Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Uitkomsten nulmeting Besluit CIO-stelsel Rijksdienst mei 2021

definitief

Colofon

Titel	Uitkomsten nulmeting Besluit CIO-stelsel Rijksdienst mei 2021
Uitgebracht aan	CIO Rijk,
Datum	19 oktober 2021
Kenmerk	2021-0000210261
Referentienummer	2020-BZK-043

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Centrale boodschap: departementale verschillen in de mate en wijze van implementatie van het Besluit; aandacht benodigd voor strategische invulling van de CIO- en CISO-functies

Informatie (I), Informatievoorziening (IV) en Informatietechnologie (IT) zijn niet meer weg te denken uit de primaire departementale processen. Ze zijn van essentiële waarde. Daarom zijn de CIO- en CISO-functies van groot belang binnen het Rijk. Het Besluit CIO-stelsel Rijksdienst (hierna: het Besluit) is in deze context ontstaan. Doel van het onderzoek is het uitvoeren van een nulmeting naar de mate van implementatie van het Besluit en het in kaart brengen van waar CIO Rijk verdere ondersteuning kan bieden aan de CIO-functie binnen de departementen. Het onderzoek heeft zich gericht op de huidige stand van implementatie bij de departementale CIO en CISO. De implementatie bij CIO Rijk is niet onderzocht.

Centrale boodschap
Hieronder presenteren wij de centrale boodschap van ons onderzoek. Deze hebben wij samengevat tot drie rode draden.

De strategische positie van de CIO- en CISO-functie is niet overal ingevuld
De achterliggende gedachte van het Besluit is een nadere verankering van I in de lijnorganisatie. Concepten zoals de CIO als C-level executive en digitaal leider zijn daarbij essentieel. Deze concepten borgen de strategische invulling van de CIO- en CISO-functie, en daarmee het strategisch belang van I voor de organisatie.

Op enkele key-elementen hebben wij afwijkingen van het Besluit geconstateerd, die te relateren zijn aan de strategische invulling van de CIO- en CISO-functie. Zo hebben wij bij vier departementen geconstateerd dat de CIO niet rechtstreeks onder de SG hangt en vaak geen vaste zitting heeft in de Bestuursraad, zoals wel bedoeld in het Besluit. CIO's geven aan dat zij kunnen deelnemen wanneer zij dat nodig achten. Wij zien een risico dat de strategische I-component dus niet bij alle punten van de Bestuursraad wordt meegenomen en geadresseerd. In dezen geven departementen aan niet goed te weten hoe zij uitzonderingen op het Besluit met CIO Rijk dienen te communiceren.

Tevens is de CIO-functie bij enkele departementen belegd bij de pSG. Hoewel I hiermee op hoog bestuurlijk niveau is belegd, zien wij een risico dat de doelstelling van de CIO als digitaal leider niet wordt behaald, indien a) departementen de pSG-functie met de CIO-rol combineren en/of b) de daadwerkelijke uitvoering van de CIO-rol wordt gedelegeerd.

Het Besluit biedt ruimte voor verscheidenheid in implementatie
De achterliggende gedachte van het Besluit is het scheppen van een zekere mate van uniformiteit: het "wat" wordt gedefinieerd. Het "hoe" (lees: de implementatie) wordt aan de departementen overgelaten. Daardoor ontstaat ruimte voor verscheidenheid in implementatie. Onderstaande punten laten zien dat departementen verschillend invulling geven aan de gezamenlijke basis. Verschillen mogen er zijn, zolang duidelijk is waar de grenzen liggen. Hieronder schetsen wij het beeld per taak van de CIO en CISO.

- **Advisering.** Departementen adviseren op een aantal manieren. Dat varieert van mondelinge (telefonische) gesprekken tot formeel vastgestelde adviesnotities. We zien variatie in de combinatie van manieren van advisering per departement.
- **Oordeel (alleen CIO).** Nagenoeg ieder departement heeft een formele procedure vastgelegd voor de oordeelsvorming van de CIO bij projecten met een ICT-component groter dan vijf miljoen euro. Vrijwel alle departementen werken met scoringsmechanismen om te komen tot een oordeel en aanbevelingen.
- **Beleidsvorming.** Alle departementen hebben in eigen vorm beleid (over IV, digitalisering en informatiebeveiliging) geformuleerd. De bijdrage van de CISO aan het departementale beleid verschilt. Departementen signaleren dat het voor hen niet duidelijk is wat de vereisten zijn voor de concrete invulling van het beleid conform het Besluit. Daarnaast stellen bij enkele departementen decentrale dienstonderdelen zelfstandig beleid op naast het departementale beleid. Wij signaleren een risico m.b.t. het borgen van de samenhang tussen departementaal beleid en beleid van dienstonderdelen.
- **Informatie en communicatie.** Alle departementen organiseren diverse activiteiten ten behoeve van de communicatie over IV/IT binnen het departement. Departementale CISO's hebben verschillende manieren ontwikkeld om informatie te verkrijgen en sturing te geven aan risico's m.b.t. informatiebeveiliging & privacy (e.g. vragenlijsten, periodieke overleggen, etc.).

Alle departementen zijn bezig met de implementatie van het Besluit

Uit ons onderzoek blijkt dat alle departementen zich voorbereiden op passende acties die voor hen nodig zijn om te voldoen aan de vereisten van het Besluit. Het merendeel van de departementen heeft hiertoe een fit/gap-analyse uitgevoerd. Hoewel bijna de helft van de departementen korte termijnplannen (tot eind 2021) heeft geformuleerd, blijven plannen voor de middellange termijn, met concrete doelstellingen, uit. Wel signaleren departementen dat er voor hen een uitdaging in de implementatie ligt om de veranderingen en geformuleerd beleid verder in te bedden in de organisatie.

Handelingsperspectief

Op basis van de bovenstaande rode draden, heeft het ADR-onderzoeksteam de volgende handelingsperspectieven geformuleerd:

(1) Schep **duidelijke en eenduidige verwachtingen omtrent de vereisten** vanuit het Besluit om gewenste vorm van uniformiteit te borgen tijdens de implementatiefase. Besluit en communiceer hierbij duidelijk op welke aspecten **uniformiteit nodig** is en op welke aspecten **ruimte voor maatwerk** bestaat.

(2) Voorkom dat opgesteld beleid een **papieren exercitie** blijft. Wij zien twee punten waarop de CIO Rijk de departementen verder kan ondersteunen.
- Zet verder in op het uitwisselen van **good practices en het bespreken van probleempunten** tussen de verschillende departementen.
- Zet in op **CIO's als digitale leiders**. Hiermee is het noodzakelijk het beeld van CIO als manager bedrijfsvoering te veranderen. Overweeg hierbij het volgende:
  - In hoeverre het wenselijk is dat de CIO niet direct onder de SG valt, noch vast lid is van de Bestuursraad in het toekennen van uitzonderingen op het Besluit;
  - In hoeverre – gelet op het belang en de zwaarte van de CIO-functie – de combinatie van de CIO-functie met een andere (lijnmanagement)functie wenselijk is.

(3) Zorg voor een **eenduidig mechanisme voor uitzonderingen** op het Besluit en neem daarbij de mate van formaliteit in overweging. Dit kan pas wanneer de verwachtingen omtrent de vereisten duidelijk zijn (zie 1).

(4) Overweeg een **onderzoek** naar de relaties tussen de CIO en CISO Rijk en de departementale tegenhangers, alsook een vervolg op het huidige onderzoek op de middellange termijn.

Leeswijzer

Onderstaand geven wij schematisch de opbouw van het rapport weer: de centrale boodschap (CB), de hoofdstukken (H) en de bijlagen (B).

CB	In de centrale boodschap (CB) geven wij antwoord op de onderzoeksvragen en presenteren wij de geformuleerde handelingsperspectieven.
H1	Aanleiding en context van het onderzoek en nadere specificatie van onderzoeksvragen
H2 **H3** **H4**	Uitgebreide beschrijving van de centrale boodschap en beantwoording van de onderzoeksvragen. Ook beschrijven we good practices en uitdagingen voor implementatie, aan de hand van onderstaande iconen.  Good practices  Uitdagingen voor implementatie
H5	Handelingsperspectief van het ADR-onderzoeksteam op basis van analyse van bevindingen. Geformuleerd handelingsperspectief herkent u aan onderstaand icoon.  Handelingsperspectief
H6	Onderzoeksverantwoording
H7	Ondertekening van het rapport
B1	Gehanteerde referentiekader
B2	Managementreactie van CIO Rijk
B3	Factstheets van de ministeries

1 Inleiding

1.1 Aanleiding en context onderzoek

IV en IT zijn niet meer weg te denken uit de primaire departementale processen. Ze zijn van essentiële waarde. Daarom zijn de CIO- en CISO-functie van groot belang binnen het Rijk. De invulling van het departementale CIO-stelsel en het takenpakket van de departementale CIO's en CISO's verschilt per departement. Om onder andere deze redenen is er een roep om meer versterking van het CIO-stelsel binnen de Rijksdienst.[1] Binnen deze context heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties als kadersteller binnen het Rijk het Besluit CIO-stelsel Rijksdienst opgesteld, in co-productie met de verschillende 'bloedgroepen' binnen het CIO-stelsel.

