26643	Informatie- en communicatietechnologie (ICT)
Nr. 1417	Brief van de minister van Buitenlandse Zaken en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 oktober 2025

Met deze brief informeren wij uw Kamer over het advies van het Adviescollege ICT-toetsing (hierna: AcICT) over het programma Transitie ICT-dienstverlening. Dit advies hebben wij op 4 februari 2025 van AcICT ontvangen. Hierbij ontvangt u het rapport met de conclusie en de aanbevelingen van AcICT. Bij dit advies hoort nog een vertrouwelijke bijlage. Het integrale advies, dus inclusief die bijlage, is op 3 maart jl. al vertrouwelijk met uw Kamer gedeeld (Kamerstuk 26 643, nr. 1304). In deze brief gaan wij in op de conclusie uit het hoofdrapport en beschrijven wij op welke manier opvolging wordt gegeven aan de aanbevelingen.

Aanleiding

Op 14 februari 2011 presenteerde de toenmalige minister van Binnenlandse zaken en Koninkrijksrelaties (BZK) het uitvoeringsprogramma compacte rijksdienst (CRD)[1]. Onderdeel van dit programma was de inrichting van een rijksbrede infrastructuur voor de ondersteunende bedrijfsvoering, inclusief de ICT-dienstverlening. In het programmaplan CRD stond dat alle ministeries (met uitzondering van het ministerie van Defensie) de uitvoering van hun ICT-dienstverlening vanaf 2013 zo veel mogelijk zouden bundelen. Zo werd op 1 januari 2012 het nieuwe Shared Services Center ICT (SSC-ICT) in het leven geroepen, een onderdeel van het ministerie van BZK, met als belangrijkste startkapitaal de ICT-dienstverleningsorganisatie van het toenmalige ministerie van Infrastructuur en Milieu.

Op 1 januari 2015 stapte het ministerie van Buitenlandse Zaken (BZ) in als opdrachtgever voor SSC-ICT, en nam SSC-ICT een groot deel van de ICT-voorzieningen en -diensten over van BZ. Daarbij ging ook een deel van de Directie Informatie Diensten van BZ over naar SSC-ICT, en werd ervan uitgegaan dat SSC-ICT het beveiligings- en beschikbaarheidsniveau zou leveren dat voor het ministerie van BZ vereist is.

[1] Kamerstuk 31 490, nr. 54.

De samenwerking tussen BZ en SSC-ICT heeft van het begin af aan de nodige struikelblokken gekend. Dat is voor een belangrijk deel toe te schrijven aan de botsing van twee werelden. Aan de ene kant die van een shared services organisatie die is bedoeld om gedeelde, en tot op zekere hoogte identieke diensten te leveren aan verschillende afnemers. Daartegenover staat dat het werk en het werkterrein van BZ met zich meebrengt dat BZ specifieke behoeften heeft, en dat BZ extra bescherming nodig heeft tegen statelijke actoren met een offensief cyberprogramma dat is gericht tegen Nederlandse belangen. Verschillende incidenten hebben gemaakt dat BZ zich in de eerste helft van 2024 genoodzaakt zag om de levering van ICT-diensten te heroverwegen, met als uiterste consequentie het onderbrengen van – een deel van – de door SSC-ICT geleverde diensten bij een of meer andere aanbieders. In dat verband heeft de minister van Buitenlandse Zaken aan AcICT gevraagd om advies uit te brengen over de manier waarop dit moet worden aangepakt.

Advies programma Transitie ICT-dienstverlening

AcICT trekt op basis van hun onderzoek als belangrijkste conclusie dat zij het besluit van BZ om nu te vertrekken bij SSC-ICT te risicovol vinden, vanuit het perspectief van BZ, en met het oog op het rijksbrede belang. Bij deze conclusie zijn ter onderbouwing, kort samengevat, door AcICT de volgende bevindingen meegegeven:

A. Vertrek brengt de urgente verbetering van de informatiebeveiliging in gevaar.
B. Grote kans op herhaling problematiek dienstverlening door onvolwassen besturing BZ.
C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed.

