



> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Binnenlandse Zaken & Koninkrijksrelaties
t.a.v. de staatssecretaris van Koninkrijksrelaties en Digitalisering,
mevrouw drs. A.C. van Huffelen
Postbus 20011
2500 EA Den Haag

Adviescollege ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon

info@adviescollegeicttoetsing.nl

Kenmerk

2024-0000257698

Uw kenmerk

n.v.t.

Datum 26 april 2024
Betreft Advies versterking CIO-stelsel

Geachte mevrouw Van Huffelen,

Wij hebben kennisgenomen van de verzamelbrief¹ die u 22 december 2023 aan de Tweede Kamer zond. U geeft daarin aan het CIO-stelsel in 2024 te evalueren en te willen versterken. Het Adviescollege ICT-toetsing heeft de afgelopen jaren bij de uitvoering van haar advies- en kennistaak verschillende waarnemingen gedaan over de opzet en werking van dit stelsel. Het Adviescollege heeft daarom uit eigen beweging² dit advies opgesteld. Wij beogen daarmee niet een compleet beeld te geven; we richten ons met name op een effectievere beheersing van ICT-activiteiten.

Het advies kan als volgt worden samengevat:

De ambitie van het CIO-stelsel is om de digitalisering van de rijksdienst te bevorderen en een betere beheersing van ICT-activiteiten te realiseren. Het CIO-stelsel definieert daartoe drie niveaus waarop CIO-functies zijn ingericht: rijksbreed, departementaal, en per organisatieonderdeel of beleidsterrein.

Advies

Wij zien dat het CIO-stelsel vrijheidsgraden bevat die het mogelijk maken om de invulling ervan op maat te maken voor departement en uitvoeringsorganisatie. Maar we zien ook dat de werking van het CIO-stelsel onvoldoende is. Daarom is onze aanbeveling de invulling van de rol van de CIO binnen het stelsel op drie gebieden te versterken:

1. de kaderstellende rol
2. het portfoliomanagement van alle ICT-activiteiten
3. de aandacht voor en kennis van de ICT-oplossing zelf

NB Hoewel het bij het versterken van het CIO-stelsel kan lijken dat het alleen gaat over het functioneren van de CIO's, is het beheersen van ICT-activiteiten een opdracht van en voor de gehele overheidsorganisatie.

Hieronder vindt u eerst een korte beschrijving van het CIO-stelsel. Daarna gaan we verder in op onze adviezen. Wij hebben per advies aandachtspunten voor de

¹ Kamerstuk II 2023/24, 26 643, nr. 1112.

² Conform artikel 2, lid 2 b Instellingsbesluit Adviescollege ICT-toetsing.

gehele organisatie. We formuleren deze aandachtspunten veelal in vragen waarop het antwoord per situatie zal verschillen.

KORTE OMSCHRIJVING VAN HET CIO-STELSEL

Het Besluit CIO-stelsel Rijksdienst³ is de formalisering van de rijksbrede en departementale taken en verantwoordelijkheden van een Chief Information Officer (CIO). In de eerste versie van het besluit CIO-stelsel (2008) lag de focus van de CIO-rol op een betere beheersing van grote ICT-projecten. Later is de rol van de CIO verbreed. In het meest recente besluit uit 2021 wordt de CIO onder meer gepositioneerd als de digitaal leider die een strategische visie voorbereidt op digitale en technologische ontwikkelingen, en zo richting geeft aan de digitale transitie van het Rijk.

Het CIO-stelsel definieert drie niveaus van CIO's:

- de CIO Rijk voor het gehele Rijk;
- de departementale CIO voor het betreffende departement;
- CIO's van tot het departement behorende organisatieonderdelen of beleidsterreinen.

In het besluit zijn zowel op rijks- als departementaal niveau meer specifieke verantwoordelijkheidsgebieden gedefinieerd, zoals voor informatiebeveiliging (CISO), IT-technische aspecten (CTO) en datamanagement (CDO). Een veel voorkomende rol binnen een CIO-Office (het ondersteunende bureau van de CIO) is die van ICT-controller, een specialist op het gebied van plannen en beheersen van de financiële middelen voor ICT-activiteiten.