Op 18 december 2020 heeft de Ministerraad dit Besluit goedgekeurd.[2] In dit Besluit wordt de rol van de CIO Rijk, CISO Rijk, departementale CIO en CISO vastgelegd. Hierin zijn de taken en verantwoordelijkheden nader gespecificeerd om ervoor te zorgen dat de departementen deze rollen op een meer uniforme manier inrichten.

De ADR is gevraagd onderzoek te doen naar het huidige beeld van de inrichting van het departementale CIO-stelsel binnen de Rijksdienst. We richting ons in dit onderzoek, in overleg met opdrachtgever en gezien de hanteerbaarheid van het onderzoek, op een deel van het besluit. Op 29 maart 2021 is de opdrachtbevestiging voor dit onderzoek getekend.[3]

1.2 Doelstelling en onderzoeksvragen

Het onderzoek betreft een nulmeting in het kader van de implementatie van het Besluit CIO-stelsel Rijksdienst. Het doel van het onderzoek is, naast inzicht te bieden in de mate van implementatie van het Besluit, op basis van de resultaten departementen meer gericht te kunnen ondersteunen bij de versterking van de CIO-functie.

De onderzoeksvraag is: "Hoe verhoudt het huidige beeld van (een deel van) de invulling van de CIO en CISO-functies bij de twaalf ministeries zich tot de voorschriften in het Besluit CIO-stelsel Rijksdienst?"

Hiervoor hebben we twee deelvragen opgesteld:

1. In hoeverre voldoen de huidige inrichtingen van de CIO en CISO-functies bij de departementen aan de vereisten van het Besluit?
2. Welke analyses hebben de departementen uitgevoerd en/of zijn de departementen van plan om uit te voeren om te kunnen voldoen aan het Besluit?

Om de eerste deelvraag te beantwoorden hebben wij het volgende onderzocht: de taken, verantwoordelijkheden en bevoegdheden van respectievelijk de departementale CIO en CISO en een aantal key elementen.[4] De key-elementen zijn in afstemming met de opdrachtgever geformuleerd. Voor een nadere specificatie van de onderzochte artikelen uit het Besluit verwijzen wij naar bijlage 1: referentiekader.

[1] Zie bijvoorbeeld: Strategische I-agenda Rijksdienst, 2019-2021, editie 2020; Kamerbrief met beleidsreactie onderzoeken IV-governance Rijk en besluit toekomst Bureau ICT-Toetsing (BIT)
[2] Besluit van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 18 december 2020, nr. 2020-0000730468, tot vaststelling van een kader houdende de organisatie-inrichting van het CIO-stelsel binnen de Rijksdienst (Besluit CIO-stelsel Rijksdienst 2021)
[3] Opdrachtbevestiging Onderzoek CIO-stelsel, versie 1.0, d.d. 25 maart 2021, kenmerk: 2021-0000060883
[4] De key elementen zijn: de ophanging van de CIO onder de Secretaris-Generaal, aanwezigheid van het CIO-stelsel, toegang van de CIO's tot de Bestuursraad, bestaan en grootte van het CIO-office, aanwezigheid van de departementale CISO.

2 Diverse departementen wijken op enkele key-elementen af van het Besluit

Dit hoofdstuk beschrijft de invulling van de vijf onderzochte key-elementen van het CIO Besluit bij de departementen.[5]

- De ophanging van de CIO onder de Secretaris-Generaal (§2.1);
- Aanwezigheid van het CIO-stelsel (§2.2);
- Toegang van de CIO's tot de Bestuursraad (§2.3);
- Bestaan en grootte van het CIO-office (§2.4);
- Aanwezigheid van de departementale CISO (§2.5).

2.1 Bij vier departementen hangt de CIO niet rechtstreeks onder de Secretaris-Generaal (SG)

In het Besluit staat dat de CIO organisatorisch onder de SG dient te worden geplaatst.[6] Onderstaande tabel illustreert de stand van zaken ten tijde van ons onderzoek.

Ministerie	Direct onder SG?	CIO als eigen-standige functie?	Toelichting
AZ	nee	nee	De CIO is de plv. directeur bedrijfsvoering (tevens Unit Manager van de ICT-afdeling).
BZ	ja	ja	De directeur IDI is tevens CIO en valt onder de pSG.
BZK	ja	ja	De CIO is een eigenstandige functie onder de SG.
OCW	ja	nee	De CIO is nu bij OCW tevens Directeur Kennis en valt onder de SG.
FIN	ja	nee	Bij Financiën is de pSG de CIO.
DEF	nee	ja	Zelfstandige functie; valt onder DG, maar wel directe lijn naar SG.
I&W	ja	nee	Per 1 mei 2021 vervalt de functie Hoofd Directeur Financiën en Integrale Bedrijfsvoering en wordt deze HD Plaatsvervangend Secretaris-Generaal. Ze behoudt de CIO-functie. De pSG/CIO draagt haar taken in uitvoering over aan de directie CDIV.
EZK/LNV	ja	nee	De rol van de CIO is belegd bij de pSG's.
SZW	nee	ja	Bij SZW is de directeur van de directie CIO-office en Integrale Veiligheid (CIV) de CIO.
J&V	ja	nee	Sinds begin mei is er een hoofddirecteur Bedrijfsvoering met de rol van CIO J&V als nieuwe functie aan de topstructuur toegevoegd. De CIO J&V heeft zitting in de Bestuursraad.
VWS	nee	nee	De Directeur Informatiebeleid is de concern-CIO, vallend onder de pSG.

Tabel 1. *Organisatorische plaatsing departementale CIO: onder Secretaris-Generaal?*

Ongeveer de helft van de departementen kent een **CIO die organisatorisch rechtstreeks onder de Secretaris-Generaal hangt**. Voor vier departementen is dit niet het geval. Bij de ministeries van AZ, Defensie, SZW en VWS hangt de CIO onder de pSG of een DG. Voor Buitenlandse Zaken geldt een andere situatie waar de

[5] Zie Bijlage 1. Referentiekader voor de bijbehorende artikelen uit het Besluit.
[6] Besluit CIO-stelsel Rijksdienst, art. 3.1: "De minister die belast is met de leiding van een ministerie draagt zorg voor de aanstelling van een departementale CIO die rechtstreeks ressorteert onder de secretaris-generaal van het ministerie."

pSG en de SG een gelijk mandaat kennen. De keuze om de CIO onder de pSG te plaatsen of te combineren met een andere functie heeft in veel gevallen te maken met het beeld dat de CIO een functie binnen de bedrijfsvoering vormt. Hiermee ontstaat een mogelijk risico dat de in het Besluit gewenste strategische positie van de CIO, de CIO als **"digitaal leider"**, en de beschreven taken en bevoegdheden van de CIO binnen deze departementen niet tot uiting komen. Het Besluit impliceert dat de CIO-rol die van een **C-level executive** zou moeten zijn. Deze rol komt mogelijk in het geding als de CIO niet rechtstreeks onder de SG ressorteert. Geen van de departementen, waar de CIO onder de pSG/DG hangt, heeft aangegeven deze positie op korte termijn te wijzigen. Het is voor de betreffende departementen niet duidelijk of en hoe ze deze afwijking van het Besluit dienen te communiceren met CIO Rijk.

Zoals aangegeven in tabel 1, is de CIO in vijf gevallen een **eigenstandige functie**, bij BZ, SZW, VWS, Defensie en BZK. Bij de overige departementen wordt de CIO-taak gecombineerd met een functie binnen het lijnmanagement (AZ, OCW en J&V), of gecombineerd met de pSG-functie (EZK/LNV, Financiën en I&W). Een gecombineerde functie van CIO en pSG betekent een vaste plek in de Bestuursraad. Dit is een mogelijk voordeel van deze constructie. Er ontstaat echter ook een risico dat de doelstelling van de CIO als digitaal leider niet wordt behaald, indien a) departementen de pSG-functie met de CIO-rol combineren en/of b) de daadwerkelijke uitvoering van de CIO-rol wordt gedelegeerd aan andere functionarissen.

Enkele departementen geven aan dat zij gebruik willen maken van de **uitzonderingsclausule** (art. 17) in het Besluit. Uit ons onderzoek blijkt tevens dat departementen niet goed weten hoe ze hiervan gebruik moeten maken. Het is niet duidelijk of dit per mail met het CIO Rijk office kan worden gecommuniceerd; of dit in de periodieke gesprekken tussen CIO Rijk en de departementale CIO kan worden besproken; of dat een formele toestemming van de minister van BZK nodig is.

2.2 Alle departementale CIO's hebben een CIO-stelsel ingericht

Volgens het Besluit, is de CIO verantwoordelijk voor het inrichten van een departementaal CIO-stelsel.[7] Elk departement kent een CIO-stelsel. Een drietal departementen (FIN, SZW en VWS) heeft een concern-CIO en een aparte CIO voor het kerndepartement. Bij de departementen waar men naast de CIO voor het departement ook CIO's voor de dienstonderdelen heeft, zijn verschillende overlegstructuren ingericht. Zelfstandige bestuursorganen (ZBO's) vallen volgens het Besluit niet onder het CIO-stelsel.[8] Wel vindt er veelal overleg en samenwerking plaats tussen de CIO's van de departementen en de CIO's van de ZBO's. AZ en BZ kennen geen CIO's voor dienstonderdelen, omdat dit niet passend is voor de grootte en de structuur van deze departementen. Het ministerie van Defensie heeft op dit moment eveneens alleen een departementale CIO, maar overweegt het aanstellen van CIO's bij de verschillende defensieonderdelen.