AcICT adviseert op basis van deze conclusie om het vertrekbesluit op dit moment niet door te zetten en eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit te geven. Dit advies is door AcICT uitgewerkt in de vorm van vier aanbevelingen:

1. Zorg dat SSC-ICT en BZ de urgente beveiligingsrisico’s terugdringen.
2. Zorg dat de besturing bij BZ fundamenteel verbetert.
3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren.
4. Evalueer na 2 jaar gezamenlijk de opvolging van de adviezen.

Opvolging van het advies

Het advies van AcICT heeft een grote reikwijdte. Er was gevraagd om te adviseren over een programma dat is gestart door BZ, maar veel van de adviezen betreffen logischerwijs ook SSC-ICT, of de samenwerkingsrelatie tussen BZ en SSC-ICT. Als belangrijk puzzelstuk voegt AcICT daar een aanbeveling aan toe die te maken heeft met een rijksbrede verantwoordelijkheid, en die dus vooral is gericht aan BZK, in het bijzonder de directeur-generaal Digitalisering en Overheidsorganisatie (DGDOO). De drie organisatieonderdelen hebben het advies samen bestudeerd, en pakken ook samen de handschoen op die er nu ligt. Zij zien de aanbevelingen als richtinggevend voor de verdere verbetering van de rijksbrede samenwerking op het gebied van ICT-dienstverlening. Dat is concreet uitgewerkt in een programmaplan dat materieel op 1 juli jl. in uitvoering is genomen: het programma SHIELD (Samenwerkingsprogramma Herziening Informatiebeveiliging En Levering Diensten).

Het programmaplan is opgezet met gebruikmaking van de principes van *Managing Successful Programmes* (MSP). De essentie is onder andere dat, binnen de context van de programmaportfolio, verschillende projecten of andere activiteiten (in het jargon: inspanningen) worden uitgevoerd waarvan de resultaten in samenhang leiden tot concrete baten. De inspanningen zelf vallen niet onder de verantwoordelijkheid van het programma. SHIELD initieert, coördineert en integreert, maar de inspanningen zelf vallen onder verantwoordelijkheid van de staande organisaties, in principe een van de drie samenwerkende organisatieonderdelen: BZ, SSC-ICT en DGDOO.

Voordat SHIELD werd opgezet was een groot aantal inspanningen al van start gegaan. Dat geldt bijvoorbeeld voor het merendeel van de inspanningen die vallen onder verantwoordelijkheid van SSC-ICT. In 2024 zijn daar verschillende trajecten in gang gezet voor het aanpakken van urgente beveiligingskwesties. Inmiddels werpen die hun vruchten af. Daarmee is er nu ook, vanuit het perspectief van risicobeheersing, een natuurlijk moment ontstaan voor openbaarmaking van het advies van AcICT.

BZ en BZK hebben de handen ineengeslagen om, geholpen door het AcICT-advies, hun samenwerking op het ICT-dossier te versterken. Het advies is inmiddels gebruikt als een extra impuls voor de ontwikkeling van maatregelen om onder andere de weerbaarheid tegen statelijke actoren te versterken. De resultaten daarvan komen aan de hele rijksoverheid ten goede. In het vervolg van deze brief is beschreven hoe de verschillende aanbevelingen concreet zijn opgepakt.

Opvolging aanbeveling 1: zorg dat SSC-ICT en BZ de urgente beveiligingsrisico's terugdringen

AcICT adviseert SSC-ICT en BZ om samen urgente beveiligingsrisico's terug te dringen. Daarvoor heeft AcICT concrete maatregelen voorgesteld. De twee organisaties hebben deze voorstellen meegenomen bij de versterking en versnelling van bestaande initiatieven en als basis voor nieuwe, aanvullende maatregelen.

