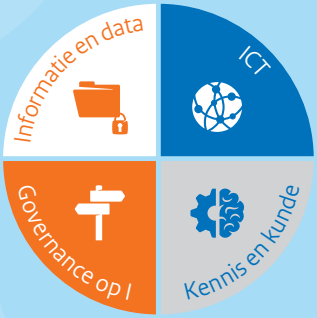
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Strategische I-agenda Rijksdienst 2019-2021



Inhoud

1 Inleiding

Het kabinet-Rutte III[1] wil dat Nederland digitaal koploper wordt van Europa. Deze ambitie uit het regeerakkoord 'Vertrouwen in de toekomst' is verwoord in de Nederlandse Digitaliseringsstrategie, Nederland Digitaal[2]. De Agenda Digitale Overheid, NL DIGIbeter[3], beschrijft de ambitie om binnen de Nederlandse overheid en bij het contact met burgers en ondernemers te zorgen dat de komende jaren veilig, snel en betrouwbaar diensten worden verleend en maatschappelijke vraagstukken worden aangepakt. Daarbij is voortdurende aandacht voor grondrechten en publieke waarden. Hierbij moet Nederland in staat zijn om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen. Deze ambities dagen de Rijksdienst uit om een volgende stap te zetten in rijksbrede samenwerking, professionalisering, doorontwikkeling van en sturing op het I-domein en zo bij te dragen aan maatschappelijke waarden. De minister van BZK heeft dit ook beschreven in haar visiebrief "Sturing op informatiebeveiliging en ICT binnen de Rijksdienst" van 11 oktober 2018[4].

Deze Strategische I-agenda richt zich op de Rijksdienst. De ambitie bij de Rijksdienst is, net als bij Nederland Digitaal, om voorop te lopen en kansen te benutten, waarbij iedereen meedoet en samenwerking binnen de Rijksdienst van groot belang is, met vertrouwen in de digitale toekomst. De CIO's (Chief Information Officers) hebben in hun departement uiteenlopende taken en verantwoordelijkheden en eigen maatschappelijke opgaven. Deze I-agenda beschrijft alleen de rijksbrede activiteiten van het CIO-beraad (het interdepartementale overleg van CIO's), gericht op stimuleren wat al goed loopt, versterken waar dat nodig is en leren van elkaar en anderen. Het ministerie van BZK vervult hier de rol van aanjager, verbinder en platform voor kennisdeling. Het CIO-beraad wil daarbij

[1] Bijlage bij *Kamerstukken II* 2017/18, 34700, 34

[2] *Kamerstukken II* 2017/18, 26643, 541

[3] *Kamerstukken II* 2017/18, 26643, 549

[4] *Kamerstukken II* 2018/19, 26643, 573

aandacht besteden aan zowel een open cultuur om fouten met elkaar te delen, als de successen benadrukken die worden geboekt, die niet altijd (breed) zichtbaar zijn.

De Strategische I-agenda Rijksdienst staat niet op zichzelf. Deze afbeelding schetst de raakvlakken van de I-agenda met diverse richtinggevende documenten op nationaal, overheids- en rijksbreed en departementaal niveau.

Samenvatting en leeswijzer

Deze I-agenda start in het tweede hoofdstuk met ***betrouwbare informatie en data***. In de digitale wereld moeten burgers en bedrijven kunnen vertrouwen op beschikbaarheid, integriteit en vertrouwelijkheid van informatie van de overheid. Informatiestromen moeten daarbij transparant en toegankelijk zijn, zoals ook genoemd in de Nederlandse Digitaliseringsstrategie. Dit alles wel op zo'n manier dat informatieveiligheid geborgd is, ook aansluitend bij het doel van de Nederlandse

Cybersecurity Agenda[5]. Daarbij ligt het accent op feitelijke veiligheid. Ook moet de overheid, als publiek orgaan, de cybersecurity intern op orde hebben en *als launching customer* of *early adopter* het goede voorbeeld geven. Bij de start van de I-agenda zal daarnaast worden bepaald hoe departementale CIO's het best gezamenlijk kunnen optrekken op het gebied van onder andere open overheid en data-analyse. Dit betreft niet alleen informatie en data rondom bedrijfsvoering binnen de Rijksdienst, maar juist informatie en data voor het primaire proces, zoals informatie en datastromen in het onderwijs of in de zorg.

Ten tweede gaat het om de meer technische kant ***goedwerkende, samenhangende en robuuste ICT***, met oog voor de continuïteit van de bedrijfsprocessen. Het doel van deze robuuste ICT is om optimaal te kunnen samenwerken binnen de Rijksdienst. Juist daar waar nodig zetten we concrete gemeenschappelijke voorzieningen in, ook op het gebied van beveiliging. We waken er nadrukkelijk voor dat schaalvergroting door gemeenschappelijkheid nooit ten koste gaat van de menselijke maat; laagdrempeligheid en toegankelijkheid van de digitale overheid blijft hier voorop staan.

Verder gaat het hier om een samenhangende strategie van *sourcing* en inkoop, waarbij ook kleine marktpartijen en startups hun bijdrage kunnen leveren aan gezamenlijke innovaties. Hiermee beslist het Rijk over *make or buy*, welke producten en diensten zij zelf ontwikkelt en welke zij door marktpartijen laat ontwikkelen en beheren. In hoofdstuk drie van dit document komt ICT aan de orde.

Ten derde gaat het om ***kennis en kunde***: permanent leren over ICT bij het Rijk. Ervaringen van bijvoorbeeld het Bureau ICT-Toetsing (BIT) uitvoeringsorganisaties worden gebruikt om te verbeteren. Daarom wordt steeds meer ontwikkeld in kleine stappen in plaats van grote projecten. Bij die kleine stappen past een "*permanent bèta*" aanpak, waarbij een dienst van start gaat zonder dat het helemaal 'af' is en waarbij van fouten wordt geleerd om de dienstverlening te optimaliseren. De overheid moet kunnen experimenteren en risico's durven nemen die nodig zijn om verder

[5] *Kamerstukken II* 2017/18, 26643, 536

te komen. Het gaat bij kennis en kunde ook vooral om samenwerking en van elkaar leren binnen de Rijksdienst en met partijen daarbuiten. Bij nieuwe initiatieven wordt zoveel mogelijk gebruik gemaakt van opgedane ervaringen. "Iedereen doet mee". Daarbij wordt gewerkt aan het versterken van I-bewustzijn en I-vaardigheden van beleidsmedewerkers en aan het werven en behouden van ICT-talent. Dit komt aan bod in het vierde hoofdstuk.

Ten slotte gaat het om sturing: ***strategische governance op I***. De rol van de departementale CIO en de CIO-offices verschuift organisch van controlerend op ICT-gebied naar partner in beleidsvorming en richting partner in het primaire proces. Aan het begin van deze planperiode wordt bepaald hoe de rol van de departementale CIO en de rijksbrede systeemverantwoordelijkheid op I verder aangescherpt en geformaliseerd moeten worden. Hoofdstuk vijf beschrijft welke activiteiten zijn voorzien om de strategische governance op I te verstevigen.

In 2011 heeft de CIO Rijk in overleg met het CIO-beraad de I-Strategie opgesteld, als uitvloeisel van het programma Compacte Rijksdienst. Deze had een looptijd van vier jaar; in 2016 is ervoor gekozen om een meerjarige Strategische I-agenda Rijksdienst op te stellen die jaarlijks wordt geactualiseerd. Dit is de derde editie van de Strategische I-agenda, voor de periode 2019-2021. In deze agenda is meer aandacht voor de maatschappelijke bijdrage van I en voor de versterking van de sturing op ICT binnen de Rijksdienst, zowel departementaal als rijksbreed. De laatste jaren heeft de Rijksdienst al veel bereikt, zoals de verdere inrichting van het CIO-stelsel bij de Rijksdienst, de oprichting van het Bureau ICT-Toetsing (BIT), de uitbouw van I-Interim Rijk (een pool van flexibel inzetbare en ervaren professionals op het gebied van informatiemanagement en ICT binnen de Rijksdienst) en de start van de versterking van I-bewustzijn en -vaardigheden bij beleidsmakers door de oprichting van de RijksAcademie voor Digitalisering en Informatisering Overheid (RADIO). Verdere stappen zijn nodig en de zaken die de komende periode in gezamenlijkheid worden opgepakt binnen de Rijksdienst komen in deze I-agenda aan de orde.