ADVIES: VERSTERK DE INVULLING VAN DE CIO-FUNCTIE

Wij constateren dat het CIO-stelsel in opzet voldoet om met de diversiteit van de organisatie van de Rijksdienst om te gaan. Maar het stelsel schiet in zijn werking te kort en is niet effectief genoeg om de risico's van de ICT-activiteiten van het Rijk voldoende te beheersen. ICT-projecten zijn regelmatig niet goed bestuurbaar, worden geconfronteerd met significante kostenoverschrijdingen en/of lopen forse vertragingen op. Daarnaast voldoet een deel van de bestaande ICT-systemen niet meer aan de verwachtingen van de uitvoering, komen continuïteitsrisico's voor en wordt een deel geplaagd door slechte onderhoudbaarheid. Ook komt het digitaal leiderschap van de CIO onvoldoende tot uitvoering.

Wij adviseren u en uw collega's daarom het effect van de CIO-functie en de ingezette instrumenten op elk niveau van de CIO-functie te versterken door een betere invulling op drie gebieden.

1. Versterk de kaderstellende rol

De drie gedefinieerde niveaus geven de mogelijkheid de CIO-functie in te vullen voor de specifieke situatie van de betreffende organisatie. Zo zijn nu binnen het Rijk vele CIO's actief op verschillende niveaus en met verschillende portefeuilles.

Het is echter van belang te voorkomen dat elke CIO zelf voor elk vraagstuk een oplossing gaat zoeken of keuzes gaat maken. De bestaande kaders en richtlijnen

³ Besluit CIO-stelsel Rijksdienst, 2020-0000730468

zijn vaak algemeen en/of procedureel gedefinieerd. Daarnaast zijn deze veelal niet bindend en is er geen toezicht op de naleving. Door de lat voor deze instrumenten hoger te leggen en ze meer in te laten gaan op de problematiek die de verschillende CIO's ervaren, versterken kaders en richtlijnen zowel het digitaal leiderschap als de ICT-beheersing.

Meer in detail stellen we voor:

- *Zorg voor rijksbreed bruikbare kaders van CIO Rijk.* Ondersteun de departementale CIO's met kaders die een startpositie vormen voor per departement te nemen besluiten over ICT-beleid of -uitvoering. Sluit daarbij aan op wat de CIO's en ICT-professionals nodig hebben om hun werkzaamheden goed te kunnen uitvoeren. Doe dat niet op basis van een theoretische benadering, maar sluit aan bij de uitgesproken behoefte aan hulp (bottom-up) of bij best practices van de departementen dan wel internationaal. Maak als CIO Rijk keuzes waarmee ook het digitaal leiderschap (top-down) ofwel de richting die je als Rijk in wilt slaan, wordt ingevuld. Denk aan richtingbepalende onderwerpen als gebruik van de cloud, standaard softwarepakketten, transparantie in gebruik van algoritmes en Artificial Intelligence, of gebruik van rijksbrede voorzieningen zoals Rijks ICT-Dashboard of Security Operations Centers (SOC). Maak het gebruik van deze kaders minder vrijblijvend. Zorg er daarbij voor dat de kaders geschikt zijn voor het effectief uitvoeren van toezicht en inspectie van de verschillende domeinen.
- *Zorg voor departementaal bruikbare kaders van departementale CIO's.* Het is zaak dat de departementale CIO's de rijksbrede kaders uitwerken voor hun eigen departement, dan wel aanvullen waar specifieke kaders voor het eigen domein nodig zijn. Ook daar is input vanuit het departement en de betrokken organisatieonderdelen nodig voor de aansluiting op de eigen werkprocessen, samenwerkingsverbanden en specifieke beveiligingsvraagstukken. Ook deze kaders zijn niet vrijblijvend.
- *Richt expliciete processen in rond kaders en adviezen.* Het is van belang voor bovenstaande kaders een besluitvormingsproces in te richten tot op het hoogste bestuurlijke niveau. Op dat niveau vindt de afweging plaats tussen de wensen vanuit de beleidsdirecties en uitvoeringsorganisaties, en de (on)mogelijkheden om die in te vullen. Zorg er daarbij voor dat de CIO een directe eigen inbreng heeft en waar nodig besluiten met ongewenst effect kan verhinderen. De bestuurders en de andere leidinggevende ICT-functionarissen verbinden zich zo aan de gemaakte keuzes. Een goede plek om dit te bespreken is de bestuursraad waar de CIO een plaats aan tafel heeft volgens het Besluit CIO-stelsel. In de praktijk heeft hij deze overigens niet altijd. Daarnaast stellen we voor een expliciet proces in te richten voor het afleggen van verantwoording over de uitvoering van ICT-activiteiten, om de uitvoering van de gemaakte afspraken te kunnen volgen en waar nodig bij te sturen. Onderdeel daarvan is het transparant maken van de opvolging van de adviezen ten behoeve van kwaliteitsbewaking en risicomanagement, zoals CIO-oordeel en adviezen van het Adviescollege. Naast dit proces is van belang dat toezicht ingericht wordt onder verantwoordelijkheid van degene die de kaders heeft gesteld.