2.3 CIO's hebben toegang tot de Bestuursraad, maar niet elke CIO heeft een eigen stoel

In het Besluit staat dat de CIO lid moet zijn van de Bestuursraad van het departement.[9] Bij vijf departementen is de CIO geen lid van de Bestuursraad, namelijk bij de ministeries van AZ, BZ, Defensie, SZW en VWS. Dit zijn voor een groot deel dezelfde departementen waar de CIO niet rechtstreeks onder de SG is gepositioneerd. Al deze departementen geven expliciet aan dat er geen belemmeringen zijn voor de CIO om aan te sluiten bij een bijeenkomst van de Bestuursraad. In veel gevallen hebben ze de mogelijkheid om te agenderen. Deze zogenaamde "standing invitations" betreffen echter wel voornamelijk I-gerelateerde onderwerpen. Het Besluit impliceert dat de CIO ook input levert op onderwerpen die niet expliciet I-gerelateerd zijn (cf. strategische rol). De betreffende CIO's maken nu

[7] Besluit CIO-stelsel Rijksdienst, art. 3.3: "De departementale CIO is tevens belast met het inrichten van het CIO-stelsel voor het ministerie en de onder haar ressorterende dienstonderdelen."
[8] Toelichting bij art. 2 Besluit CIO-stelsel Rijksdienst: "Het besluit is niet van toepassing op zelfstandige bestuursorganen."
[9] Besluit CIO-stelsel Rijksdienst, art. 3.4: "De departementale CIO is lid van de bestuursraad van het ministerie."

zelf de inschatting wanneer zij het relevant achten een vergadering bij te wonen. Een risico is dat I-onderwerpen niet altijd meegenomen worden in de besluitvorming van de departementen.

Good practice: periodiek specifieke aandacht voor I-onderwerpen in de Bestuursraad

Het managementteam van OCW (is gelijk aan de Bestuursraad) maakt periodiek tijd beschikbaar om specifiek I-onderwerpen gebundeld te bespreken door regelmatig een "I-blok" in de wekelijkse vergaderagenda te reserveren.

Good practice: bilateraal overleg met de bewindspersoon

Bij het ministerie van Defensie heeft de CIO om de week a) een bilateraal overleg met de SG en b) een trilateraal overleg met de SG en de Staatssecretaris. Daarnaast heeft de CIO maandelijks een bilateraal overleg met de Staatssecretaris. Hierbij kan de CIO alle relevante zaken op I-gebied aankaarten.

2.4 Eén departementale CIO beschikt niet over een eigen CIO-office

Uit het Besluit blijkt dat iedere CIO een CIO-office tot zijn/haar beschikking dient te hebben.[10] Voor dit onderzoek hebben wij het aantal FTE geïnventariseerd (zie tabel 2). Vrijwel alle CIO's hebben beschikking over een eigen CIO-office. Bij het ministerie van Financiën heeft de departementale CIO geen eigen CIO-office ingericht, maar maakt deze gebruik van het office van de CIO van het kerndepartement. De hoeveelheid beschikbare 'FTE's verschilt. Dit hangt waarschijnlijk samen met de diversiteit aan werkzaamheden en omvang van de verschillende ministeries. Veel departementen met een decentraal stelsel kennen aparte CIO-offices voor diverse dienstonderdelen. De verschillende CIO-offices zijn lastig te vergelijken. Dit heeft te maken met de diversiteit aan inrichtingen van de CIO-stelsels. Bij tekorten of in geval er behoefte is aan specifieke expertise worden regelmatig externe krachten ingehuurd. Het ministerie van I&W is voornemens het office uit te breiden.

Onderstaande tabel bevat het aantal FTE voor de centrale CIO-offices van de verschillende departementen in april/mei 2021.

Ministerie	Aantal FTE in centraal CIO-office	Ministerie	Aantal FTE in centraal CIO-office
AZ	8	I&W	14
BZ	22	EZK/LNV	22 intern, 15 extern
BZK	21	SZW	9
OCW	14	J&V	30
FIN	maakt gebruik van CIO-office kerndepartement	VWS	8
DEF	20		

Tabel 2. *Aantal FTE in departementale CIO-offices.*

2.5 De CISO-rol wordt overal de facto uitgevoerd maar op verschillende functies

Het Besluit schrijft voor dat de departementale CISO rechtstreeks dient te ressorteren onder de CIO.[11] Wij hebben hierbij onderzocht in hoeverre de CISO onderdeel is van het departementale CIO-office. De meerderheid van de departementen beschikt over een formeel aangestelde CISO. De ministeries van Financiën en I&W zijn bezig met het werven van een departementale CISO. Bij FIN en I&W wordt de functie in de praktijk reeds uitgevoerd, maar moet er nog een officiële aanstelling en benoeming plaatsvinden. Bij J&V ligt de CISO-rol bij twee adviseurs van de afdeling I-control en

[10] Besluit CIO-stelsel Rijksdienst, art. 3.4: "Een CIO beschikt over een CIO-office."
[11] Besluit CIO-stelsel Rijksdienst, art. 6.1: "De minister die belast is met de leiding van een ministerie draagt zorg voor de aanstelling van een departementale CISO die rechtstreeks ressorteert onder de CIO van het ministerie."

Security; aan het hoofd daarvan staat de beoogd CISO J&V. De positie van de beoogd CISO is nog niet formeel in praktijk gebracht.

Bij SZW valt de CISO onder het team van de beveiligingsambtenaar (BVA), die valt onder de CIO. De CISO kan wel zelfstandig advies uitbrengen aan de CIO. Bij BZ is de CISO het clusterhoofd van het Security Centre. Het departementale CIO-office is belegd bij het cluster Strategie & Portfolio. De CISO valt daarmee niet direct onder het CIO-office, maar wel onder de CIO.

3 Taken en bevoegdheden van de departementale CIO en CISO worden vervuld bij de departementen, soms verschillend of met obstakels

In dit hoofdstuk beschrijven wij de uitkomsten van ons onderzoek naar:[12]

- de adviestaak van de CIO en CISO (§3.1);
- de oordeelstaak van de CIO (§3.2);
- de coördinatie- en ontwikkeltaak m.b.t. beleid van de CIO en CISO (§3.3.);
- de communicatietaak van de CIO en CISO (§3.4); en
- de informatietaak bij de CISO m.b.t. IB&P-risico's (§3.5).

3.1 Alle departementale CIO's en CISO's adviseren het lijnmanagement maar doen dit in verschillende vormen

3.1.1 CIO's en CISO's adviseren gevraagd en ongevraagd het primaire proces

In het Besluit staat dat de CIO en CISO een adviesfunctie hebben ten behoeve van het lijnmanagement en de bewindslieden.[13] De adviestaak van de CIO is op alle departementen in opzet beschreven. Elk departement heeft aangegeven zich bewust te zijn van de adviesfunctie van de CIO en CISO. Zoals al benoemd in §2.5 zijn twee departementen (FIN en I&W) nog bezig met het werven van een CISO. Bij het ministerie van SZW, FIN, BZK en EZK/LNV worden CISO-adviezen ook geïncorporeerd in CIO-adviezen.

Good practice: linking pins tussen CIO-office en de lijn

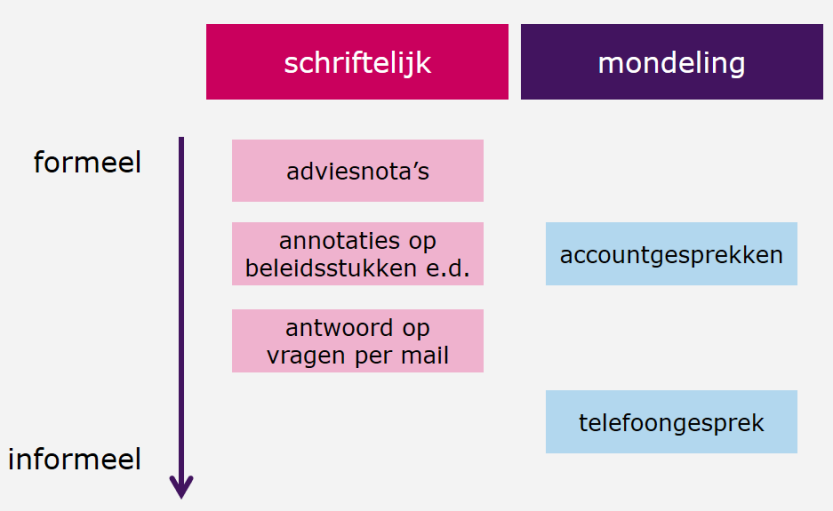
Enkele departementen werken met een systeem van linking-pins tussen het CIO-office en de lijn. Dit bevordert de communicatie tussen beide partijen: de drempel wordt verlaagd om advies te vragen en te geven. Onder andere de ministeries van BZ en SZW werken met een dergelijk systeem.