De filosofie van de Strategische I-agenda Rijksdienst is steeds om met kleine stappen een grote sprong te maken en per jaar te bezien of we nog

op de goede weg zitten. Dat geeft ruimte om innovatieve ontwikkelingen gedurende de looptijd samen uit te denken. Komende periode gaat het hierbij bijvoorbeeld over de Rijksbrede sturing op en de (gezamenlijke) aanpak van data, open overheid en grote ICT-projecten. Voor 2019 is een *roadmap* gemaakt die doorlopend zal worden aangepast in overleg met de departementen, gebaseerd op de inhoud van deze I-agenda.

In deze I-agenda gaat het om realiseren van gezamenlijk vastgestelde ambities. Een aantal concrete acties en maatregelen is uitgewerkt. Immers, het is de combinatie van een lonkend vergezicht met het daadwerkelijk doen en waarmaken, wat de Strategische I-agenda tot een waardevol instrument maakt.

2 Informatie en data

2.1 Informatiehuishouding en openbaarheid

Ook in de digitale wereld is het belangrijk dat burgers kunnen vertrouwen op de beschikbaarheid, integriteit, vertrouwelijkheid[6] en onweerlegbaarheid van informatie van de overheid. Het op orde houden en verbeteren van de informatiehuishouding is daarom niet alleen een uitdaging voor experts binnen het ICT-domein, maar vergt significante inzet van álle medewerkers binnen de Rijksdienst. Zij zijn als makers en ontvangers van informatie in grote mate bepalend voor de vindbaarheid, duurzame toegankelijkheid en bruikbaarheid ervan. De insteek is daarom dat de gebruiker een zeer eenvoudige en laagdrempelige wijze van informatiemanagement heeft, by design, met zo min mogelijk handmatig werk. De juiste informatie wordt automatisch opgeslagen, gearchiveerd en vernietigd. Het wordt voor de medewerkers mogelijk om de betreffende informatie sneller te doorzoeken. Het "Meerjarenplan verbetering informatiehuishouding"[7] voor de implementatie van het wetsvoorstel Open Overheid (Woo) bij de Rijksdienst maakt integraal onderdeel uit van deze Strategische I-agenda.

Achtergrond

Een goede informatiehuishouding is cruciaal voor het uitvoeren van overheidstaken en voor de controleerbaarheid van diezelfde overheid door burgers, bedrijven en het parlement. De Erfgoedinspectie concludeert in haar meest recente rapport "Wel digitaal, nog niet duurzaam"[8] dat er ten aanzien van de Rijksinformatiehuishouding de afgelopen vier jaar wel vooruitgang is geboekt, maar dat ministeries nog onvoldoende zicht hebben op het totaal aan informatie dat zich in de digitale systemen bevindt. Het kabinet constateert dat intensivering van het beleid gericht

[6] Beschikbaarheid, integriteit en vertrouwelijkheid vormen samen de betrouwbaarheid in het domein van informatiebeveiliging, zie artikel 1 onder a Voorschrift Informatiebeveiliging Rijksdienst 2007, Stcrt. 2007, 122/11

[7] *Kamerstukken II* 2018/19, 33328, L

[8] *Kamerstukken II* 2017/18, 29362, 269

op verbetering van de informatiehuishouding noodzakelijk is.
De motie-Segers[9] vraagt om aanpassing van de Archiefwet aan de digitale ontwikkelingen en eisen van transparantie door onder meer de huidige overbrengingstermijnen van overheidsinformatie sterk terug te brengen. En ten slotte stelt het wetsvoorstel Open Overheid[10] nieuwe eisen aan de informatiehuishouding: meer dan in het verleden zal informatie actief openbaar gemaakt moeten kunnen worden. Deze verbeteringen kunnen alleen tot stand komen door een gezamenlijke inzet.

Verbetering duurzame toegankelijkheid en vindbaarheid

De meeste rijksonderdelen werken inmiddels vooral digitaal; daardoor is het van strategisch belang dat digitale informatie die zij ontvangen, maken en verzenden, duurzaam toegankelijk is en blijft.

Ter ondersteuning van het rijksbreed archiveren van e-mail is een werkwijze ontwikkeld en zijn er pilots en onderzoeken (naar privacy, duurzame toegankelijkheid, sleutelfunctionarissen en de ervaringen van medewerkers) afgerond voor het bewaren van, in beginsel, alle relevante e-mail. De zo veiliggestelde e-mails kunnen dan worden gebruikt bij verzoeken van burgers om openbaarmaking van informatie (op grond van de Wob of de Woo). Een aantal relevante bronnen kan na verloop van tijd voor duurzaam beheer worden overgedragen aan het Nationaal Archief, waar zij in beginsel openbaar toegankelijk zijn m.u.v. uitzonderingen hierop in de Archiefwet. Ook voor de websites van de Rijksdienst wordt een kader ontwikkeld als voorbereiding op een centrale voorziening voor automatische archivering.

Daarnaast zal een heldere beleidslijn voor archivering en openbaarheid van communicatie via berichtenapps worden gecommuniceerd en geïmplementeerd.

De documentmanagementsystemen van de ministeries zijn ingericht als opslag en ondersteunen de formele stukkenstroom in een ministerie. De systemen kennen een mappenstructuur en zoekfunctionaliteit, waardoor

[9] *Kamerstukken II* 2015/16, 34362, 21

[10] *Kamerstukken II* 2011/12-2018/19, 33328

toegankelijkheid in principe is gewaarborgd. Dat geldt met name voor de documenten die onderdeel zijn van de stukkenstroom. De systemen groeien echter door de jaren heen in omvang en ontwikkelen zich onder invloed van nieuwe technologieën. Dat biedt ook mogelijkheden voor betere toegankelijkheid en bijvoorbeeld meer geautomatiseerd openbaar maken.

Kaderstelling

In de uitvoeringspraktijk bestaat behoefte aan een meer actueel en integraal uitvoeringskader voor informatiehuishouding, ter vervanging van de sinds 2009 geldende Baseline Informatiehuishouding Rijksoverheid[11]. Hiervoor wordt aansluiting gezocht bij het "Toetsingskader informatie van de centrale overheid" dat recent door de Erfgoedinspectie is vastgesteld[12]. In dit toetsingskader heeft de Erfgoedinspectie uitgewerkt hoe zij invulling geeft aan haar toezicht op de informatiehuishouding van het Rijk. Daarnaast vraagt de motie-Segers om in het licht van de digitalisering en de eisen van transparantie te komen tot een aanpassing van de Archiefwet.

Toegankelijkheid en vindbaarheid

Informatie moet niet alleen worden vastgelegd in een e-mailarchief of een documentmanagementsysteem, maar moet ook goed toegankelijk en vindbaar zijn, zodat medewerkers in het primair proces te allen tijde beschikken over voldoende en juiste informatie om hun werk te kunnen doen. Ook bijvoorbeeld voor het beantwoorden van een Wob- of Woo-verzoek is het essentieel dat relevante informatie goed en snel vindbaar is in de steeds omvangrijkere systemen van de Rijksdienst. Informatiesystemen moeten voldoende aansluiten op toekomstige toepassingen, zoals *linked data* en *artificial intelligence*. Bovendien moeten de informatiestromen daarbinnen transparant zijn. Geavanceerde zoek- en vind-applicaties helpen bij het ontsluiten van informatie uit een e-mailarchief, een documentmanagementsysteem en netwerkschijven en ook het ordenen daarvan. Geautomatiseerde selectie en ordening kan ook

[11] *Kamerstukken II*, 2008/09, 29362, 156

[12] Toetsingskader informatie van de centrale overheid, *Erfgoedinspectie* 21 december 2017, erfgoedinspectie.nl

helpen bij de voorbereiding van overdracht van (permanent te bewaren) informatie naar het Nationaal Archief.

De komende periode zullen rijksbrede protocollen (modelprocedures, instructies en selectiebesluiten) voor de toegang tot veiliggestelde informatie (zoals e-mails) worden ontwikkeld. Deze worden ondersteund met geavanceerde zoek- en vind-applicaties. Daarnaast wordt geïnvesteerd in de kennisontwikkeling van de medewerkers op het gebied van informatiehuishouding en openbaarheid.

2.2 Informatiebeveiliging

Doordat de samenleving en de overheid in toenemende mate digitaliseren, ontstaan nieuwe bedreigingen die om nieuwe oplossingen vragen. De digitale rijksdienst moet daarom voortdurend aandacht hebben voor goede informatiebeveiliging. In de afgelopen periode hebben de ministeries de implementatie van de Baseline Informatiebeveiliging Rijksdienst 2017 (BIR 2017) opgepakt. Eind 2018 is door de Ministerraad de Baseline Informatiebeveiliging Overheid (BIO)[13] vastgesteld waardoor meer uniformiteit tussen de verschillende overheidslagen ontstaat. Het Basisbeveiligingsniveau 3 (BBN3-niveau) van de BIR zal in 2019 worden opgeleverd. Verder is de rijksbrede governance rond informatiebeveiliging opnieuw ingericht.