De verschillende initiatieven voor het aanpakken van beveiligingsrisico's zijn bij SSC-ICT ondergebracht in een Integraal Security Programma (ISP), dat in het voorjaar van 2024 van start is gegaan. De activiteiten van het ISP die specifiek zijn voor BZ, zijn ondergebracht in een Agile Release Train (ART BZ). Een deel van de gesignaleerde kwetsbaarheden had te maken met een achterstand in de vernieuwing van – componenten – van de infrastructuur. Voor de vervanging en het up-to-date houden van deze componenten loopt er nu een Life Cycle Management programma (LCM). Daarbij wordt gestuurd op het minimaliseren van risico's; de grootste beveiligingsissues komen als eerste aan de beurt. Naast ISP en LCM wordt er nog een derde programma uitgevoerd: het Integraal Control Framework (ICF). Dat bundelt alle activiteiten op het gebied van compliance en procesvolwassenheid.

AcICT adviseert SSC-ICT en BZ om samen op te trekken bij het aanpakken van beveiligingskwesties. Al enige tijd hadden SSC-ICT en BZ een tactisch security-overleg. Dat is naar aanleiding van het AcICT-advies uitgebreid. In aanvulling daarop wordt momenteel een gezamenlijk team opgezet waarin specifieke deskundigheid van de beide organisaties wordt gecombineerd, om meer focus aan te brengen in de verdere versterking van de informatiebeveiliging.

Specifiek voor de dienstverlening aan BZ bestaat er binnen SSC-ICT een zogenoemd klantteam. Dit klantteam is het centrale aanspreekpunt voor projecten en zogenoemde Niet Standaard Klantvragen (NSK's). Het klantteam is inmiddels ook uitgebreid. In de afgelopen periode heeft deze manier van werken geleid tot een versnelling van – het opstarten van – projecten en het reduceren van de doorlooptijd van de afhandeling van NSK's. Het aanpakken van kwetsbaarheden en beveiligingsissues wordt nu ook aangestuurd door dit klantteam. Zo kunnen BZ en SSC-ICT sneller schakelen, en eerder tot oplossingen komen. Ook op strategisch niveau vindt er intensieve samenwerking plaats in een specifiek voor BZ ingericht Bestuurlijk Overleg (BO). De belangrijkste punten op de agenda zijn de voortgang van de programma's ISP, LCM en ICF, en de

samenwerking tussen BZ en SSC-ICT. In het BO wordt de opvolging van het AcICT-advies gemonitord, zowel de maatregelen als de resultaten.

In het licht van het programma SHIELD heeft BZ een voorstel gedaan voor meetwaarden (*metrics*) en streefwaarden (*targets*) waaraan de dienstverlening van SSC-ICT aan BZ zou moeten voldoen. De uitvoeringstoets daarvoor is op dit moment in voorbereiding. Dat is de basis voor de definitieve vaststelling van de targets, en het doorvoeren van de daarvoor benodigde aanpassingen in de dienstverlening. Dit gebeurt binnen de scope van het programma SHIELD. Een van de nieuwe initiatieven binnen het kader van SHIELD is verder het valideren van de door BZ gevraagde dienstverlening in die zin dat wordt nagegaan welke dienstverlening goed past binnen de portfolio en de roadmap van een shared services center als SSC-ICT.

Opvolging aanbeveling 2: zorg dat de besturing bij BZ fundamenteel verbetert

BZ neemt niet alleen ICT-dienstverlening af van SSC-ICT, maar ook van andere leveranciers. In dat laatste geval gaat het bijvoorbeeld om connectiviteitsdiensten in het buitenland. Dit vraagt om zorgvuldige, samenhangende regievoering vanuit de opdrachtgever. In principe is het altijd aan BZ om de ‘wat-vraag’ concreet te beantwoorden, terwijl de leverancier de ‘hoe-vraag’ voor zijn rekening moet nemen. Voor SSC-ICT is de laatste vraag de kern van de dienstverlening; onder de motorkap moeten alle verschillende onderdelen, in stelling gebracht voor BZ maar ook voor andere ministeries, in samenhang effectief en efficiënt ingezet kunnen worden. Dat betreft niet zozeer de techniek, omdat er wordt gewerkt met gescheiden omgevingen, maar vooral de kennisbasis en de organisatiekant. Alleen, een complexe ‘wat-vraag’ is soms het eenvoudigst te formuleren in technische termen. BZ is zich goed bewust van deze valkuil. In de onderdelen van SHIELD die te maken hebben met verbetering van de sturing op de ICT-dienstverlening, waarbij BZ samen optrekt met SSC-ICT, staat het principe van strikte(re) rolscheiding hoog op de agenda. De aanbevelingen die AcICT doet voor het versterken van de besturing zijn gebruikt als evenzovele aanknopingspunten voor de desbetreffende plannen en projecten.