- Bij het ministerie van BZ werkt men met adviseurs Informatiebeveiliging en Privacy die zich specifiek op een bepaald BZ domein of directie richten. De adviseurs zijn onderdeel zijn van het zogenaamde Security Centre. De CISO is hiervan het afdelingshoofd en valt onder de CIO.
- Bij het ministerie van SZW werken **Informatiemanagers** (voor CIO-gerelateerde werkzaamheden) en **Veiligheid & Privacy Liaisons** (voor o.a. CISO-gerelateerde werkzaamheden). Zij werken in de werkvelden en zijn dus onderdeel van de lijn. Voor twee beleidswerkvelden geldt dat de informatiemanagers volledig voor de lijn werken, maar voorlopig bij de directie CIV zijn gepositioneerd. Daarmee zijn zij ook het eerste aanspreekpunt voor de lijn, maar ook voor het CIO-office. Dit bevordert de samenwerking tussen het CIO-office en de lijn bij SZW.

[12] Zie Bijlage 1. Referentiekader voor de bijbehorende artikelen uit het Besluit.
[13] Besluit CIO-stelsel Rijksdienst, art.4(a) en art. 4(b): "a. het adviseren van het lijnmanagement en de minister over het beleid ten aanzien van informatievoorziening en digitalisering; b. het adviseren van het lijnmanagement en de minister over de implicaties voor informatievoorziening en digitalisering van (voorgenomen) wet- en regelgeving, beleids- en uitvoeringstrajecten en investeringen;" art. 7(f): "het gevraagd en ongevraagd adviseren van de departementale CIO, het verantwoordelijk lijnmanagement en CISO's van dienstonderdelen over de informatiebeveiliging en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen;"

3.1.2 *Advisering kent verschillende maten van formaliteit*

In verschillende vormen adviseren CIO's en CISO's zowel schriftelijk als mondeling. De verscheidenheid in schriftelijke advisering en mondelinge advisering hangt samen met de mate van formaliteit en diepgang van advisering. Hieronder schetsen we een categorisatie van advisering door de CIO, CISO en medewerkers van het CIO-office.



Figuur 1. *Vormen van advisering, naar mate van formaliteit.*

Enkele departementen werken met formele **adviesnota's**. Hiermee komen CIO-offices met een gestructureerd advies. Andere departementen geven aan dat het onderscheid tussen deze vorm van advies en oordeel soms lastig te duiden is. Daarnaast **annoteren** verscheidene CIO's, CISO's en medewerkers van de CIO-offices beleidsstukken met hun opmerkingen en zienswijzen. Tevens ontvangen zij vragen per **mail** die zij vervolgens beantwoorden.

Uit ons onderzoek blijken grotendeels twee vormen van mondelinge advisering. Telefoongesprekken is een brede categorie. Daarnaast hebben we bij enkele departementen (o.a. EZK/LNV en J&V) geconstateerd dat **(account)gesprekken** worden gevoerd tussen de CIO/CISO en de lijn.

Good practice: Risk Letters als advisering

Het ministerie van AZ werkt met zgn. Risk Letters. Deze Risk Letters worden door CISO-adviseurs van het CIO-office opgesteld. Op basis van een risicoanalyse (die de adviseurs zelf uitvoeren) stellen de CISO-adviseurs een voorstel voor mitigerende maatregelen op voor de systeemeigenaar. De systeemeigenaar moet vervolgens reageren op de Risk Letter of deze a) het (rest-)risico accepteert, b) de maatregelen overneemt, c) andere maatregelen neemt. De CISO-adviseurs monitoren vervolgens het risico en de opvolging van mitigerende maatregelen.

We constateren een soortgelijke vorm bij het CIO-office van de ministeries van EZK en LNV met de zgn. CISO-brieven.

3.2 Alle departementale CIO's geven CIO-oordelen over grote ICT-projecten

Conform het Besluit dient de CIO oordelen te geven bij grote ICT-projecten.[14] Bij een negatief oordeel, moeten de adviezen meegenomen worden alvorens een project kan

[14] Besluit CIO-stelsel Rijksdienst, art. 4(i): "het zorgdragen voor voldoende aandacht binnen het ministerie voor continue beheeractiviteit en verbetering van de ICT-infrastructuur inclusief de benodigde technologische vernieuwing en informatiebeveiliging;"

beginnen.[15] Alle departementale CIO's voeren de taak uit van het vellen van een oordeel bij projecten met een ICT-component groter dan vijf miljoen euro. Bij het ministerie van Financiën velt de departementale CIO zelf geen oordelen, maar kan wel zijn mening geven over de oordelen van decentrale CIO's. De ministeries van AZ en BZ hebben minder vaak te maken met grote projecten dan – bijvoorbeeld – de ministeries van I&W en EZK/LNV. Het ministerie van AZ kan momenteel zelf geen onafhankelijke CIO-oordelen geven, vanwege de dubbelfunctie van de CIO als Unitmanager ICT. Voor het project AZ-Next heeft het ministerie van AZ het oordeel uitbesteed aan een derde partij.

Wij constateren dat departementen deze taak van de CIO **formeler invullen** dan de adviesfunctie. Acht departementen hebben een procedure (of een document met vergelijkbare inhoud) opgesteld. Aan de hand van dit document voeren de CIO-offices de oordelen uit. Veelal gebruiken zij scores.

In sommige gevallen voeren de **dienstonderdelen** met een eigen CIO ook het CIO-oordeel uit. Wij constateren dat de departementale CIO hier dan nog wel op kan reageren en het oordeel – indien nodig – kan wijzigen.

Departementen geven aan dat er vrijwel geen sprake is van **negatieve oordelen**. Wel zien we in de onderzochte CIO-oordelen van diverse departementen dat onderdelen binnen het oordeel slecht worden gescoord. Er wordt dan geen negatief oordeel gegeven, maar er worden strenge adviezen meegegeven, aldus betrokkenen. Daarnaast geven verschillende departementen aan dat het uitblijven van negatieve oordelen te maken heeft met de functie van de linking-pin die al proactief kan adviseren en bijsturen, voordat een CIO-oordeel wordt gevraagd. Desgevraagd geven departementen aan dat alleen de SG beargumenteerd zou kunnen afwijken van een negatief oordeel.

3.3 Betrokkenheid in het schrijven van beleid, strategieën en procedures is op alle departementen aanwezig; betrokkenen ervaren enkele obstakels

3.3.1 CIO: informatievoorzieningsbeleid en digitaliseringsbeleid

Conform het Besluit dient een CIO het informatievoorzieningsbeleid en digitaliseringsbeleid op te stellen.[16] We constateren dat er onduidelijkheid is bij de departementen over wat van hen verwacht wordt voor deze twee vormen van beleid. Het is voor hen tevens onduidelijk wat het verschil is tussen deze twee en wat er inhoudelijk van hen verwacht wordt bij beide beleidsstukken: wat is de reikwijdte, waar zit overlap, wat is een *must-have* in het beleid, wat is *nice-to-have*?

Alle departementen hebben I-beleid opgesteld. Voorbeelden hiervan zijn I-visies en I-strategieën. De CIO-offices zijn actief betrokken bij het opstellen van beleid. Daarnaast schrijven dienstonderdelen van departementen zelf ook aanvullend beleid.

3.3.2 CISO: departementaal risicobeeld, -beleid, informatiebeveiligingsbeleid en calamiteitenplan

Uit het Besluit blijkt dat de CISO een bijdrage dient te leveren aan het opstellen van het integrale beveiligingsbeeld, de risicoanalyse en het calamiteitenplan.[17] De bijdrage van de CISO m.b.t. het departementale beleid verschilt. We zien dat de CISO veelal bijdraagt aan het schrijven van beleidsstukken omtrent IB (o.a. bij de ministeries van AZ, BZ, OCW, FIN, SZW en VWS). Daarnaast zien we dat ook

[15] Besluit CIO-stelsel Rijksdienst, art. 5.3: "Voor het aanvangen van ICT-ontwikkelprojecten en onderhoudsactiviteiten met een grote ICT-component, die onder verantwoordelijkheid van het ministerie worden uitgevoerd, is een positief CIO-oordeel, of een beargumenteerde afwijking hiervan door de secretaris-generaal van het ministerie, vereist."
[16] Besluit CIO-stelsel Rijksdienst, art. 3.2: "De departementale CIO is belast met de ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid en het zorgdragen voor de ontwikkeling en het beheer van de informatiesystemen van het ministerie conform dit beleid."
[17] Besluit CIO-stelsel Rijksdienst, art.7(e): "het bijdragen aan het opstellen van het rijksbrede informatiebeveiligingsbeleid, het risicobeeld en het calamiteitenplan, bedoeld in artikel 13, onder a, c en j, en de rijksbrede I-strategie, bedoeld in artikel 11, onder a, en aan het integrale beveiligingsbeleid, de risicoanalyse en het calamiteitenplan, bedoeld in artikel 4, eerste, derde en zesde lid, van het Besluit BVA-stelsel Rijksdienst 2021, met betrekking tot de departementale informatiebeveiliging;"

decentraal beleid wordt opgesteld en dat de CISO dan veelal een toezichthoudende rol heeft (o.a. bij de ministeries van BZK, VWS en FIN). Bij enkele departementen zien we dat het calamiteitenplan primair behoort tot het takenpakket van de BVA, maar dat de CISO wel input levert (o.a. bij de ministeries van BZ, FIN en VWS).

Enkele departementen geven aan dat onduidelijk is wat verwacht wordt omtrent het risicobeeld. Andere departementen geven hier al invulling aan. Het ministerie van AZ gebruikt hiervoor bijvoorbeeld het dreigingsbeeld van de veiligheidsdiensten.

Uitdagingen in implementatie: samenhang en "levend" beleid

Departementen geven aan voor twee uitdagingen te staan met betrekking tot de ontwikkeling en coördinatie van beleid.