Aandachtspunten

Een open vraag is de mate waarin deze kaders verplichtend zijn dan wel meer vrijblijvend. We stellen voor dit te bespreken met de betrokkenen in een daarvoor

relevant overleg, zoals CIO-Beraad, bestuursraad of directie van een organisatieonderdeel. En daarbij expliciet te maken wanneer en op basis van welke overwegingen de kaders worden toegepast, bijvoorbeeld vanwege het financiële, juridische of maatschappelijke belang. Hierbij kan overwogen worden de CIO Rijk in het CIO-Beraad de beslissende stem te geven gehoord de departementale CIO's.

2. Versterk portfoliomanagement van alle ICT-activiteiten

Hoewel op elk genoemd niveau van de CIO-functie wel een vorm van portfoliomanagement is ingericht, is er nog veel verbetering nodig. Ook missen we vaak nog de verbinding tussen portfoliomanagement en lifecycle-management. Daardoor worden kansen gemist om onderhoud meer planmatig en met een goede financiële en technische onderbouwing vorm te geven. Zowel het Rijks ICT-Dashboard als de door ons ontvangen projectoverzichten per departement of grotere uitvoeringsorganisaties zijn incompleet en worden veelvuldig gecorrigeerd. Informatie over onderhoud en beheer ontbreekt daarbij vrijwel volledig; vaak is onduidelijk wie waarover beslist en waar dat vastligt. Ten slotte is er nog steeds geen goed inzicht in de kosten van ICT per organisatie. Terecht wordt in het Besluit CIO-stelsel het portfoliomanagement gezien als het instrument van de CIO om op de digitale ontwikkelingen in de samenleving of binnen het ministerie in te spelen. Dit geldt zowel voor het onderhoud en beheer van bestaande informatiesystemen als voor nieuwe ICT-projecten en -wijzigingen. Ook door tekortschietend portfoliomanagement komt de CIO in zijn of haar rol van digitaal leider onvoldoende naar voren.