In de Kamerbrief “Sturing op informatiebeveiliging en ICT bij de Rijksdienst” staan reeds vier initiatieven in het domein van informatiebeveiliging genoemd. Drie van deze initiatieven worden vermeld in de paragraaf over gemeenschappelijke voorzieningen in het volgende hoofdstuk. Het vierde initiatief is het opstellen van een lijst van vereiste concrete beveiligingsmaatregelen, waarbij onderzocht zal worden of *Security Technical Implementation Guides (STIGs)* hiervoor kunnen worden gebruikt.

[13] Tot stand gekomen op basis van de BIR 2017

In aanvulling op de initiatieven in de brief, zullen ook de volgende zaken worden opgepakt:

- *Uitwerking proportionele beveiliging*: de BIR 2017 legt de nadruk op een proportionele beveiliging van informatie en informatiesystemen, door de introductie van BBN's (Basisbeveiligingsniveaus). Daarbij is een differentiatie aangebracht in de verantwoordelijkheid voor:
  - het risicomanagement;
  - het verlenen van toestemming voorafgaand aan ingebruikname;
  - monitoring / controle achteraf.

  Zowel de verantwoordelijkheidsverdeling als de inhoud van deze onderwerpen zullen worden uitgebouwd. Het onderdeel gerubriceerde informatie (waaronder staatsgeheimen) en continuïteit van vitale systemen zal daarbij integraal worden meegenomen. Daarbij wordt ook aangesloten op het vraagstuk van rolverdeling dat uit de ontwikkeling van BBN3 is voortgekomen. Bij het uitwerken van het onderwerp monitoring / controle zal worden bezien welke aansluiting op de Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn) nodig is; ook kan voor gerubriceerde informatie worden gedacht aan een systeem van hands-on inspecties;
- *Bepalen en formaliseren CISO-rol:* bij ieder ministerie bestaat een Chief Information Security Officer (CISO). De taken die bij deze rol horen zijn niet geformaliseerd en daardoor verschilt het feitelijk takenpakket van de CISO per ministerie aanzienlijk. De CISO opereert in het speelveld met de CIO en de Beveiligingsambtenaar (BVA), waarbij de rol van deze laatste in het Beveiligingsvoorschrift Rijksdienst 2013 (BVR) is geformaliseerd. Voor het juiste mandaat in het rijksbrede CISO-overleg moet een minimale set taken van de CISO rijksbreed worden vastgelegd. Dit wordt bekeken in samenhang met de herijking van de rol van de departementale CIO;
- *Evaluatie rubriceringsschema:* het instrumentarium voor het rubriceren van informatie en het beveiligen van deze informatie kan beter aansluiten bij de praktijk. Twijfel over het benodigde beveiligingsniveau kan leiden tot structureel te hoge rubriceringen. De hiermee gepaard gaande hoge beveiligingskosten, ook bij de ontvangers van gerubriceerde informatie, zijn moeilijk te verantwoorden. Voorts is schaarse specialistische technische kennis van geavanceerde dreigingen nodig. Voorgesteld wordt om het stelsel te evalueren om te komen tot een systeem van rubriceringen waarin lijnmanagement en medewerkers intuïtiever

zorgvuldig met gevoelige informatie kunnen werken. In aansluiting op internationale ontwikkelingen, zoals de vereenvoudiging van het rubriceringschema in het Verenigd Koninkrijk (gerealiseerd) en in Frankrijk (loopt), is vermindering van het aantal rubriceringsniveaus een te onderzoeken optie.

2.3 Privacy

De overheid komt in belangrijke mate aan de haar benodigde informatie doordat burgers die aan haar toevertrouwen. Zij mogen in ruil verwachten dat de overheid deze persoonsgegevens op een verantwoorde manier beschermt en privacy te allen tijde goed geborgd is. Op privacy-gebied heeft de overheid daarom een voorbeeldfunctie naar de maatschappij. In 2018 is een nieuwe privacy-rol en -procedure voor rijksbrede trajecten geïntroduceerd, de *PAR (Privacy Adviseur Rijksbrede Kaders en Voorzieningen)*.

Specifiek worden de komende planperiode de volgende acties ondernomen:

- Faciliteren van doorlopende aandacht voor compliance aan de AVG;
- Integreren van de PAR-procedure binnen de bestaande rijksbrede governance;
- Onderzoeken of de Quick scan Informatiebeveiliging kan worden geïntegreerd binnen het bestaande Rijksmodel *PIA*;
- Starten van een onderzoek naar de mogelijkheden van een standaard authenticatiefunctie voor afhandeling van inzage- en Wob-verzoeken;
- Initiëren van overleggen om de implementatie van de nieuwe *e-Privacy Verordening (ePV)* te ondersteunen, wat naar verwachting in 2020 zal starten;
- Opzetten van een rijksbreed privacy-platform.

2.4 Data

Een vraagstuk dat steeds belangrijker wordt is hoe de Rijksdienst met data omgaat. De Rijksdienst verwerkt al heel lang veel gegevens, denk aan het NFI, de IND, DUO, de Belastingdienst en Rijkswaterstaat. Door technologische ontwikkelingen, zoals slimmere apparaten met sensoren, komt in

hoog tempo meer data beschikbaar. Door gebruik te maken van data-analysetools en visualisatiemogelijkheden kan de Rijksdienst data steeds beter toepassen in alle processen. Door data in te zetten in beleid, uitvoering, bedrijfsvoering en toezicht worden processen niet alleen efficiënter en beter, maar ook vaak goedkoper. Om de kwaliteit van overheidshandelen te kunnen garanderen is een goede datakwaliteit dan ook essentieel, evenals heldere afspraken over het gebruik en de uitwisseling van deze data.

Informatiegericht werken betekent het beschikbaar hebben van gegevens en de functies die erbij horen om deze gegevens te kunnen verwerken op het moment wanneer deze nodig zijn. Dit betekent dat de functies en gegevens centraal moeten gaan staan en niet de applicaties die de functies leveren (ofwel: het voorkomen van *legacy* en *vendor lock in*). Ook *dataportabiliteit* is een belangrijk uitgangspunt hierbij.

Het managen van de complexe data-vraagstukken waar de Rijksdienst voor staat, vraagt dus een inzet op zowel organisatorisch vlak met regie op data als innovatieve partnerschappen met marktpartijen en wetenschap.

Begin 2019 verschijnt de overheidsbrede Nationale Data Agenda. Ook innoveren ministeries reeds met datalabs en samenwerkingsverbanden. Zoals in de inleiding genoemd, zal aan het begin van de planperiode van deze I-agenda worden bepaald hoe departementale CIO's het best gezamenlijk op kunnen trekken op het gebied van o.a. data-analyse en de bijbehorende uitdagingen, zoals andere eisen aan de inzet van mensen en systemen. Daarnaast zullen de departementen onderling kennis uitwisselen over inzet van data, zoals benoemd bij Kennis en kunde verderop in deze I-agenda.

3 ICT

3.1 Connected enterprise en gemeenschappelijke voorzieningen

Een samenhangende Rijksdienst

Het belang van samenwerking binnen de Rijksdienst neemt verder toe. Rijksambtenaren moeten efficiënt kunnen samenwerken, daarbij ondersteund door goed werkende en samenhangende ICT. Er moet rekening gehouden worden met eigen eisen die internationale samenwerkingsverbanden van ministeries kunnen stellen aan die samenwerking. Daarom zijn gezamenlijke rijksbrede inrichtingseisen voor interoperabiliteit nodig. Dit traject is al in gang gezet met de vorige I-strategie. Intussen is het Interoperabiliteitskader voor Digitale Werkomgevingen in de Rijkskantoren (IDWOR) voor het grootste deel gerealiseerd. Er zal aandacht worden besteed aan de verdere implementatie hiervan. Waar mogelijk en zinvol wordt aansluiting gezocht bij de afspraken over interoperabiliteit die per sector gelden, of die in internationaal verband worden gemaakt.

In deze planperiode wordt de interoperabiliteit van de afzonderlijke systemen verder onderzocht en uitgewerkt. Ook de samenwerking tussen diverse onderdelen van de Rijksdienst, inclusief uitvoeringsorganisaties, als "*connected enterprise*" wordt verder versterkt, net als de controle op naleving van de bestaande kaders.