Al in de beginfase van het programma Transitie ICT-dienstverlening heeft BZ ingezien dat versterking van de vraagsturing noodzakelijk is om duurzaam en betrouwbaar te kunnen voorzien in de eigen ICT-behoeften. AcICT reikt daarvoor de volgende trits aan: risicomanagement – specificatie van eisen – regievoering. Dat wordt

door BZ gezien als een behulpzaam denkmodel. De aanbeveling om de eisen voor de ICT-dienstverlening – inclusief informatiebeveiliging – vooral in de combinatie van BZ en SSC-ICT beter uit te werken heeft dan ook een prominente plek gekregen in het programma SHIELD. In lijn met het advies van AcICT zullen programma's van eisen categorisch gebaseerd worden op risicoanalyses. Daarvoor sluit BZ zo veel mogelijk aan op een rijksbreed programma dat in het leven is geroepen voor de versterking van het risicomanagement.

Verder is BZ aan de slag gegaan met de manier waarop het opdrachtgeverschap wordt ingevuld. Voor de opdrachtgever-opdrachtnemerrelatie met SSC-ICT doet BZ dat samen met SSC-ICT. Dat is inmiddels zo opgenomen in de jaarplannen van BZ. De belangrijkste elementen daarbij zijn: contractmanagement, portfoliomanagement en architectuur. Daarvoor wordt ook extra capaciteit ingezet. Het resultaat van deze verbeteractie is dat de dienstverlening van alle leveranciers zorgvuldig georkestreerd wordt en dat de BZ-organisatie kan beschikken over passende voorzieningen: op tijd, tegen uitlegbare kosten, en veilig, gebaseerd op risicoanalyses die rekening houden met de bijzondere kenmerken van BZ. AcICT doet ook de oproep om in de aansturing van de opdrachtnemers rolvast en voorspelbaar te zijn, en daarbij de samenhang tussen de verschillende voorzieningen scherp in het oog te houden. BZ beschouwt dat als een speerpunt, en heeft hiervoor inmiddels belangrijke stappen gezet. Richting SSC-ICT is de regievoering op informatiebeveiliging nu gecombineerd met de gebruikelijke regievoering op de afzonderlijke voorzieningen. Er is nu één centraal punt voor het stellen van vragen en het prioriteren van de afhandeling daarvan.

De aanbeveling om de uitvoering van de processen op het gebied van informatiebeveiliging te verbeteren neemt BZ ter harte. Dat gebeurt onder andere door versterking van de regie – voor het onderwerp informatiebeveiliging – op de leveranciers. Zij zullen ervoor moeten zorgen dat de ICT-diensten consequent en navolgbaar zijn afgeleid van de toepasselijke *baselines*. Het verbeteren van de afhandeling van beveiligingsincidenten, waar AcICT voor pleit, heeft BZ meegenomen als onderdeel van het project C-SOC (Centraal Security Operations Center). Dat project gaat over het moderniseren en centraliseren van de huidige SOC-voorzieningen, over alle dienstverleners heen. BZ houdt daarbij rekening met de mogelijkheid dat er op enig moment een rijksbrede, ook voor BZ passende SOC-voorziening beschikbaar komt.

Terecht vraagt AcICT aandacht voor het naleven van de regels op het gebied van accreditatie. Voor BZ is dat essentieel. Ten eerste omdat actieve bescherming tegen statelijke actoren nodig is om de

weerbaarheid van de organisatie op peil te houden, maar ook omdat dit een vereiste is om de NATO/EU-accreditatie te behouden. De informatiebeveiligingseisen die hieruit voortvloeien worden daarom onverkort meegenomen als eisen die BZ als opdrachtgever stelt aan de ICT-dienstverlening.