(1) Borgen van samenhang. Met name op departementen waar dienstonderdelen aanvullend beleid schrijven op centraal beleid, is dit een aandachtspunt. Onder andere bij het ministerie van VWS is niet aantoonbaar duidelijk hoe decentraal beleid aansluit op de centrale strategie. Hiermee ontstaat een potentieel risico op beleid (en vervolgens uitvoering) dat niet overeenkomt met doelstellingen van centraal geformuleerd beleid.

(2) Levend maken van beleid. Enkele departementen geven aan dat voorkomen moet worden dat het vastgestelde beleid "van het CIO-office" is, maar dat het moet gaan leven in de hele organisatie. In andere woorden: dat het onderdeel wordt van het primaire proces en niet louter een taak van de afdeling bedrijfsvoering is.

3.3.3 CIO en CISO: Rijksbreed beleid en strategie

In het Besluit staat vermeld dat de CISO een bijdrage levert aan het opstellen van het rijksbrede informatiebeveiligingsbeleid, het risicobeeld en het calamiteitenplan.[18] Bijdragen aan Rijksbreed beleid c.q. strategie verlopen volgens departementen via het CI(S)O-beraad. Het staat departementen vrij om daar punten in te brengen. Alle departementen geven aan dat zij de CISO Rijk adviseren via het CISO-beraad over de IB&P-risico's op hun departement.

3.4 CIO's, CISO's en CIO-offices ondernemen een diversiteit aan activiteiten ter bevordering van kennisdeling en bewustwording

Uit het Besluit blijkt dat de CIO met regelmaat activiteiten moet organiseren voor het delen van good practices en nieuwe inzichten rond digitalisering.[19] Alle departementen ondernemen verschillende activiteiten om *good practices* en nieuwe inzichten vanuit het CIO-office te delen. We constateren dat deze activiteiten worden ondernomen voor ofwel medewerkers van het CIO-office, ofwel voor medewerkers van het hele departement. Communicatie verloopt veelal via het intranet.

3.5 De CISO's bij de departementen krijgen informatie voor hun adviesrol m.b.t. informatiebeveiliging en privacy (IB&P) in verschillende vormen

Volgens het Besluit is de CISO belast met de advisering rondom IB&P op het departement.[20] CISO's en CIO-offices op alle departementen hebben verschillende manieren ontwikkeld om informatie tot zich te nemen voor deze risico's. Hieronder volgt een categorisatie.

[18] Zie noot 16.
[19] Besluit CIO-stelsel Rijksdienst, art. 4(d): "het richten op en stimuleren van digitale transformatie en technologisch gedreven innovatie binnen het ministerie door het investeren in een cultuur van kennisdeling en door het lerend vermogen op het gebied van digitalisering binnen het ministerie te bevorderen;"
[20] Besluit CIO-stelsel Rijksdienst, art.7(f): "het gevraagd en ongevraagd adviseren van de departementale CIO, het verantwoordelijk lijnmanagement en CISO's van dienstonderdelen over de informatiebeveiliging en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen;"

1. **Eigen risico-signalering.** Het ministerie van AZ verricht eigenstandige risicoanalyses, waarbij CISO-adviseurs tevens verantwoordelijk zijn voor de risicosignalering m.b.t. IB&P.

2. **Periodieke overleggen met dienstonderdelen.** Met name op departementen die een concern-inrichting hebben (zoals VWS), dan wel CISO's op dienstonderdelen (zoals BZK), worden periodieke overleggen gevoerd. In deze overleggen komen dan ook IB&P-risico's aan bod.

3. **Periodieke vragenlijsten.** Meerdere departementen werken met vragenlijsten c.q. zelf-evaluaties, op basis waarvan op maat gemaakt advies geleverd kan worden. We hebben dit gezien bij o.a. de ministeries van BZ, EZK/LNV en VWS.

4. **Projectaanvragen**. Diverse departementen gebruiken projectaanvragen als input voor hun advisering. Veelal wordt het CIO-office dan ook gevraagd om een advies bij een dergelijk project. Dit hebben wij o.a. geconstateerd bij de ministeries van BZ en SZW.

5. **Rapportages en audits**. Vanuit verschillende onderzoeken c.q. audits en maandelijkse rapportages komen risico's naar voren. De CISO en CIO-offices gebruiken dit vervolgens. Dit hebben wij o.a. geconstateerd bij de ministeries van AZ en J&V.

6. **Reguliere P&C-cyclus.** Verschillende departementen gebruiken het proces rondom de in control verklaring of het informatiebeveiligingsbeeld als input voor de advisering op IB&P-risico's.

7. **Incidenten en behoefte.** De laatste categorie voor input betreft incidenten rondom IB&P dan wel vragen vanuit de organisatie.

Good practice: site visits bij dienstonderdelen

Om op de hoogte te blijven van de IB&P-risico's bij dienstonderdelen, werkt het ministerie van VWS met zgn. site visits. De concern-CISO gaat samen met de FG of CPO naar een ander onderdeel van VWS om daar aan de hand van een agenda een inzicht te krijgen in de beheersing rondom IB&P.

Dit bevordert kennisdeling en inzicht bij de concern-CISO in specifieke risico's bij VWS, als ook verbinding tussen het concern en de dienstonderdelen.

Kortom: informatie en communicatie blijven niet louter een papieren exercitie.

4 Analysefase voltooid; plannen voor implementatie nog niet gereed

In dit hoofdstuk beschrijven wij de uitkomsten van ons onderzoek naar de verschillende analyses (§4.1) en plannen (§4.2) die de departementen hebben uitgevoerd om te voldoen aan de vereisten uit het Besluit.

4.1 Vrijwel alle departementen hebben fit-gap-analyses uitgevoerd

Om te analyseren in hoeverre de departementen voldoen aan de vereisten van het Besluit hebben vrijwel alle departementen een fit-gap analyse uitgevoerd, met uitzondering van de ministeries van BZK en Defensie. BZK geeft aan dat ze al in grote mate voldoet aan het Besluit. De analyses verschillen in uitvoerigheid. Bij sommige departementen zijn hier acties aan gekoppeld: een afwijking van het Besluit leidt in dat geval tot veranderingen of uitleg over het uitblijven daarvan.

4.2 De departementen zijn actief bezig met het Besluit, maar zijn afwachtend met het maken van plannen

Op het moment van onderzoek hadden zes departementen een korte termijnplanning. Geen departement had een middellange termijnplanning. Een aantal departementen gaf aan al op korte termijn (2022) klaar te zijn met de implementatie.

De bestaande korte termijnplanningen verschillen in uitvoerigheid. Twee departementen hebben SMART-doelen geformuleerd met acties en actiehouders, namelijk I&W en EZK/LNV. Deze acties zijn terug te leiden naar de doelen en dragen bij aan het voldoen aan de eisen vanuit het Besluit. De benodigde middelen worden meestal nog niet benoemd in de beschikbare plannen.

Departementen die nog niet over een korte termijnplanning beschikken, geven aan dat de deadline voor het opstellen van plannen na de zomer van 2021 ligt en dat ze de uitkomsten van deze audit willen meenemen.

Wij signaleren twee risico's wanneer plannen niet tijdig worden opgesteld, acties onvoldoende concreet (lees: SMART) zijn, en/of wanneer acties niet duidelijk zijn belegd bij een actiehouder:

- Departementen implementeren het Besluit niet volgens het geplande tijdspad.
- De acties sluiten onvoldoende aan op de vereisten van het Besluit.

Mogelijk gevolg is dat de doelstellingen van het Besluit niet worden behaald.
De departementen die nog geen plan opgesteld hebben, geven aan dat ze wel voornemens zijn in de zomermaanden van 2021 een plan op tafel te kunnen leggen.

Good practice: scenarioplanning voor implementatie Besluit

Binnen EZK/LNV is er een programma met meerdere sporen opgestart om (o.a.) aan het nieuwe CIO-besluit te voldoen. Voor elk spoor is er een actiehouder en is er een vergevorderd concept gereed met o.a. een fit-gap analyse en verschillende scenario's afhankelijk van de beschikbare middelen. In combinatie met een extern advies wordt er een implementatieadvies aan de CIO gedaan en is begin juni een eerste versie van het implementatieplan gereed in de vorm van een scenariobeschrijving.

Uitdaging in implementatie: wat wordt er verwacht van de plannen?

Departementen geven aan dat ze zoekende zijn naar de mate van diepgang in inhoud van de implementatieplannen. Wat wordt er precies van ze verwacht? Zoals hierboven aangegeven zien wij de implementatieplannen van EZK/LNV als een good practice.

5 Handelingsperspectief voor implementatie van het Besluit CIO-stelsel Rijksdienst: borg duidelijkheid en eenduidigheid door heldere communicatie en interpretatie

5.1 Schep duidelijke en eenduidige verwachtingen omtrent de vereisten vanuit het Besluit

Uit hoofdstuk 2 en hoofdstuk 3 van dit rapport blijkt dat de departementen op verschillende manieren invulling geven aan de key-elementen, de taken en bevoegdheden van de CIO en de CISO. Dit geldt bijvoorbeeld voor de adviesfunctie van de CIO en de CISO, maar ook voor de plaatsing van de CIO in de organisatie (een key-element). Uit de fit-gap-analyses (hoofdstuk 4) blijkt dat departementen op veel punten aangeven dat ze reeds voldoen aan het Besluit.