Het bovenstaande betekent niet noodzakelijk dat alle voorzieningen gemeenschappelijk voor alle departementen gaan gelden – dat is vaak onmogelijk –, maar dat ervoor wordt gekozen om de diversiteit te managen en verbinden. Dit is gericht op samenhang en interoperabiliteit van systemen en het ondersteunen van processen die hergebruik van (bron)gegevens mogelijk maken. Eenmalige vastlegging en uitwisseling van data, bijvoorbeeld tussen uitvoeringsorganisaties, zal dan ook specifieke aandacht krijgen in het CIO-beraad. Er wordt gewerkt aan een I-landschap dat is gekoppeld volgens heldere standaarden. Diversiteit gekoppeld aan goede kennisdeling levert als bijvangst extra inzichten op die Rijksbreed ingezet kunnen worden.

Gemeenschappelijke voorzieningen waar nodig

Een aantal initiatieven rond gemeenschappelijke voorzieningen wordt in deze planperiode van de I-agenda doorgezet. Het gaat hier om generieke kaders, diensten en producten die beschikbaar worden gesteld aan alle organisaties binnen de Rijksdienst om standaardisatie en hergebruik te stimuleren. Daarnaast wordt in 2019 bezien welke innovatieve gemeenschappelijke toepassingen later worden toegevoegd aan danwel nader uitgewerkt in de roadmap. Het betreft de volgende gemeenschappelijke initiatieven:

- *Vernieuwen Rijksportaal*: het verzorgen van één toegang tot een scala aan rijksbrede en departementspecifieke informatiebronnen en toepassingen voor rijksambtenaren vraagt om vernieuwing. Vanuit een nog te ontwikkelen sourcingstrategie wordt onderzocht hoe hier afgewogen producten en diensten uit de *(public) cloud* kunnen worden ingezet;
- *Onderzoeken Samenwerkfunctionaliteit (SWF)*: in 2018 is besloten een onderzoek te starten naar een volwaardig alternatief voor de bestaande omgevingen voor samenwerking tussen ambtenaren onderling en met externe partijen;
- *Single-sign-on (SSOn) Rijk-platform*: in 2017 en 2018 is rijksbrede *SSOn*-toegang tot *cloud*-voorzieningen voor departementen gerealiseerd, op een pragmatische en gecontroleerde wijze. Dat betekent dat rijksambtenaren zich niet onnodig hoeven aan te melden op ICT-voorzieningen en op een veilige manier toegang krijgen. Er worden een visie en scenario's ontwikkeld om *SSOn* binnen de Rijksdienst toekomstvast neer te zetten. Dat is nodig om goed in te kunnen spelen op de toenemende vraag, op ontwikkelingen die de Rijksdienst doormaakt in de dienstverlening naar burgers en bedrijven en op de wens om rijksambtenaren via de eigen (mobiele) digitale werkplek veilig en eenvoudig toegang te kunnen geven tot *cloud*-voorzieningen;
- *Rijkspas*: De multifunctionele toegangspas wordt doorontwikkeld en vernieuwd om de veiligheid en betrouwbaarheid te borgen én in te spelen op technologische ontwikkelingen en nieuwe (digitale) gebruikerswensen. Om steeds beter het hoofd te bieden aan cybercrime en in lijn met de BIR 2017 wordt de komende jaren expliciet aandacht gegeven aan veilige digitale processen. De Rijkspas is hiervoor standaard uitgerust met chiptechnologie voor multifactor-authenticatie (het benutten van twee of meer factoren om een identiteit en daaraan

gekoppelde toegangsrechten te verifiëren). Een groeiende behoefte aan nieuwe toepassingen als de digitale handtekening, *smart card logon*, digitalisering van (self-service) aanvragen en uitgifte van middelen, kan door de Rijkspasvoorziening worden ingevuld. Door gebruik te maken van dezelfde pas, dezelfde identiteiten en dezelfde processen zijn de toepassingsmogelijkheden vrijwel onbeperkt uitbreidbaar en opschaalbaar. De ICT-dienstverleners spelen een belangrijke rol bij het beschikbaar stellen van deze functionaliteiten in de werkomgeving;

- *Rijks Identity Management (RidM)*: door een centraal gecoördineerde kwaliteitsverbetering van identiteitsgegevens is een betrouwbaar Rijk Identificerend Nummer ontstaan dat ook een uniek koppelnummer is voor het verstrekken van middelen en voorzieningen aan medewerkers. Er is gewerkt aan een veilige en betrouwbare uitwisseling van gegevens tussen departementale systemen en centrale voorzieningen. Centrale voorzieningen zoals de Rijkspas en mobiliteitskaart worden eenmalig verstrekt en gaan een loopbaan lang mee. Gemeenschappelijke afspraken borgen een veilige en betrouwbare uitgifte en beheer van rijksbrede middelen. Het normenkader wordt in 2019 aangevuld met normen voor de dienstverleners van de centrale voorzieningen;
- *Overheidsdatacenters:* ICT-dienstverleners binnen de Rijksdienst maken voor de huisvesting van hun eigen hardware (*housing*) altijd gebruik van een van de vier overheidsdatacenters (ODC's). De consolidatie van datacenters loopt volgens plan. Bij veranderende omstandigheden wordt de planning opnieuw bekeken. Het inzicht in de consolidatie staat in de "plot"[14] van de ICBR. Aanpassingen van de plot hebben altijd instemming nodig van de CIO Rijk en het CIO-beraad. De lopende plot van de ICBR zal naar verwachting in december 2019 worden afgerond, waarmee de basis wordt gelegd voor verdere kwaliteitsverbetering van de ODC's, waarbij ook de mogelijkheden van (public) *cloud* worden meenomen;
- *Enterprise Architectuur Rijk (EAR)*: in deze planperiode wordt een onderzoek uitgevoerd naar relevantie van en het benodigde onderhoud aan de Enterprise Architectuur Rijk (EAR). De EAR moet verwijzingen naar architectuurafspraken in de primaire processen van specifieke sectoren bevatten en verwijzen naar de Nederlandse Overheid Referentie

[14] Bindend schema voor datacenter consolidatie

Architectuur (NORA). Het CIO-beraad zal vervolgens bepalen wat het doel van de EAR op lange termijn is.

In de Kamerbrief "Sturing op informatiebeveiliging en ICT binnen de Rijksdienst" staan de volgende initiatieven op het gebied van informatiebeveiliging reeds vermeld:

- *Vulnerability scanning:* ontwikkeling en inrichting van een gezamenlijke faciliteit voor vulnerability scanning. Dat wil zeggen: het geautomatiseerd controleren van alle systemen van de Rijksdienst die met het internet zijn verbonden op bekende kwetsbaarheden;
- *Uitbouw van het Nationaal Detectie Netwerk (NDN) bij de Rijksdienst:* het NDN is steeds effectiever als meer partijen aansluiten. Toenemende digitale dreigingen verhogen de urgentie van deze maatregel voor een goede informatiebeveiliging binnen de Rijksdienst. De ministeries hebben daarom afspraken gemaakt over een versnelde uitbouw van het NDN bij de Rijksdienst;
- *Staatsgeheime werkplek:* er wordt een gezamenlijk kader voor een voorziening voor staatsgeheime toepassingen ontwikkeld. Mede op basis van dit kader wordt de haalbaarheid van een gezamenlijke voorziening onderzocht, die recht doet aan de specifieke eisen van departementen en internationale eisen, zodat deze voorziening zo breed mogelijk binnen de Rijksdienst kan worden ingezet.

Uit Interoperabiliteit, Rijks Identity Management (RidM) en informatiehuishouding volgt ook de ontwikkeling van een aantal noodzakelijke voorzieningen, waaronder:

- VC-brug (ondersteuning rijksbreed videovergaderen);
- MasterCas (gezamenlijk printen in rijkskantoren);
- Platform Open Overheid Informatie (PLOOI), bevordert de vindbaarheid van gepubliceerde open overheidsinformatie door openbaar gemaakte documenten te ontsluiten op Overheid.nl en andere geselecteerde websites;
- WID-scan hub (veilig uitwisselen van wettelijke identificatiedocumenten);
- *Harvesting* van websites (archiveren van aan de Rijksdienst gerelateerde websites).

3.2 Sourcing en inkoop

De Rijksdienst maakt gebruik van de markt als dat kan, maar doet zaken zelf als het noodzakelijk of beter is. Om optimaal gebruik te maken van de deskundigheid en mogelijkheden van marktpartijen worden komende periode een sourcingstrategie en de bijbehorende bouwstenen verder uitgewerkt. Zo wordt het gebruik van (standaard-) producten en diensten uit de markt bevorderd. Belangrijke aandachtsgebieden hierbij zijn het afgewogen gebruik van producten en diensten uit de zogenaamde (public) *cloud* en de wijze waarop het Rijk omgaat met softwareontwikkeling en applicatiebeheer. Hiervoor wordt een instructie geschreven.