Opvolging aanbeveling 3: realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren

De toenemende cyberdreiging die uitgaat van statelijke actoren vraagt voor de rijksoverheid om een integrale, gezamenlijke aanpak. Die conclusie is bijvoorbeeld te trekken uit het Cybersecuritybeeld 2024, waar ook AcICT naar verwijst. Samenwerking op het gebied van cybersecurity is daarnaast, breder dan binnen het Rijk, noodzakelijk in verband met de ketensamenwerking tussen partijen binnen en buiten de rijksoverheid. Dit betekent dat digitale risico's de grenzen van afzonderlijke ministeries ver overschrijden. Statelijke actoren en cybercriminelen werken steeds intensiever samen, beschikken over geavanceerde intrusietechnieken en maken gebruik van mondiale digitale infrastructuren. Deze actoren zien zogenoemde koppelvlakken en de scheidsvlakken tussen verantwoordelijkheden als dankbare aanvalspunten. We moeten de gelederen dus sluiten.

De oproep om te komen tot een rijksbrede aanpak tegen statelijke actoren wordt dus herkend en van harte onderschreven. AcICT richt zich met zijn aanbeveling in eerste instantie tot BZK, in de verwachting dat verschillende resultaten van die aanpak vervolgens BZ kunnen helpen om zijn doelstellingen te bereiken. De CIO Rijk heeft, in samenwerking met andere onderdelen van de rijksoverheid, al verschillende initiatieven gestart die aansluiten op deze aanbeveling. Bijvoorbeeld het traject Hoog-Gerubriceerde Informatie (HGI), waarover de Staatssecretaris Digitalisering de Tweede Kamer heeft geïnformeerd. Dit moet onder meer leiden tot centrale, gestandaardiseerde dienstverlening op het gebied van hoogbeveiligde voorzieningen. Daarnaast wordt er gewerkt aan de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO), gebaseerd op de aanpak van het ministerie van Defensie. Verder is er onlangs een kader opgesteld voor het risicomanagement dat van toepassing is op departementoverstijgende ketens. Bij de uitrol daarvan zijn de adviezen van AcICT goed te gebruiken. Op 4 juli jl. heeft de ministerraad ingestemd met een actualisatie van het VIR-BI, wat een kader vormt voor de beveiliging van bijzondere informatie, zoals staatsgeheimen. Tevens is de BIO, de baseline voor de beveiliging van informatie bij de overheid, geactualiseerd, inhoudelijk afgestemd en klaar om als verplicht normenkader vastgesteld te worden. Tot slot is er het programma Versterking SOC-stelsel Rijk (VSSR), dat het functioneren van en de samenwerking tussen SOCs versterkt. Dat gebeurt door bundeling en door het gezamenlijk ontwikkelen van detectieregels. Zo vormen HGI, ABRO, het traject voor risicomanagement en VSSR een solide basis voor de opvolging van de derde aanbeveling van AcICT.

Departementen zijn zelf verantwoordelijk voor het treffen van passende beveiligingsmaatregelen. AcICT geeft terecht aan dat samenwerking en gemeenschappelijke uitgangspunten daarbij nodig zijn. Maar de bescherming van specifieke Te Beschermen Belangen (TBB) tegen statelijke actoren vraagt in veel gevallen om maatwerk. Als er gebruik wordt gemaakt van een breed aanvullend kader bestaat het risico dat het effect onvoldoende is, en dat het onnodig duur wordt. Daarom is in de Baseline Informatiebeveiliging Overheid (BIO) afgezien van een normenkader op BBN3-niveau. Bovendien is in de nieuwe BIO het onderscheid tussen de verschillende basisbeveiligingsniveaus vervallen.

Tegen deze achtergrond, en in aanvulling op de vier eerdergenoemde trajecten, is er een serie van acties in gang gezet. De CIO Rijk zal eerst samen met BZ, SSC-ICT en gespecialiseerde diensten, op basis van gangbare normen zoals ISO27001, BIO en NATO-normen, een aanvulling op de BIO ontwikkelen. Dit gaat over de actieve bescherming van Departementaal Vertrouwelijke gegevens tegen statelijke actoren. Hierbij worden ook uitgangspunten zoals ‘assume breach’ en ‘Zero Trust’ meegenomen. Deze normen en voorschriften worden in eerste instantie toegesneden op de casuïstiek bij BZ, in verband met de urgentie die daar wordt gezien. Naar verwachting kunnen de eerste resultaten aan het einde van dit jaar opgeleverd worden. De tweede stap is dat die aanvulling wordt doorontwikkeld tot een generiek inzetbare handreiking waaruit de ministeries kunnen putten voor het treffen van passende maatregelen om hun TBB’s te beschermen tegen statelijke actoren.