Hieruit maken wij op dat het Besluit veel ruimte laat voor **interpretatie**, deze ruimte wordt gebruikt door de departementen. Een mogelijk gevolg is dat er een **verscheidenheid in de implementatie** van het Besluit ontstaat. In de praktijk tot dusver blijkt dit uit de keuze van departementen om bepaalde (operationele) zaken wel op te pakken, maar belangrijke strategische key-elementen zoals de plaatsing van de CIO onder de SG te laten voor wat ze zijn.

Essentiële concepten zoals de CIO als **C-level executive** en **digitaal leider** dreigen hierdoor bij een deel van de departementen verloren te gaan. Daarnaast zijn definities niet altijd helder voor departementen. Genoemde voorbeelden zijn o.a. informatievoorzieningsbeleid en digitaliseringsbeleid. Bovendien worden de verschillende taken en verantwoordelijkheden van de CIO en de CISO verschillend opgepakt (bijv. de adviesfunctie).

De implementatie van het Besluit vraagt om een **sturingsrelatie** tussen CIO Rijk en de departementale CIO's die verdergaat dan het huidige coördineren en ondersteunen. Ondanks dat er al stappen op dit gebied genomen zijn, blijft er veel ruimte bestaan voor eigen invulling en interpretatie bij de departementen. Operationeel wordt het Besluit geïmplementeerd, maar op strategisch vlak bestaat het risico dat het idee achter het Besluit, zoals naar voren komt in het ABD-rapport en het Memorandum van Toelichting bij het Besluit, verloren gaat.

Handelingsperspectief

Als handelingsperspectief willen wij de CIO Rijk meegeven om duidelijke en eenduidige verwachtingen te scheppen omtrent de vereisten vanuit het Besluit om **een gewenste vorm van uniformiteit te borgen** tijdens de implementatiefase, zodat het strategische idee achter het Besluit niet verloren gaat. Besluit en communiceer hierbij duidelijk op welke aspecten **uniformiteit nodig** is en op welke aspecten **ruimte voor maatwerk** bestaat en stuur hier actief op.

5.2 Voorkom dat opgesteld beleid een papieren exercitie blijft

In hoofdstuk 3 hebben we reeds aangegeven dat het creëren van **"levend beleid"** een uitdaging vormt. Beleid wordt opgesteld door het CIO-office, maar wordt niet opgenomen in de uitvoering, terwijl het bijzonder relevant is dat een heel departement I-beleid serieus oppakt. Andere departementen lukt het wel "levend

beleid" te creëren. Er wordt gevraagd om uitwisseling van good practices tussen de departementen.

Mogelijk hangt dit samen met het feit dat de CIO-functie bij veel departementen een bedrijfsvoeringsfunctie is. Ook speelt de dubbele pet die de CIO vaak op heeft mogelijk een rol.[21] Een C-level executive met een vaste plek in de Bestuursraad heeft wellicht een sterkere positie om beleid actief te promoten en waar nodig de opvolging af te dwingen. Overkoepelend is zichtbaar dat het Besluit hier weinig verandering in dreigt te brengen, omdat een belangrijk deel van de departementen bij de implementatie dreigt te focussen op het aanpassen van beleidsstukken i.p.v. het aanpassen van kritieke zaken, zoals het creëren van een strategische positie voor de CIO. Een mogelijk risico is dat in opzet (op papier) het Besluit wordt geïmplementeerd, maar dat **er in de dagelijkse praktijk geen verandering zichtbaar wordt.**

Handelingsperspectief

Om te voorkomen dat departementaal intern beleid een papieren exercitie blijft en om te voorkomen dat het effect van het Besluit achterblijft bij de beschrijving van het Besluit, zien wij twee punten waarop de CIO Rijk de departementen verder kan ondersteunen:

(1) Zet verder in op het **uitwisselen van good practices** en het bespreken van probleempunten tussen de verschillende departementen.

(2) Zet in op **CIO's als digitale leiders**. Hiermee is het noodzakelijk het beeld van CIO als manager bedrijfsvoering te veranderen. Overweeg het volgende:

- In hoeverre het wenselijk is dat de CIO niet direct onder de SG valt, noch vast lid is van de Bestuursraad in het toekennen van uitzonderingen op het Besluit;
- In hoeverre – gelet op het belang en de zwaarte van de CIO-functie – de combinatie van de CIO-functie met een andere (lijnmanagement)functie wenselijk is.

5.3 Zorg voor een eenduidig mechanisme voor uitzonderingen op het Besluit

Het Besluit CIO-stelsel Rijksdienst heeft onder meer als doel om door beschrijving van taken en verantwoordelijkheden ervoor te zorgen dat de departementen de CIO- en CISO-rollen op een meer **uniforme manier** inrichten. Uit ons onderzoek blijkt dat deze rollen in de praktijk nog niet op uniforme wijze worden ingevuld. Zoals aangegeven in §5.1, geven wij als eerste handelingsperspectief mee dat de CIO Rijk duidelijke verwachtingen dient te scheppen over de vereisten in het Besluit.

Vervolgens blijkt uit ons onderzoek dat departementen op enkele onderzochte aspecten nog niet voldoen aan het Besluit. Enkele departementen geven aan dat zij gebruik willen maken van de **uitzonderingsclausule** (art. 17) in het Besluit. Uit ons onderzoek blijkt dat departementen niet goed weten hoe ze hiervan gebruik moeten maken (zie hoofdstuk 2).

Handelingsperspectief

Als handelingsperspectief willen wij de CIO Rijk meegeven om te zorgen voor een **eenduidig mechanisme voor uitzonderingen** op het Besluit, zodat departementen weten hoe zij uitzonderingen c.q. afwijkingen conform artikel 17 kunnen afstemmen. Neem hierbij de **mate van formaliteit** van een dergelijk mechanisme in overweging, zodat deze aansluit bij de geest van het Besluit, de implementatie ervan en de relatie tussen CIO Rijk en de departementale CIO's.

[21] Zie hoofdstuk 2: Departementen vullen de key-elementen van het Besluit verschillend in.

5.4 Overweeg een onderzoek naar de relaties tussen de CIO en CISO Rijk en de departementale tegenhangers, alsook een vervolg op het huidige onderzoek op de middellange termijn

Dit onderzoek had als scope specifieke aspecten van de functie van de departementale CIO en CISO. De functie van de CIO Rijk en de CISO Rijk, alsook de relatie tussen deze en de departementale tegenhangers hebben wij niet onderzocht. Dat betekent dat dit rapport en de daaruit voortvloeiende resultaten een gedeelte van het besluit hebben onderzocht. Voor een goed functionerend, rijksbreed CIO-stelsel is de relatie tussen de CIO en CISO Rijk enerzijds en de departementale tegenhangers anderzijds van uiterst groot belang.

Handelingsperspectief

Overweeg een **onderzoek naar de verhoudingen en relaties** tussen de departementale CIO en CISO en de CIO en CISO Rijk. Overweeg tevens **een vervolg op dit onderzoek** op de middellange termijn (twee à drie jaar) om (beleids)effecten in kaart te brengen.

6 Verantwoording onderzoek

6.1 Werkzaamheden en afbakening

Op 25 maart 2021 is de opdrachtbevestiging, met het kenmerk 2021-0000060883 ondertekend. Het veldwerk heeft plaatsgevonden in de periode april en mei 2021.

6.1.1 Doelstelling en onderzoeksvragen

Het doel is van het onderzoek is, naast inzicht bieden in de mate van implementatie van het Besluit, op basis van de resultaten departementen meer gericht te kunnen ondersteunen bij de versterking van de CIO-functie. De onderzoeksvraag is: "Hoe verhoudt het huidige beeld van (een deel van) de invulling van de CIO- en CISO-functies bij de twaalf ministeries zich tot de voorschriften in het Besluit CIO-stelsel Rijksdienst?"

Hiervoor hebben we twee deelvragen opgesteld:

1. In hoeverre voldoen de huidige inrichtingen van de CIO- en CISO-functies bij de departementen aan de vereisten van het Besluit?
2. Welke analyses hebben de departementen uitgevoerd en/of zijn de departementen van plan om uit te voeren om te kunnen voldoen aan het Besluit?

In hoofdstuk 2 en 3 geven wij antwoord op de eerste onderzoeksvraag; in hoofdstuk 4 wordt antwoord gegeven op de tweede onderzoeksvraag.

6.1.2 Object van onderzoek en afbakening

Het onderzoek kent twaalf objecten van onderzoek: de twaalf departementen binnen de Rijksoverheid. De ministeries van EZK en LNV zijn in samenhang onderzocht, omdat zij dezelfde CIO en CIO-office delen.

We hebben niet de implementatie van het hele Besluit onderzocht. In overleg met de opdrachtgever hebben wij een aantal onderwerpen uitgekozen. Deze zijn verwerkt in het referentiekader (zie bijlage 1).

6.1.3 Referentiekader

Als referentie is het "Besluit CIO-stelsel Rijksdienst 2021" genomen. Gekozen artikelen van het besluit zijn verwerkt in het referentiekader, zie bijlage 1. Het referentiekader is gehanteerd voor de eerste deelvraag.

Naast de referenties vanuit het Besluit hebben wij de tweede deelvraag nader geoperationaliseerd met een aantal criteria. Deze zijn verwerkt in het referentiekader (zie bijlage 1).