Uiteraard moeten dienstverleners voldoen aan alle wetten en regels, voor zover relevant voor hun dienstverlening, zoals de BIR (hieronder valt ook nationale- en economische veiligheid) en de AVG. Voorwaarden worden altijd vastgelegd in verifieerbare contracten. Hoewel dit speelt bij alle externe vormen van dienstverlening, is er bijzondere aandacht voor "hosting" door een marktpartij. Daarbij moet worden gedacht aan: *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 afweging zal bij open overheidsdata uiteraard tot andere uitkomsten leiden dan bij gegevens die gerubriceerd zijn als staatsgeheim.

Aan het besluit om een externe partij in te zetten of om een dienst aan te besteden gaat een risicoanalyse vooraf en waar nodig een *Privacy Impact Assessment (PIA)*. Het risico van afhankelijkheid van één leverancier (*vendor lock-in*) wordt altijd zo klein mogelijk gemaakt, bijvoorbeeld door consequent gebruik van vastgestelde open standaarden.

In de voorgaande planperiode van de I-agenda is de Handreiking Sourcing opgesteld. Met de handreiking kan in een specifiek geval worden afgewogen of een externe vorm van dienstverlening een passende en kosteneffectieve oplossing is, of dat een dienstverlener binnen de Rijksdienst beter is. *Sourcing* moet snel en doelgericht, op zo'n manier dat ook kleine innovatieve spelers mee kunnen doen om functionaliteiten (bijv. rekenregels) te leveren. Bij *sourcing*-afwegingen spelen verder criteria een rol als (functionele) kwaliteit van software, privacy (AVG), kosten,

eisen aan de informatiebeveiliging (nationale veiligheid), continuïteit van de dienstverlening en het risico van afhankelijkheid van één leverancier of beschikbaarheid van beperkte cruciale expertise. Er wordt onderzocht hoe innovatieve partnerschappen en marktoplossingen kunnen worden ingezet waar risicoafwegingen dit toestaan.

Prioriteiten rondom interne leveranciers / shared service centers zijn:

- *Vereenvoudiging landschap IDV en IDV-dienstverlening*: het landschap van ICT-dienstverleners binnen de Rijksdienst is de afgelopen jaren gegroeid en tamelijk ingewikkeld geworden, onder meer als gevolg van de grote diversiteit in de aangeboden diensten. Vereenvoudiging en specialisering is mogelijk en nodig. Op basis van de herijking van onder meer de sourcingstrategie zal worden bezien wat dit betekent voor het interne landschap van ICT-dienstverleners en hun dienstverlening;
- *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 zo laag mogelijke kosten. In deze planperiode wordt een benchmark uitgevoerd waarin de prijs (kosten) en geleverde kwaliteit van diensten van interne ICT-dienstverleners worden vergeleken, rekening houdend met de verschillen in regelgeving.

Rondom inkoop en de gerelateerde thema's zoals categoriemanagement, strategisch leveranciersmanagement, *Software Asset Management (SAM)* en externe leveranciers zijn in samenwerking met het ICT-domein de plannen:

- *Inkoop*: de versterking van inkoop en het optimaliseren van de inrichting worden voortgezet. categoriemanagement (CM) en strategisch leveranciersmanagement (SLM) ondersteunen sourcingsbeslissingen door het inbrengen van kennis over de ICT-markt, kennis van de cyclus van producten en diensten en ervaringen met aanbestedingen en het uitnutten van contracten en door het effectiever controleren en sturen op afgesproken dienstverlening (waaronder beveiliging);
- *Versterken en professionalisering van de ICT-inkoop:* 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 toebedeelde inkoopcategorieën. Het inkoopstelsel kent zeven ICT-inkoopcategorieën: ICT Werkomgeving Rijk, Datacenters, Dataverbindingen, ICT-inhuur, *Enterprise Business Applications*, Totaaloplossingen en Standaard Software. Ook is voor een vijftal ICT-leveranciers strategisch leveranciersmanagement (SLM) ingericht. In 2019 vindt een herijking van de categorieën plaats om het categoriemanagement op een strategischer niveau te brengen en daarmee een volgende stap te maken in deze ontwikkeling. Dit kan mogelijke leiden tot een nieuwe herindeling en herverdeling van de ICT-inkoopcategorieën, aansluitend op de wensen van opdrachtgevers;

- *Rijksbreed 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 Rijksdienst. Deze ervaring leert dat de opzet van strategisch leveranciersmanagement rijksbreed inzicht en overzicht over deze leveranciers oplevert, wat de positie van de Rijksdienst als opdrachtgever versterkt. 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 de Rijksdienst aan de markt. Deze ontwikkeling wordt voortgezet. De uitbreiding van het rijksbreed strategisch leveranciersmanagement met de leveranciers KPN en IBM is gaande. Voor de uitvoering zal voor deze leveranciers een rijksbrede leveranciersmanager worden benoemd, die namens de Rijksdienst richting deze leveranciers zal optreden;
- *Software Asset Management*: voor de versterking van het rijksbreed strategisch leveranciersmanagement wordt gewerkt aan de ontwikkeling van Software Asset Management (SAM) binnen de Rijksdienst. Dit geeft inzicht in de software die binnen de Rijksdienst in gebruik is. Een rijksbreed programma ondersteunt de ministeries in de ontwikkeling van hun SAM, zodat de strategisch leveranciersmanagers een rijksbreed beeld krijgen. Met de licentie-informatie die beschikbaar komt, kunnen strategisch leveranciersmanagers een strategie en aanpak namens de Rijksdienst ontwikkelen richting de leverancier(s). Gelijktijdig met deze

ontwikkeling wordt gewerkt aan het opstellen van een rijksbreed kader voor SAM, waarin wordt aangegeven welke rollen, taken en verantwoordelijkheden de betrokkenen hebben bij het benutten van de beschikbare informatie. Het streven is om het rijksbrede kader in 2019 gereed te hebben.

- *Digitaliseringsstrategie Rijksinkoop*: leidende digitaliseringsthema's binnen de Rijksinkoop zijn:
  - Het meer delen en combineren van data en informatie ter ondersteuning van de strategische en waardetoevoegende rol van inkoop;
  - Het herontwerpen en volledig automatiseren van de operationele inkoopprocessen om de efficiëntie en rechtmatigheid te verbeteren;
  - Het voor klanten en gebruikers makkelijker maken van bestellen;
  - Het versimpelen en verder digitaliseren van het aanbestedingsproces om administratieve lasten voor leveranciers en inkoopadviseurs te verlagen.

  Voor digitalisering van deze en andere Rijksinkoopprocessen is een strategie ontwikkeld die rekening houdt met het complexe landschap waarin de Rijksinkoop opereert en met lessons learned die afgelopen jaren bij ICT-projecten zijn opgedaan. Het accent ligt in deze digitaliseringstrategie op een benadering met ruimte voor verschillende initiatieven, maar ook met aandacht voor samenhang en synergie: *Managed Diversity*. De komende periode wordt deze digitaliseringsstrategie verder uitgewerkt en geïmplementeerd. Belangrijke onderdelen in deze strategie zijn de benoeming van een portefeuillehouder digitalisering, het instellen van een board waarin periodiek de projectenportfolio wordt besproken en het instellen van een architectuurboard, allen specifiek gericht op inkoop;
- *Digitale veiligheid van hard- en software (DVHS)*: met de "Roadmap Digitaal Veilige Hard- en Software"[15] heeft de staatssecretaris van EZK een samenhangende aanpak geboden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software. De Roadmap geeft mede invulling aan de Nederlandse Cybersecurity Agenda (NCSA). Via de Roadmap DVHS is inmiddels aan de Tweede Kamer gemeld dat de Rijksoverheid de digitale veiligheid van de gehele productontwikkelingscyclus kan bevorderen. Door criteria hierover in

[15] *Kamerstukken II* 2017/18, 26643, 535

het inkoopbeleid op te nemen moeten aanbieders van de overheid voldoen aan deze eisen. De overheid kan met haar inkoopbeleid de vraagzijde van digitaal veilige producten stuwen. Zij is namelijk een belangrijke gebruiker. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten op de markt te brengen. Ook geeft de overheid hiermee het goede voorbeeld: kijk naar de digitale veiligheid van hard- en software voordat je dit koopt. Zodoende wordt onderzocht welke aanvullende maatregelen voor de digitale veiligheid van hard- en software bij inkoop binnen de (Rijks)overheid nodig en gewenst zijn;

- *Werken aan een professionele omgangsvorm met de markt:* de markt (samen met de wetenschappelijke wereld) is voor de Rijksdienst de belangrijkste bron van kennis en innovatie. Het is belangrijk dat de netwerken voor uitwisseling van informatie, kennis en ideeën worden onderhouden en uitgebouwd. Er zal daarom ook gezocht worden naar samenwerkingsvormen om een integere en rechtmatige, tevens ontspannen omgang met de markt mogelijk te maken. Ook wordt meer aandacht besteed aan marktconsultaties, *challenges* en bijeenkomsten waarin ambtenaren en medewerkers van marktpartijen en andere kennispartners elkaar kunnen ontmoeten en informatie kunnen uitwisselen;
- *ICT en duurzaamheid*: ook de duurzaamheid van de ICT is van belang. ICT-hardware is een van tien risicocategorieën waarop de Internationale Sociale Voorwaarden[16] van toepassing zijn. Dit kader betreft het voorkomen van misstanden in de productieketen. Energie-efficiency is een vereiste vanuit de Europese energie-efficiency richtlijn[17] en ook het kabinetsbeleid gericht op de circulaire economie heeft invloed op de ICT van de Rijksdienst[18]. Afgedankte ICT-apparatuur van de Rijksdienst wordt zoveel mogelijk voor hergebruik aangeboden en er wordt onderzocht hoe de levensduur verlengd kan worden. Verduurzaming van de ICT sluit aan bij de kabinetsambitie om de inkoopkracht van de overheid beter te benutten voor de duurzame transitie van Nederland

[16] *Actieplan MVI Rijkinkoopstelsel, www.rijksoverheid.nl/documenten/rapporten/2017/10/24/actieplan-mvi-rijksinkoopstelsel*

[17] Richtlijn 2012/27/EU van het Europees Parlement en de Raad van 25 oktober 2012 betreffende energie-efficiëntie

[18] *Kamerstukken II* 2017/18, 32852, 59

en bij de kabinetsreactie op de transitieagenda's circulaire economie. Doelen zijn onderdeel van het door de ICBR vastgestelde programma duurzame bedrijfsvoering Rijk en het actieplan MVI Rijksinkoopstelsel (Maatschappelijk Verantwoord Inkopen). De ambitie om zoveel mogelijk ICT te hergebruiken is door de minister van BZK recent nog bevestigd aan de Kamer[19]. De ICT-dienstverleners werken hierin samen via een verduurzamingsagenda ICT. Duurzaamheid wordt daarbij actief verbonden aan de andere thema's van de I-agenda. Meer inzicht in de productieketen en een zorgvuldige schoning en afdanking van apparatuur dragen bijvoorbeeld bij aan de veiligheid. Slim sturen op energie-efficiency en levensduurverlenging leiden tot lagere kosten.

[19] *Kamerstukken II* 2018/19, 30196, 610

4 Kennis en kunde

4.1 Kleine stappen in plaats van grote projecten

Goede ICT-ontwikkeling vereist een goede balans tussen robuustheid en lenigheid. Steeds vaker worden diensten en systemen bij de Rijksdienst daarom in kleine stappen (door)ontwikkeld. Dit betekent sneller resultaat met minder risico op grote fouten en ruimte voor aanpassingen onderweg. De kortcyclische aanpak werkt zowel bij nieuwbouw als bij onderhoud van bestaande systemen (*legacy*), biedt meer ruimte voor experiment en is zichtbaar als een meer permanente stroom van kleine vernieuwingen. *Permanent bèta* en leren van fouten horen hierbij. Uitgangspunt blijft dat men bij doorontwikkeling altijd moet kunnen teruggevallen op een werkende, eerder gebruikte versie van een systeem. Hiermee worden veiligheid, betrouwbaarheid en bruikbaarheid van overheids-ICT verbeterd. Deze en andere uitgangspunten komen in een handreiking 'beheerst vernieuwen', die samen met andere overheidslagen ontwikkeld wordt voor overheidsbreed gebruik.

Een succesvolle implementatie van deze werkwijze vraagt een organisatorische aanpassing van werkprocessen en cultuuromslag bij medewerkers en het management. Naast technologische vernieuwing is hier dus sprake van proces en sociale innovatie. Deze aspecten zullen ook in de handreiking meegenomen worden.

4.2 Verbinden van kennis en kunde binnen de I-community

In de vorige I-agenda stond dat er een kennisbank zou worden ingericht om documentatie, kennis en ervaringen uit ICT-projecten tussen departementen te delen. Omdat er al diverse platforms beschikbaar zijn, lijkt het verstandiger en waardevoller om eerst bestaande platforms, fora en expert-communities beter met elkaar te verbinden. Samen met de andere koepels binnen de overheid zal een verkenning worden uitgevoerd om al deze platforms in zicht te krijgen. Op basis van dit overheidsbrede beeld zal vervolgens een '*message house concept*' worden ontwikkeld, dat betekent

één landingspagina voor o.a. platforms en fora. Kennis en ervaringen van het BIT, de recent opgestarte Rijks Innovatie Community en uitvoeringsorganisaties krijgen hierin ook een plek. De verbreding van rijksbreed naar overheidsbreed kennisdelen past binnen de kabinetsvisie.

Zoals in de inleiding aangegeven, volgt het CIO-beraad de ontwikkelingen rondom onderwerpen als data en artificial intelligence en deelt hierover onderling kennis.

4.3 Versterken I-bewustzijn en I-vaardigheden beleidsmakers (RADIO)

Succesvolle digitalisering van de Rijksdienst vraagt niet alleen voldoende ICT'ers, maar vooral ook dat "gewone" ambtenaren (inclusief management) in beleid, uitvoering en toezicht, voldoende inzicht hebben in de mogelijkheden en effecten van digitalisering op hun werk. Het recent gestarte initiatief RADIO (RijksAcademie voor Digitalisering en Informatisering Overheid) moet daarom krachtig uitgebouwd worden. De focus van de opleidingen van RADIO ligt op het herkennen van de impact van beleid op uitvoering, opdrachtgeverschap, het inpassen van vernieuwing in bestaande processen en IT-landschap (zoals legacy), het veilig handelen, de omgang met privacy, de inzet van data en algoritmen, ethiek en ICT, etc.

Voor de iets langere termijn streeft RADIO ook naar de verbetering van de ICT-skills van de jonge instromende ambtenaren, door het uitbreiden van de ICT-component van opleidingen die door veel startende ambtenaren zijn gevolgd, zoals bestuurskunde.

RADIO zal voorts een nieuw aanbod ontwikkelen op basis van door de klankbordgroep en door de eigen organisatie aangegeven thema's en technologieën. Het gaat daarbij na ontwikkeling van een basiscursus ICT voor beleid voor de kerndepartementen om een klassikaal aanbod en *webinars* over nieuwe technologieën. Voor 2019 gaat het vooralsnog om kennisoverdracht over het inzetten van data en algoritmen (datagedreven beleid maken), *on going* aanbod, opdrachtgeverschap en het toepassen van de AVG, de omgang met privacy en informatiebeveiliging. Dit gebeurt

op klassikale, digitale en *blended* wijze. Daarbij zal ook gezocht worden naar aansluiting op aanbod wat al rijksbreed beschikbaar is, maar nog niet overal bekend of volledig uitgenut.

4.4 Versterken positie Rijksdienst als ICT-werkgever (HR ICT)

Om de digitaliseringsambities uit te voeren zijn voldoende kwalitatief goede ICT'ers nodig, zowel op de ministeries, dicht bij de beleidsmakers, als in de uitvoering. ICT is niet meer weg te denken in zowel bedrijfsvoering als primaire processen van het Rijk. De noodzakelijke ICT-kennis en -kunde om daarin toekomstbestendig te voorzien moet daarvoor op orde zijn. Daarom is het werven en ontwikkelen van ICT-talent van strategisch belang voor de Rijksdienst.