Voor de ontwikkeling van deze handreiking is goede interdepartementale samenwerking een belangrijke voorwaarde. Er worden verschillende experts samengebracht: van ministeries, uitvoeringsorganisaties en gespecialiseerde diensten. Zo kunnen domeinkennis, materiedeskundigheid en goede voorbeelden worden gedeeld. BZ speelt daarbij een sleutelrol; AcICT dringt erop aan om de expertise en de kennispositie van BZ goed te benutten voor de opvolging van hun derde aanbeveling. Het resultaat is een breed gedragen kader voor het efficiënt inzetten van generieke beveiligingsmaatregelen, dat tegelijkertijd helpt bij het aanpakken van specifieke beveiligingsuitdagingen.

AcICT adviseert om centrale, gecombineerde dienstverlening op te zetten voor de actieve bescherming van Departementaal Vertrouwelijke gegevens tegen statelijke actoren. Als eerste stap zal BZK een behoefteonderzoek uitvoeren, waarbij wordt meegenomen dat BBN3 komt te vervallen. Vervolgens zal er een business case worden opgesteld om de kosten en de baten van een centrale voorziening in kaart te brengen, en duurzame financiering te kunnen verzekeren.

Opvolging aanbeveling 4: evalueer na 2 jaar gezamenlijk de opvolging van de adviezen

Het overkoepelende advies van AcICT is om topprioriteit te geven aan de urgente verbetering van de huidige ICT-dienstverlening. De vierde aanbeveling die in dat verband wordt gedaan is het gezamenlijk evalueren van de opvolging van het advies, na twee jaar of zoveel eerder als passend wordt gevonden. Daarbij gaat het vooral om de eerste twee aanbevelingen, en dus om wat BZ en SSC-ICT daarmee hebben gedaan: welke maatregelen zijn er genomen, welk effect heeft dat gehad, en welke nieuwe mogelijkheden dienen zich vervolgens aan? AcICT hanteert voor deze evaluatie een vrij ruime termijn. Tegelijkertijd is de urgentie hoog. Het is dus belangrijk om van het begin af aan de vinger goed aan de pols te houden, en het evaluatiemoment als dat mogelijk is wat naar voren te halen.

Aanbeveling 1 (samen urgente beveiligingsrisico's terugdringen) gaat over acute kwesties. BZ en BZK zijn dus voortvarend aan de slag gegaan met dit onderdeel van het AcICT-advies. Beide organisaties hebben vertrouwen in de wenselijkheid van deze koers, en in elkaars goede wil. Dat is ook nodig, want de inhoudelijke opgave is niet gering. Daarbij zal ook de vraag opnieuw worden beantwoord of het principe van een shared services organisatie zich wel verdraagt met het kunnen leveren van gespecialiseerde diensten en het voldoen – voor een enkele opdrachtgever – aan complexe, bijzondere eisen. Op onderdelen geldt mogelijk dat 'nee' verkopen ook een antwoord is, wat vervolgens voor de opdrachtgever aanleiding is om op zoek te gaan naar een alternatief.

De aanbeveling om de besturing bij BZ te verbeteren is ook belangrijk. De opvolging daarvan wordt gezien als een diepte-investering, die verder gaat dan alleen de dienstverlening die wordt geleverd door SSC-ICT. Er zullen bijvoorbeeld aanpassingen moeten worden gedaan in de organisatie en in de manier van werken. Het programma SHIELD voorziet in een passende systematiek voor het monitoren van de voortgang en de resultaten op dit punt.