Het referentiekader is met de opdrachtgever samengesteld en afgestemd.

6.1.4 Uitvoering veldwerk

Het onderzoeksteam heeft het veldwerk uitgevoerd in de periode april en mei 2021. We hebben de volgende activiteiten uitgevoerd.

Vragenlijst

Aan de hand van een vooraf opgestelde vragenlijst hebben wij informatie vergaard bij alle departementen. Hierbij is documentatie opgevraagd om de antwoorden te ondersteunen. Eventuele onduidelijkheden hebben wij in de interviews behandeld.

Documentenstudie

De volgende documenten zijn geanalyseerd:

- interne beleidsstukken;
- interne procedures en procesbeschrijvingen;
- taakomschrijvingen van CIO, CISO en CI(S)O-office medewerkers;
- fit/gap-analyses (indien van toepassing);
- plannen om te voldoen aan het besluit (indien van toepassing);
- overige relevante documentatie zoals opgeleverd door de departementen.

Interviews
Met ieder departement is een verdiepend interview gevoerd. Dit interview diende om eventuele onduidelijkheden vanuit de vragenlijst op te helderen, dan wel om verdieping aan te brengen in de analyse van het onderzoeksteam. In onderstaande tabel geven wij per departement aan met welke functionarissen wij hebben gesproken in de onderzoeksperiode.

Dept.	Functionarissen	Onderzoekperiode
AZ	CIO, CISO, medewerker CIO-office	10-05 t/m 11-05
BZ	CIO, CISO, medewerker CIO-office	28-04 t/m 30-04
BZK	plaatsvervangend CIO, medewerker I-interim Rijk	28-04 t/m 30-04
OCW	adviseur en coördinerend adviseur Cluster Strategisch Informatiebeleid, waarnemend hoofd Cluster Informatiebeleid	17-05 t/m 22-05
FIN	medewerker CIO-office	20-05 t/m 21-05
DEF	medewerkers CIO-office	10-05 t/m 12-05
I&W	medewerkers CIO-office	19-04 t/m 23-04
EZK/LNV	CIO, CISO	20-04 t/m 28-04
SZW	CIO, CISO, BVA, medewerker CIO-office	03-05 t/m 04-05
J&V	beoogd CISO, medewerker CIO-office	10-05 t/m 17-05[22]
VWS	medewerker CIO-office, aanvullende schriftelijke communicatie met waarnemend CISO	12-05 t/m 13-05

Tabel 3. *Overzicht geïnterviewde functionarissen en onderzoeksperiode per departement.*

6.1.5 *Analyse*
Per departement is een eerste analyse gemaakt in de factsheets. Dit valt onder de bovengenoemde onderzoeksperiode. De overkoepelende analyse heeft voornamelijk plaatsgevonden in de laatste twee weken van mei. Het onderzoeksteam heeft de gegevens gestructureerd en geanalyseerd middels verwerking in een gegevenstabel.

6.1.6 *Rapportage*
De uitkomsten van de analyse zijn verwerkt in dit rapport. De conceptrapportage is besproken met de opdrachtgever d.d. 1 juli 2021; met het voorportaal van het CIO-beraad d.d. 23 augustus 2021; en met het CIO-beraad d.d. 15 september 2021. Hierna is het onderzoeksrapport definitief gemaakt.

6.2 Gehanteerde standaard en kwaliteitsborging
Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van

[22] Op 27 mei 2021 heeft de Minister van Justitie en Veiligheid een Besluit genomen, waaruit blijkt dat de CIO rechtstreeks onder de SG valt en zitting heeft in de Bestuursraad. Dit Besluit werkt terug tot en met 10 mei 2021. Hoewel het nemen van het Besluit buiten de onderzoeksperiode valt, heeft het effect op de situatie in de onderzoeksperiode, gelet op de terugwerkende kracht.

kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

6.3 Verspreiding rapport

De opdrachtgever is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

7 Ondertekening

Den Haag, 19 oktober 2021

Projectleider

Auditdienst Rijk

Bijlage 1: Referentiekader

Hoofdvraag
Hoe verhoudt het huidige beeld van (een deel van) de invulling van de CIO en CISO-functies bij de twaalf ministeries zich tot de voorschriften in het Besluit CIO-stelsel Rijksdienst?

Deelvraag 1
Op welke wijze voldoen de huidige inrichtingen van de CIO- en CISO-functies bij de departementen aan de vereisten van het Besluit?

Aanwezigheid key-elementen

- De CIO* is organisatorisch rechtstreeks onder de SG van het departement geplaatst (art. 3.1).
- De CIO heeft een CIO-stelsel ingericht voor het ministerie en de dienstonderdelen (art. 3.3).
- De CIO is lid van en neemt actief zitting in de Bestuursraad van het ministerie (art. 3.4.).
- De CIO beschikt over een CIO-office met een aantal FTE (art. 3.5).
- De CISO* is onderdeel van het departementale CIO-office (art. 6.1).

CISO | taken | verantwoordelijkheden | bevoegdheden

- advies -

Lijnmanagement

- De CISO geeft schriftelijke en mondelinge adviezen aan het lijnmanagement en CISO's van dienstonderdelen over informatiebeveiliging en risico's bij: wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten en informatieprocessen en informatiesystemen (art. 7.f).

CISO Rijk

- De CISO geeft schriftelijke en mondelinge adviezen aan de CISO Rijk over informatiebeveiliging en risico's bij het betreffende ministerie (art. 7.g).

- beleid, procedures & strategie -

- De departementale CISO is betrokken bij het opstellen van het rijksbrede informatiebeveiligingsbeleid, het risicobeeld en het calamiteitenplan en de rijksbrede I-strategie en aan het integrale beveiligingsbeleid, de risicoanalyse en het calamiteitenplan (art. 7.e).

- informatie -

- De departementale CISO is op de hoogte van de risico's bij: wet- en regelgeving, investeringen en beleids- en uitvoeringstrajecten (art. 8.2).

CIO | taken | verantwoordelijkheden | bevoegdheden

- advies -

- De CIO heeft een rol als adviseur in het primaire proces (art. 3.2)
- De CIO geeft mondelinge en schriftelijke adviezen aan het lijnmanagement en de minister over IV- en digitaliseringsbeleid (4.b).
- De CIO geeft schriftelijke en mondelinge adviezen aan het lijnmanagement en de minister over de implicaties voor IV en digitalisering, met betrekking tot (voorgenomen) veranderingen in: wet- en regelgeving; beleidstrajecten; uitvoeringstrajecten; en investeringen.

- oordeel -

- De CIO velt bij activiteiten met een grote ICT-component een oordeel over: de beheersing, de haalbaarheid, de risico's en de implicaties van de activiteit (art. 4.i).
- Bij een negatief CIO-oordeel worden de adviezen meegenomen voor de start van een ICT-ontwikkelproject of wordt hier beargumenteerd van afgeweken (art. 5.3)

- beleid -

- De CIO heeft informatievoorzieningsbeleid opgesteld (art. 3.2).
- De CIO heeft digitaliseringsbeleid opgesteld (art. 3.2)

- communicatie -

- De CIO organiseert met regelmaat activiteiten waarin nieuwe inzichten en good practices rond digitalisering worden gedeeld binnen het departement (art. 4.d).

Deelvraag 2
Welke analyses hebben de departementen uitgevoerd en/of zijn de departementen van plan om uit te voeren om te kunnen voldoen aan het Besluit?

- Er is een korte (tot eind 2021) en middellange planning (tot eind 2023).
- Doelen zijn SMART-geformuleerd.
- Acties zijn terug te leiden naar de geformuleerde doelen.
- Per actie is één primaire actiehouder aangewezen.
- Er zijn voldoende middelen beschikbaar gesteld.
- Uit het plan is duidelijk hoe de acties bijdragen aan het voldoen aan de eisen vanuit het Besluit.

** Waar wij "CIO" dan wel "CISO" optekenen, bedoelen wij "departementale CIO" en "departementale CISO".*

Bijlage 2 Managementreactie CIO Rijk

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Auditdienst Rijk
Aan de Accountdirecteur BZK-JNV

_
Postbus 20201
2500 EA Den Haag

DG Overheidsorganisatie
Directie CIO Rijk

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Contactpersoon
_

Kenmerk
2021-0000543891

Datum	15 oktober 2021
Betreft	Managementreactie op het rapport 'Uitkomsten nulmeting Besluit CIO-stelsel Rijksdienst'

Geachte _,

Ik dank u voor het rapport 'Uitkomsten nulmeting Besluit CIO-stelsel Rijksdienst' - het finaal concept van mei 2021 (exacte datum niet vermeld) - en de daarin opgenomen aanbevelingen. De bijdrage van de Auditdienst Rijk (ADR) is belangrijk voor de implementatie van dit besluit en het verder versterken van de CIO- en CISO-functies binnen het Rijk.

De centrale boodschap van het rapport valt uiteen in drie rode draden die ik hieronder kort samenvat. Ik vind het daarbij waardevol om ook te kijken naar de bedoeling van het CIO-besluit, namelijk dat de positie van de CIO zodanig is dat hij of zij toegang heeft tot het hoogste bestuursniveau. Als laatste ga ik in op uw overwegingen voor het doen van vervolgonderzoek.