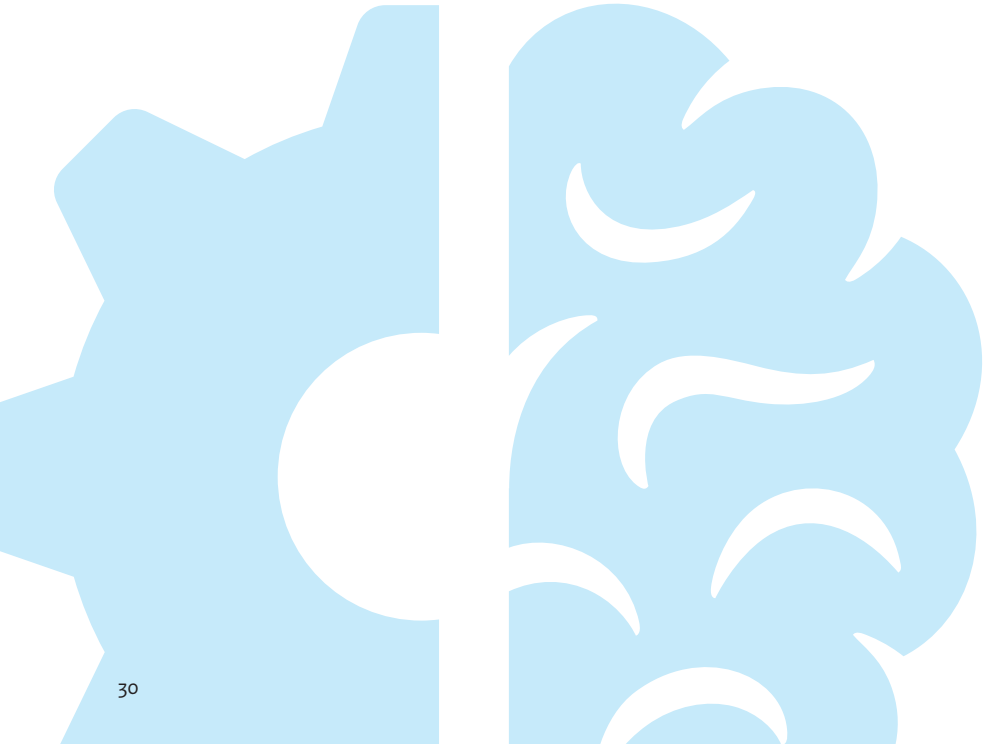
Medio 2018 is het interdepartementale programma Versterking HR ICT Rijksdienst 2018-2021 opgezet. Binnen dit programma wordt gewerkt aan (beleids)initiatieven ter bevordering van het aantrekken, ontwikkelen en behouden van ICT'ers bij de Rijksdienst. Het ministerie van BZK vervult daarbij de rol van aanjager, verbinder en platform voor kennisdeling.

Binnen het programma worden diverse rijksbrede initiatieven doorgezet, zoals een permanent opengesteld ICT-stageloket, het delen van CV's en twee jaarlijkse rijksbrede ICT-arbeidsmarktcampagnes.

Daarnaast wordt een verdere impuls gegeven aan de ICT-traineeprogramma's van het Rijk. Naast de continuering van het Rijks ICT Traineeprogramma en het meer specialistische Rijks Datascience (trainee) Programma wordt in 2019 een specialistische track op het gebied van cybersecurity opgezet. Aanvullende rijksbrede initiatieven worden toegevoegd, waaronder het opzetten van een om- en bijscholingsprogramma (I-flow) en het tot stand laten komen van een samenwerkingsplan tussen ICT-opleiders in het Hoger Onderwijs en de Rijksdienst.

In 2018 is gestart met het versterken van de informatiepositie over ICT-personeel, mede gebaseerd op een interdepartementale afbakening van ICT-profielen, wat ook bij zal dragen in de samenwerking tussen

departementen en het delen van schaarse resources. In 2019 wordt deze monitoringrol verder uitgewerkt en ingezet voor focus in de diverse initiatieven in het programma en strategische personeelsplanning.



5 Governance op I

De digitaliseringsambities van het kabinet vragen om integrale aansturing van alle I-aspecten, zowel binnen bedrijfsvoering als in het primair proces. Heldere gemeenschappelijke uitgangspunten, kaders en voorzieningen helpen hierbij. De minister van BZK heeft in de Kamerbrief "Sturing op Informatiebeveiliging en ICT binnen de Rijksdienst" aangegeven dat zij ook de sturing op I rijksbreed steviger wil invullen, onder meer door het gewijzigde "Coördinatiebesluit Organisatie en Bedrijfsvoering binnen de Rijksdienst" dat met de brief werd meegestuurd.[20]

De I-functie is afgelopen jaren volwassener en sterker geworden; de rol van de departementale CIO's[21] en hun offices verschuift organisch van controlerend op ICT-gebied naar partner in beleidsvorming en verander-manager. Het CIO-beraad ziet dit als een positieve ontwikkeling, omdat bijna elke beleidsaanpassing tegenwoordig I-aspecten heeft. De Rijksdienst zet daarom stappen naar "*I by design*": de rol van en impact op informatie, inclusief aspecten als informatiebeveiliging en privacy, worden zo vroeg mogelijk in het besluitvormingsproces meegenomen.

5.1 Versterking van de rol van de departementale CIO

De rol van de departementale CIO wordt versterkt door te zorgen dat zijn deskundigheid beter wordt ingezet bij besluitvorming in de beleids- en begrotingscyclus. Hiermee stuurt het departement op kritische succesfactoren van ICT-ontwikkeling. Het maatschappelijk belang komt hiermee ook eerder in beeld en beter aan bod.

Daarnaast wordt de rol en positie van de departementale CIO opnieuw gedefinieerd en daarmee verder versterkt. Dit past bij de verschuiving van de rol die in de praktijk plaatsvindt, van controlerend naar meer adviserend. Een belangrijk punt hierbij is dat de departementale CIO verant-

[20] *Stb.* 2018, 354

[21] Betreft ook de CIO's van de uitvoeringsorganisaties

woordelijk wordt voor het departementale I-plan (zie ook volgende paragraaf). De verantwoordelijkheid voor projecten en beheer blijft daarbij overigens bij de lijnorganisatie liggen. De CIO-oordelen die CIO's afgeven veranderen onder invloed van de wijzigende rol van de CIO. Een CIO-oordeel blijft formeel, maar kan en zal geen verrassing zijn. De impact van het CIO-oordeel wordt door de versterking van de rol van de CIO groter.

Het profiel van de departementale CIO uit 2016 wordt in overleg met de ministeries herzien en er komt een standaardparagraaf 'taken en bevoegdheden van de departementale CIO'. Departementen kunnen deze tekst opnemen in hun organisatie- en mandaatbesluiten.

Genoemde documenten zullen na vaststelling in het CIO-beraad en de ICBR worden doorgeleid naar SGO en Ministerraad voor akkoord.

5.2 I-cyclus: sturing op ICT integreren in de beleidscyclus en besluitvorming

De vorige I-agenda bevatte al passages over departementale I-plannen en dit onderwerp is verder uitgewerkt in de Kamerbrief "Sturing op informatiebeveiliging en ICT binnen de Rijksdienst". Daarin staat dat er een kwaliteitskader komt, gericht op doorontwikkeling naar kwaliteitseisen voor departementale I-plannen. Voor de kwaliteitseisen worden o.a. rijksbrede best practices, BIT-adviezen en lessons learned uit grote ICT-projecten gebruikt. De bedoeling is om zo beter zicht te krijgen op de consequenties van beleid voor het gehele bestaande ICT- en gegevenslandschap. Dit ondersteunt goed opdrachtgeverschap, een goede beheersing van ICT-ontwikkeling en -onderhoud en een betere aansluiting van de departementale informatieplanning op de begrotings- en beleidscyclus.

Voorbeelden van elementen voor het kwaliteitskader kunnen zijn: de geactualiseerde maatschappelijke opgave voor de organisatie, de beleidsdoelen die de organisatie stelt voor de komende periode, een overzicht van de gewenste vernieuwing op basis van de opgave en beleidsdoelen, een samenvattend overzicht van het projectportfolio om

dit te realiseren. Daarnaast ook onderhoudsaspecten, zoals een analyse van het bestaande applicatielandschap, een inventarisatie van het benodigde onderhoud en technische vernieuwing en een onderhoudsplan met de benodigde middelen. Hierbij wordt mogelijk een onderscheid gemaakt tussen het departementale I-plannen en meer technische beheers/onderhoudsplannen. Dit kwaliteitskader wordt in 2019 uitgewerkt, inclusief de aansluiting van de I-cyclus op de Rijksbegrotingscyclus.

5.3 Rijksbrede kaderstelling, monitoring en verantwoording op informatiesystemen Rijksdienst

In het najaar van 2019 zal de minister van BZK kenbaar maken hoe zij nadere invulling zal geven aan de monitoring van de kaders rondom informatiesystemen. Uitgangspunten zijn dat de effectiviteit van elk kader wordt bekeken en dat dubbele uitvragen worden voorkomen. Kamerlid Middendorp heeft via een motie[22] gevraagd om een mogelijke Rijksinspectie Digitalisering te onderzoeken. Relevante uitkomsten uit dat onderzoek komen ook terug in het genoemde advies.