AcICT dringt erop aan om het 'vertrekbesluit' uit te stellen, en pas na evaluatie van de verbeteracties opnieuw te bekijken of zo'n besluit nog nodig is. De koppeling die daarmee wordt gemaakt is begrijpelijk. Als aanbeveling 1 (samen beveiligingsrisico's aanpakken) en aanbeveling 2 (besturing door BZ versterken) tot resultaten hebben geleid ligt alle informatie op tafel om een definitief standpunt te kunnen bepalen over het weghalen van – een deel van de – de dienstverlening bij SSC-ICT. Maar dat laat onverlet dat het mogelijk is om eerder al in gezamenlijkheid te bezien of er specifieke diensten zijn die SSC-ICT nu levert aan BZ waarvoor geldt

dat het niet in het belang is van BZ en SSC-ICT om die als zodanig te blijven leveren. Die analyse – of validatie, zoals het eerder in deze brief is genoemd – wordt in de komende maanden ter hand genomen binnen het kader van SHIELD.

De activiteiten die door BZ en BZK worden ontplooid om opvolging te geven aan de aanbevelingen 1 en 2 omvatten in feite ook vrijwel alle activiteiten die moeten worden uitgevoerd voor het voorbereiden van een eventuele – gedeeltelijke – ontvlechting. Dat betekent dat BZ een extra reden heeft om zich in te zetten voor het slagen van de maatregelen in het verlengde van deze aanbevelingen. Als dit vervolgens loopt zoals het BZ en SSC-ICT nu voor ogen staat dan is de uitkomst na evaluatie van die maatregelen dat een vertrekbesluit alleen hoeft te worden genomen voor die voorzieningen waarvan in gezamenlijkheid wordt vastgesteld dat die niet goed passen in de portfolio van SSC-ICT. Door op deze manier te werk te gaan (een *no regret* aanpak) treedt er voor BZ geen vertraging op als er vervolgens zou worden besloten tot een al dan niet gedeeltelijke ontvlechting.

Gezien de urgentie van het bovenstaande hebben BZ en SSC-ICT de afspraak gemaakt niet pas twee jaar na het uitbrengen van het advies de genoemde evaluatie uit te voeren, maar dit uiterlijk begin september 2026 te doen. Tot die tijd houden de twee organisaties in de gaten of daarin, al dan niet op onderdelen, nog een versnelling nodig en mogelijk is, bijvoorbeeld op basis van de genoemde validatie (de beantwoording van de vraag wat past binnen de portfolio en roadmap van SSC-ICT). Dat sluit ook aan op het advies van AcICT om elke drie maanden bestuurlijk over de opvolging van het advies te rapporteren.

Tot slot

Aan AcICT is gevraagd advies uit te brengen over een programma van BZ. Vervolgens heeft AcICT zich in zijn beantwoording gericht op twee ministeries, BZ en twee onderdelen van BZK, waarbij een breed terrein aan verbetertrajecten is bestreken. Daarmee ligt er een veelomvattend en betekenisvol advies op tafel. Veel van de bedoelde verbeteringen waren op dat moment al in beeld of zelfs in gang gezet. Maar het advies heeft de verschillende trajecten van nieuwe inzichten voorzien, en heeft gezorgd voor een nieuwe dynamiek in de onderlinge samenwerking.

BZ en BZK zijn overtuigd van de noodzaak om de investeringen te doen waar AcICT voor pleit. Samen hebben zij daarvoor de nodige plannen uitgewerkt. De verdere uitvoering daarvan is voortvarend

ter hand genomen, en BZ en BZK houden samen de vinger aan de pols, om zeker te weten dat het nieuwe elan beklijft en rendeert.

Graag willen wij AcICT dus bedanken voor het advies dat zij ons hebben aangereikt. Het moment bleek goed gekozen, en de uitkomst was behulpzaam. Wij hebben het vertrouwen dat in deze brief duidelijk is toegelicht hoe wij opvolging geven aan het advies van AcICT. Via de gebruikelijke rapportages over de bedrijfsvoering van het Rijk zullen wij u blijven informeren over de voortgang van de verschillende acties en maatregelen in dit verband.

De minister van Buitenlandse Zaken,
D.M. van Weel

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum