zoals het Rijksportaal, de Samenwerkingsfunctionaliteit (SWF) en de Rijkspas. Deze bijdrage wordt jaarlijks vastgesteld door de ICBR op basis van de Nota Kostenverdeling Rijksbrede ICT-voorzieningen ("Tarievennota"[19], €24,7 miljoen in 2016).

Sommige rijksbrede ICT-voorzieningen hebben hun eigen financiering (bijvoorbeeld Digi-Inkoop) of worden gefinancierd door hun functionele eigenaar (bijvoorbeeld P-direct).

Naast de genoemde structurele middelen zijn voor specifieke programma's en projecten aanvullende middelen nodig. Deze worden over het algemeen op basis van een business case met financiële en niet-financiële aspecten vastgesteld door de ICBR.

Naar verwachting zal dat in deze planperiode (2016-2019) vooral gaan om de programma's "Rijk aan Informatie", "Rijks Identity Management", optimaliseren van het netwerk en de versterking van de "Rijksdienst als ICT Werkgever". Voor het programma Rijkscloud is financiering eind tot 2017 reeds besloten.

Financiering van GDI-gerelateerde uitgaven en implementatietrajecten bij de departementen vallen buiten de scope van deze strategische I-agenda.

Tabel met "Eliasgelden" (€ miljoenen)[20]:

Elias	**2016**	**2017**	**2018**	**2019**	**2020**
Inrichten BIT/kenniscentrum	2,8	2,8	2,8	2,8	
Uitbreiding I-interimpool Rijk met 100 fte	0,3	0,2			
Opzetten van trainingen en opleidingen CIO-adviseurs en de Algemene Bestuursdienst	0,2	0,2	0,2	0,2	0,2
Opzetten van ICT-Traineeproject, waarbij ieder departement betaalt voor de eigen trainees					
Uitbreiding strategisch leveranciersmanagement	0,6	0,6	0,6	0,6	0,6
Mogelijkheden voor Rijkscloud verder verkennen binnen programma Rijkscloud (voorheen consolidatie ODC)	1,0				
Totaal Elias	**4,9**	**3,8**	**3,6**	**3,6**	**0,8**

[18] Aanvullend stellen departementen op incidentele basis ook medewerkers ter beschikking voor rijksbrede projecten

[19] Notitie kostenverdeling rijksbrede ICT-voorzieningen, 2016

[20] In aanvulling hierop is jaarlijks €0,1 miljoen voorzien voor opleiding van beleidsmedewerkers

APPENDIX B: Aansluiting bij I-strategie van 2011

De volgende thema's uit de vorige I-strategie komen veelal in iets andere vorm terug in deze deze strategische I-agenda:

1. Het thema "Aanbodstructurering" komt terug in hoofdstuk 5 van deel II.
2. Het thema "Sourcing" komt ook terug in hoofdstuk 5 van deel II.
3. Het thema "Sturings- en verantwoordingsinstrumenten" is deels gereed en wordt deels doorontwikkeld, bijvoorbeeld EAR (zie hoofdstuk 3 van deel II).
4. Het thema "I-infrastructuur" blijft uiteraard ook in deze planperiode relevant. Na de Digitale Werkomgeving Rijkdienst (DWR) wordt met het "Interoperabiliteitskader Rijkswerk Omgeving" meer interoperabiliteit van gebruikers van werkplekken binnen de rijksdienst beoogd (zie hoofdstuk 3 van deel II). Een belangrijke slag is gemaakt met datacenter consolidaties; deze consolidatie zal – conform plan – nog geruime tijd doorlopen.
5. Het thema "Personeel en kwaliteit" heeft blijvend aandacht nodig (zie hoofdstuk 1, deel II).
6. Het thema "Vertrouwen en beveiliging van informatie" behoeft verdere aandacht in deze planperiode met bijvoorbeeld Baseline Informatiebeveiliging 2.0 (zie hoofdstuk 4, deel II).
7. Het zevende thema uit de I-strategie van 2011, "Samenwerking met de markt" vereist ook deze planperiode aandacht (zie hoofdstuk 5, deel II).