De grote ICT-projecten van de Rijksoverheid worden sinds 2012 gepubliceerd op het Rijks ICT-dashboard en aan de Kamer gemeld in de Jaarrapportage Bedrijfsvoering. Deze transparantie, waarbij op uniforme wijze verantwoording wordt afgelegd over ICT-uitgaven, blijft belangrijk. Zeker ook als projecten voortaan in kleinere stappen plaatsvinden (‘*agile*’) en steeds meer geïntegreerd met ICT-beheeractiviteiten worden uitgevoerd. Beheeractiviteiten vormen immers het leeuwendeel van de totale ICT-kosten binnen de Rijksdienst. In 2019 zal een pilot uitgevoerd worden voor een mogelijk rapportagemodel dat past bij dat soort ICT-activiteiten. Dat model zal vervolgens getoetst worden op haalbaarheid en impact bij een aantal grote uitvoeringsorganisaties. De onderzoeksopdracht aan de ADR rond gegevens uit het ICT-dashboard wordt hierop daarna eventueel aangepast.

[22] *Kamerstukken II* 2018/19, 35000-VII, 34

Het Bureau ICT-Toetsing (BIT) is een tijdelijke organisatie, waarbij het uitgangspunt is dat de taken van het BIT op termijn overgaan naar de departementale CIO. Om de transitie mogelijk te maken wordt deze planperiode een aanzet gemaakt voor rollen en functies binnen departementale CIO-offices. Daarnaast worden standaard-elementen van een CIO-oordeel uitgewerkt in samenhang met/als onderdeel van het eerdergenoemde kwaliteitskader voor departementale I-plannen.

Bijlage Financiële paragraaf

De Strategische I-agenda Rijksdienst 2019-2021 is ambitieus en zal ook financiële implicaties hebben. Zoals in de Kamerbrief “Sturing op informatiebeveiliging en ICT binnen de Rijksdienst” is aangegeven, streeft het ministerie van BZK ernaar de benodigde middelen binnen de eigen begroting op te vangen.

Daarnaast zijn er ook de bestaande geldstromen voor gezamenlijke ontwikkeling van voorzieningen en voor bijvoorbeeld het programma HR ICT is een meerjarige bijdrage toegezegd door de ministeries. De ambities uit deze I-agenda zijn verder uitgewerkt dan de brief “Sturing op informatiebeveiliging en ICT binnen de Rijksdienst”. De rijksbrede investeringen die dit vraagt, zal het ministerie van BZK meenemen bij de vorming van de Voorjaarsnota. Ten slotte zullen uit deze Strategische I-agenda extra investeringen bij de ministeries voortvloeien. Deze investeringen zorgen ervoor dat de informatiehuishouding, informatiebeveiliging en de voorzieningen per ministerie op orde zijn. Ministeries dragen deze eigen kosten.

Bijlage Verklarende woordenlijst en afkortingen

ADR – Auditdienst Rijk

Agile – lenige, flexibele en iteratieve methodiek van (ICT-)ontwikkeling

AVG – Algemene verordening gegevensbescherming

Artificial intelligence – kunstmatige intelligentie

BBN – basisbeveiligingsniveau

Blended learning – een combinatie van online leren en contactonderwijs

BIO – Baseline Informatiebeveiliging Overheid

BIR – Baseline Informatiebeveiliging Rijksdienst

BIT – Bureau ICT-Toetsing

BVA – Beveiligingsambtenaar

BVR – Beveiligingsvoorschrift Rijksdienst

Challenges – werkwijze waarbij met behulp van start-ups innovatieve oplossingen voor bestaande problemen worden gezocht

CIO – Chief Information Officer

CIO-beraad – interdepartementaal overleg van *CIO's*

CISO – Chief Information Security Officer

Cloud computing (of kortweg cloud) –een leveringsmodel om op afroep op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare ICT-componenten (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers (zie ook *Public cloud*)

Connected enterprise – model van de Rijksdienst waarbij de nadruk ligt op interoperabiliteit

Dataportabilititeit – het (in een gestructureerde, gangbare en machineleesbare vorm) kunnen meenemen van data van de ene naar de andere leverancier

EAR – Enterprise Architectuur Rijk

ePV - e-Privacy Verordening

Early adopter – iemand die een bepaalde technologische innovatie gaat gebruiken voordat de grote massa dit overneemt

Enterprise Business Applications – een van de inkoopcategorieën binnen de Rijksdienst

Harvesting - archiveren van websites

Hosting – beschikbaar stellen van software

Housing - huisvesten van eigen hardware (buiten de eigen organisatie)

I by design – strategie waarbij tijdens de ontwikkeling van een product, dienst of beleid al zo vroeg mogelijk wordt nagedacht over de impact op en mogelijkheden van informatievoorziening

IaaS (Infrastructure as a Service) - een vorm van *cloud computing*. De infrastructuur wordt virtueel aangeboden, zodat organisaties er zelf software op kunnen installeren. De hardware, waaronder servers, zijn eigendom van de leverancier

ICBR – Interdepartementale Commissie Bedrijfsvoering Rijk

IDV – interne dienstverlener

Launcing customer - de eerste klant die een nieuw product in gebruik neemt en op basis van deze eerste ervaringen meedenkt over de doorontwikkeling daarvan

Legacy - bestaande systemen met een verlengde levensduur

Linked data - een manier om gestructureerde gegevens en onderlinge relaties via internettechnologie beschikbaar te stellen, zodat de gegevens door anderen betekenisvol gebruikt kunnen worden

Make or buy - een bedrijfsbeslissing die de voor- en nadelen van het zelf maken tegen het inkopen van een product afweegt, zoals kosten en flexibiliteit

Managed diversity - een benadering met ruimte voor verschillende initiatieven, maar ook met aandacht voor samenhang en synergie

Message house concept - een communicatieconcept dat in één oogopslag overzicht geeft over hoofdboodschap, deelboodschappen en onderbou-

wing, en helpt een lijn in de communicatie te brengen

NCSA – Nederlandse Cybersecurity Agenda

NORA – Nederlandse Overheid Referentie Architectuur

ODC – Overheidsdatacenter

PaaS (Platform as a Service) – een leverancier stelt een platform beschikbaar dat afnemers kunnen gebruiken, bestaande uit hardware, een besturingssysteem en databases (zie ook *Cloud computing*)

PAR – Privacy-adviseur rijksbrede kaders en voorzieningen

Permanent bèta - werkwijze waarbij software gebruikt wordt terwijl voortdurend wordt gewerkt aan nieuwe versies met bijvoorbeeld meer functionaliteit of meer gemak

PLOOI - Platform Open Overheid Informatie

Plot – het schema voor consolidatie van 64 rijksdatacenters naar 4 overheidsdatacenters (ODC's)

Privacy Impact Assessment (PIA) - privacy-effect-beoordeling, een gestandaardiseerd instrument om de impact van een voornemen op privacy-aspecten te kunnen bepalen

Public cloud - software en gegevens staan in deze vorm van *cloud computing* op de servers van een externe dienstverlener

Roadmap - een schema dat overzicht biedt op de planning van een complex project, programma of uitvoeringsagenda

SaaS (Software as a Service) - software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker, eventueel in combinatie met andere parameters (zie ook *Cloud computing*)

Security Technical Implementation Guides (STIGs) – technische handreikingen voor de inrichting van beveiliging van netwerken, servers, computers e.d., afkomstig van het Ministerie van Defensie van de Verenigde Staten

SGO - Secretarissen-Generaal Overleg

Single-sign-on (SSOn) – gebruikers melden zich eenmalig aan waarna zij toegang krijgen tot voorzieningen waar zij rechten op hebben, zonder dat zij zich hiervoor steeds opnieuw hoeven aan te melden

Smart card logon – stelt eindgebruikers in staat om aan te melden op een computer met een smart card in plaats van of in combinatie met een gebruikersnaam en wachtwoord

Software Asset Management (SAM) - het complete proces rondom het beheren en optimaliseren van de aankoop, het onderhoud en de implementatie van softwarepakketten binnen een organisatie

Sourcing - het proces waarbij bepaald wordt of werkzaamheden zelf worden gedaan, in samenwerking met anderen worden uitgevoerd, of worden uitbesteed aan een overheidsorganisatie of marktpartij

Vendor lock in – ongewenste afhankelijkheid van één leverancier

Vulnerability scanning – proces waarbij netwerken, computers en software worden gescand op bekende zwakheden

Webinar - online lezing, workshop, college of soortgelijke presentatie of vorm van kennisoverdracht

Wob – Wet openbaarheid van bestuur

Woo – Wet open overheid

Dit is een uitgave van CIO Rijk in
samenwerking met het CIO-beraad

Januari 2019