We stellen voor het portfoliomanagement als volgt te versterken:

- *Werk samen met de financiële functie bij vergroten transparantie ICT-kosten.* Alle departementen hebben een proces voor Planning & Control (P&C) ingericht waarin de jaarlijkse begroting wordt vertaald naar budgetten en formatie per organisatieonderdeel en afdeling. Binnen deze budgetten zijn ook de ICT-kosten opgenomen, maar deze zijn veelal niet apart gespecificeerd. Om een beter inzicht te krijgen in de besteding van de financiële middelen en de inzet van eigen personeel stellen we voor rijksbreed en per departement afspraken te maken over het transparant maken van die kosten in de administraties. Of om, als dat niet kan, afspraken te maken over werkwijzen om kosten zo goed mogelijk in te schatten. Doe dit in samenwerking met de Directeur FEZ en waar nodig met het ministerie van Financiën. Zorg er vervolgens voor dat de ICT-controlfunctie zowel in planning als periodieke verantwoording aansluit op deze P&C-cyclus, niet alleen departementaal, maar ook op het niveau van de CIO Rijk voor de rijksbrede ICT-activiteiten.
- *Maak duidelijk wie, in welke rol, via welke structuur, beslist over welk portfolio.* Om te voorkomen dat onduidelijk is wie welk ICT-portfolio bestuurt en daarover verantwoording aflegt, stellen we voor dat expliciet te maken. Op dit moment is portfoliomanagement veelal beperkt tot de projectportfolio's op departementaal niveau en op het niveau van de uitvoeringsorganisaties. Beheerportfolio's zijn vaak niet of maar ten dele aanwezig. Daarmee is niet voldoende scherp wie over welke set van ICT-activiteiten besluit en deze bestuurt. Komt de sturing vanuit de bestuurders, vanuit de CIO (op verschillende niveaus) of vanuit ICT-organisaties? Ook zien we onduidelijkheden over ICT-activiteiten van de veel voorkomende interdepartementale of binnen-departementale samenwerkingsverbanden.

Besteed bij het definiëren van het portfolio binnen en tussen overheidsorganisaties expliciet aandacht aan:

- onderscheid tussen projecten, doorontwikkeling en beheer van een ICT-systeem;
- wanneer iets een organisatie-specifieke, departementale, interdepartementale of rijksbrede voorziening is;
- de verantwoordelijkheidsverdeling tussen opdrachtgever, kadersteller of ICT-controller, CIO's en CIO Rijk voor de hierboven genoemde voorzieningen.

Aandachtspunten

Bij het maken van afspraken over de inrichting van portfoliomanagement - en de daarbij behorende bestuurlijke afspraken - is een belangrijke vraag welke inhoudelijke beslissingen tot het portfoliomanagement worden gerekend en welke niet. Is portfoliomanagement alleen een procesmatige werkwijze om geld en capaciteit te verdelen of gaat het ook om de aansturing van verbeteringen in het functioneren van de betrokken organisatie(s) en ICT-oplossingen? En hoe is dan de rol- en verantwoordelijkheidsverdeling tussen de CIO's, beleids-DG's en -directeuren en eindverantwoordelijken van organisatieonderdelen? Hoe wordt daarbij de balans bewaakt tussen het investeren in technisch onderhoud en het realiseren van wensen van de business? Dit is een belangrijke taak voor de bestuursraad. Ook de verschillende kaderstellende en coördinerende rollen en verantwoordelijkheden van de departementen BZK, EZK en JenV voor de inzet van ICT vragen hierbij om aandacht.

3. Versterk de inhoudelijke aandacht voor de ICT-oplossing zelf

We zien dat er de laatste tijd meer aandacht is voor de inrichting van de CIO-Offices en het geven van een sterkere positie aan de CIO. Ook wordt meer gebruik gemaakt van instrumenten voor beheersing van ICT-activiteiten, zoals bijvoorbeeld Gateway-onderzoeken, externe reviews, CIO-oordelen en onderzoeken van het Adviescollege. Dan is het toch opvallend dat de ICT-oplossingen die de projecten voorstellen vaak te ver afstaan van de eigen praktijk. En dat de interne reviews vooral op de aanpak gericht zijn en niet op de ICT-oplossing zelf. Dat betekent dat het relatief vaak voorkomt dat een suboptimale oplossing wordt ontwikkeld en in gebruik genomen, die vervolgens ook in onderhoud en beheer tot extra problemen leidt.