1. Strategische positie van de CIO- en CISO-functie niet overal ingevuld

CIO niet overal in de Bestuursraad
Een van de uitkomsten van de nulmeting is dat bij vijf van de 12 departementen de CIO niet rechtstreeks onder de SG is gepositioneerd en vaak geen actieve rol heeft in de Bestuursraad. Tegelijkertijd geven de betreffende CIO's aan dat zij wel aan de Bestuursraad kunnen deelnemen indien zij dit nodig vinden.

- In het kader van de persoonsafhankelijke borging van CIO's op een departement vind ik dit een waardevolle constatering. Juist vanuit de gedachte dat I meer in het hart van beleidsvorming wordt gebracht, hecht ik eraan dat de CIO's in het stelsel digitaliseringsvraagstukken vanuit een actieve rol agenderen en hun collega's in de Bestuursraad direct kunnen adviseren.
- Echter, de bedoeling van artikel 3 lid 4 in het Besluit CIO-stelsel is dat de CIO's op het juiste moment aan de juiste tafel(s) en/of op de juiste bestuursniveaus zitten. En bij bijvoorbeeld het ministerie van VWS is dat effectief een andere tafel dan bij het ministerie van Defensie.

Indien nodig zal ik het gesprek over de strategische positionering ook agenderen in andere gremia, bijvoorbeeld het overleg van de secretarissen-generaal (het SGO). Het gaat mij er vooral om dat de interventiekracht op het juiste niveau ligt.

Comply or explain: maar wanneer en waar
In een aantal gevallen zouden departementen niet goed weten hoe zij hun uitzonderingen op het Besluit met mij kunnen communiceren.

- Om de collega's van de CIO-offices zoveel als mogelijk de gelegenheid te geven om vragen te stellen en andere zaken waar zij tegenaan lopen bij de implementatie van het Besluit bespreekbaar te maken, organiseert mijn directie periodiek informatiebijeenkomsten.
- Kijkend naar de formele kant is het - op grond van het al eerdergenoemde Coordinatiebesluit - de minister van BZK die de geadresseerde is voor de 'explains' vanuit de departementen. De CIO Rijk is in dat geval de partij die de minister adviseert over hoe om te gaan met de (gevraagde) explain. Ik zal ervoor zorgen dat deze formele lijn ook voor het voetlicht wordt gebracht bij een van de komende informatiebijeenkomsten voor de CIO-offices.
- Daarnaast staat de implementatie van het Besluit ook op de agenda van de voor- en najaarsgesprekken die ik met de CIO's van de ministeries en grote uitvoerders heb.
- Tenslotte neem ik uw aanbeveling ter harte om te zorgen voor een eenduidig mechanisme voor uitzonderingen op het Besluit en neem daarbij de mate van formaliteit in overweging. Welke vorm dat precies krijgt, verken ik nog voor het einde van dit jaar.
- Ik verwacht dat met deze acties begin volgend jaar de eventuele onduidelijkheid over het hoe en wanneer communiceren van uitzonderingen op het Besluit is weg genomen. Bij ingewikkelder vraagstukken is er desgewenst ook een jurist beschikbaar die de departementen kan bijstaan met interpretatie- of implementatievragen.

Combinatie pSG- en CIO-rol
Tenslotte geeft u aan zorgen te hebben bij het halen van het doel van 'CIO als digitaal leider' in het geval de CIO-rol wordt gecombineerd met de functie van pSG.

- Deze zorg onderstreept de beweging die ik van harte ondersteun, namelijk het weg bewegen van IV en ICT van het bedrijfsvoeringsdomein, meer richting het primair proces: I in het hart. Het positioneren van een aparte vakman of -vrouw in de rol van CIO met directe toegang tot de juiste bestuurlijke tafel (al dan niet met een vaste plek in de Bestuursraad) sluit daar goed op aan. Daarbij merk ik op dat digitaal leiderschap over meer gaat dan een positie in de Bestuursraad; de essentie is een leidende rol in de ondersteuning van het primair proces met de middelen die er zijn.
- Indien gewenst kan en zal ik vanuit de directie CIO Rijk ondersteuning bieden bij de verdere invulling van digitaal leiderschap. Bijvoorbeeld door het faciliteren van het goede gesprek en het delen van good practices. Het hebben van bilateraal overleg met de bewindspersoon - door een aantal

CIO's in de nulmeting genoemd - vind ik een heel mooi voorbeeld dat naadloos aansluit bij de bedoeling van het CIO-stelsel.
- In het rapport miste ik de nuance waar het gaat om de rol van de pSG. Deze is in uw rapport enkel belicht als bedrijfsvoeringsrol en dat is niet correct; een pSG heeft immers ook een eigenaarsrol met verantwoordelijkheden voor uitvoering en toezicht.
- Verder geef ik u graag de notie mee dat de leden van het CIO-beraad waarbij deze dubbelrol geldt, (ook tijdens de interviews) nadrukkelijk hebben aangegeven dat er voordelen zijn bij deze combinatie en dat de ADR zelf ook heeft aangegeven dat naast nadelen ook voordelen zijn aan deze dubbelrol. In het rapport zijn echter alleen de nadelen belicht.

2. Het Besluit biedt ruimte voor verscheidenheid in implementatie

U constateert dat het Besluit ruimte biedt voor verschillen in de wijze van implementatie bij de departementen op het gebied van advisering, het doen van CIO-oordelen, beleidsvorming, informatie en communicatie over hun ICT/informatievoorziening.
- Ik deel uw advies om de uniformiteit van het Besluit zoveel als mogelijk te borgen. Feit blijft dat artikel 17 van het Besluit ruimte biedt om op onderdelen af te wijken wanneer het de effectiviteit van beoogde doelen ten goede komt. Elk departement heeft immers haar eigen kleur, cultuur en daarbij passende organisatiestructuren en -gebruiken, en daar moet ruimte voor zijn. En dat geldt natuurlijk ook voor de grote uitvoerders.
- Ik zal in de nog geplande informatiebijeenkomsten extra aandacht geven aan het meer expliciete gesprek over op welke aspecten van het Besluit uniformiteit nodig is en op welke aspecten er ruimte is voor maatwerk.

3. Alle departementen zijn bezig met de implementatie van het Besluit

De laatste constatering is dat alle departementen zich voorbereiden op passende acties die voor hen nodig zijn om te voldoen aan de vereisten van het Besluit. Het merendeel heeft een fit/gap-analyse uitgevoerd en bijna de helft heeft korte termijnplannen. Tegelijkertijd geeft u aan dat de plannen voor de middellange termijn veelal nog niet klaar zijn en dat de departementen signaleren dat er een uitdaging in de implementatie ligt om de veranderingen en geformuleerd beleid verder in te bedden in de organisatie.
- Ik ben blij te horen dat departementen zich voorbereiden op acties om te kunnen voldoen aan de vereisten van het Besluit.
- Ik verwacht dat de departementen de departementale implementatieplannen, zoals afgesproken in het SGO, eind september gereed hebben. Hoewel de verantwoordelijkheid voor het (tijdig) opstellen van de departementale implementatieplannen bij de departement zelf ligt, zal ik hen via het CIO-beraad aanmoedigen een tandje bij te zetten om deze planning te halen.
- Ook vraag ik de dossierhouders van mijn directie om met de CIO-offices in gesprek te blijven over (de ontwikkeling van) hun plannen, daar waar nodig extra te ondersteunen met uitleg over onduidelijkheden en het interdepartementaal delen van good practices te bevorderen.

DG Overheidsorganisatie
Directie CIO Rijk

Datum
15 oktober 2021

Kenmerk
2021-0000543891

Vervolgonderzoek
Als laatste van de geformuleerde handelingsperspectieven geeft u de overweging mee een onderzoek naar de relaties tussen de CIO Rijk en CISO Rijk en de departementale tegenhangers te doen, alsook voor de middellange termijn een vervolg op deze nulmeting te doen.

- Het Besluit is zeker ook bedoeld om het CIO-stelsel navolging te laten krijgen op de eigen departementen. Uw advies om vervolgonderzoek te doen naar de relaties tussen de CIO Rijk en CISO Rijk en hun departementale tegenhangers neem ik dan ook aan. U ontvangt hiervoor te zijner tijd van mij de opdracht. Ik vind het daarbij belangrijk dat er ook goed wordt gekeken naar de integrale I-verantwoordelijkheid van de CIO; die is immers belast met de ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid, het zorgdragen voor de ontwikkeling en het beheer van de informatiesystemen van het ministerie, en het inrichten van het CIO-stelsel voor zijn of haar ministerie en de onder haar ressorterende dienstonderdelen. Daarbij vraag ik bij voorbaat aandacht voor het ministerie van Justitie en Veiligheid; vanwege de sui generis organisaties in haar stelsel ligt de integrale I-verantwoordelijkheid aldaar anders.
- Een vervolgonderzoek op deze nulmeting op de middellange termijn klinkt logisch. Ik verwacht hier in de loop van 2022 bij u op terug te komen.

Tenslotte meld ik voor de volledigheid dat ik, gezien de status van het rapport (een finaal concept) en de geanonimiseerde weergave van de bevindingen, voornemens ben het rapport te publiceren op www.rijksoverheid.nl.

Met vriendelijke groet,

CIO Rijk

Bijlage 3: Factsheets van de ministeries

De factsheets zijn separaat aan dit onderzoeksrapport meegezonden als bijlage aan de opdrachtgever.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00