We stellen voor al vanaf het eerste moment meer aandacht te besteden aan de ICT-oplossing zelf. Dat kan als volgt:

- *Versterk de ICT-kennis en -ervaring bij CIO's en CIO-Offices en opdrachtgevers.* We stellen voor nog meer in te zetten op de ICT-inhoudelijke kennis en ervaring van de CIO's en CIO-Offices, waaronder kennis van architectuur. Neem mensen met deze kennis aan en versterk het opleidingstraject, ook voor (top)management dat als opdrachtgever fungeert. De verschillende ICT-functionarissen kunnen veel van elkaar leren, bijvoorbeeld door meer peerreviews en georganiseerde feedback. Ruim daar in elk jaarplan voldoende tijd en capaciteit voor in. Waar dat (vooralsnog) nog niet voldoende deskundigheid naar binnen haalt, valt de introductie van een flexibele schil van ICT-specialisten te overwegen. Voor het verder versterken van de rol van de CIO is investeren in de kennispositie van de CIO een basisvoorwaarde.

- *Zorg bij aansturing van ICT-activiteiten voor aandacht voor de ICT-oplossing.* Dat kan door bij de besluitvorming over programma's en projecten de verschillende ICT-alternatieven en architectuuroplossingen systematisch te evalueren. Niet alleen met het oog op de kosten-batenafweging van het project, maar ook vanuit de beleidsdoelstellingen, en het gebruik en beheer over een langere termijn. Aandachtspunten voor beoordeling van de alternatieven zijn de aansluiting bij de, soms snelle, ontwikkelingen in de ICT-wereld en het langetermijneffect van deze ICT-oplossing voor de eigen (beheer)organisatie.

Aandachtspunten

Meer aandacht voor de ICT-oplossing zelf versterkt de positie van de CIO als digitaal leider. Niet alleen de positie ten opzichte van de integrale (beleids-) verantwoordelijkheid van de directeurs-generaal, maar ook ten opzichte van de (ministeriële) verantwoordelijkheid van departementen op bepaalde aspecten van de beoogde digitale transitie, zoals regeldruk (EZK), digitale veiligheid (JenV) en digitale overheid en digitale samenleving (BZK).

Ook bij het definiëren van de benodigde kennis en ervaring voor de CIO-functie en CIO-Offices is de begrenzing van hun verantwoordelijkheid een aandachtspunt. In welke mate zijn zij ook de opdrachtnemer voor de ICT-activiteiten of verantwoordelijk voor de kwaliteit van informatie? Bijvoorbeeld omdat ze, via (de aansturing van) de Chief Technology Officer (CTO), Chief Data Officer (CDO), Chief Information Security Officer (CISO) of als directeur IT direct betrokken zijn? Hoe groter het verantwoordelijkheidsgebied, hoe meer eisen aan de benodigde kennis en ervaring worden gesteld. Maar ook het risico op te sterke concentratie van rollen is dan groter. Functiescheiding om betere feedback en besluitvorming te organiseren is daarbij een belangrijk punt van overweging.

Wij hopen dat wij met dit advies een bijdrage kunnen leveren aan het versterken van het CIO-stelsel en de rol van de CIO-functie in de breedste zin van het woord, en daarmee aan een betere beheersing van de ICT-activiteiten.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

drs. H.J.A. van Osch
Voorzitter

w.g.

drs. S.J. van Amerongen
Secretaris-directeur

Bijlage

Informatie over het uitgevoerde onderzoek

Nr	Onderwerp	Toelichting
1.	Type onderzoek	Advies uit eigen beweging; conform artikel 2, lid 2 sub b Instellingsbesluit Adviescollege ICT-toetsing
2.	Aanmelddatum	19-03-2024
3.	Start onderzoek	01-01-2024
4.	Afronden onderzoek	25-03-2024
5.	Datum concept advies	25-03-2024
6.	Datum definitief advies	26-04-2024
7.	Eerder onderzoek	n.v.t.
8.	Onderzoeksmethode	Documentstudie.