Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid'

Colofon

Titel	Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid'
Uitgebracht aan	CIO Rijk
Datum	3 juli 2024
Kenmerk	2024-0000370881
Referentienummer	2023-BZK-026

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

(Management)samenvatting

Op verzoek van de CIO Rijk heeft de Auditdienst Rijk (ADR) een onderzoek uitgevoerd met als doel inzicht te bieden in de operationele toepasbaarheid van de elf voorwaarden uit het rijksbrede public cloudbeleid 2022 (verder: RPCB) voor de Rijksoverheid. Hiertoe is onderzoek gedaan naar de toepassing van het RPCB voor drie public clouddiensten die worden ingezet binnen de Rijksoverheid en die vrijwillig door departementen in overleg met CIO Rijk zijn aangemeld voor dit onderzoek. De eerste dienst betreft een Software as a Service (SaaS) applicatie ten behoeve van een uitvoerende dienst van een departement. Ontwikkeling en beheer vindt hierbij plaats door een klein Nederlands bedrijf waarbij daadwerkelijke levering van de betreffende applicatie plaatsvindt middels het platform van een grote Amerikaanse public cloudprovider. De tweede en de derde dienst zijn gerelateerd aan de digitale werkplek van rijksambtenaren. Het betreft het gebruik van Microsoft 365 (voor licentiebeheer via de public cloud van kantoorsoftware op locatie) en MS Teams (videoconferencing en chat) respectievelijk Microsoft Exchange Online voor de (gedeeltelijke) verwerking van e-mail van een departement in de public cloud.

Samenvattend beeld is dat de invoering van het RPCB een proces in uitvoering is. Het RPCB is bijvoorbeeld nog maar deels vertaald in departementaal cloudbeleid. De drie onderzochte diensten zijn gebaseerd op departementaal beleid en strategie dat dateert van voor het RPCB uit 2022. Bij de implementatie van deze diensten is op onderdelen al wel gebruik gemaakt van het RPCB. Het onderzoek heeft geresulteerd in een aantal bevindingen en aanbevelingen. De belangrijkste worden opgesomd.

Uitbreiden RPCB op onderwerpen buiten informatiebeveiliging en privacy
De voorwaarden zoals beschreven in het huidige RPCB hebben met name betrekking op privacy en informatiebeveiliging. Gesignaleerd wordt dat ook buiten deze voorwaarden behoefte is aan strategische richting voor de inzet van cloud. Een eerste onderwerp is ketenregie. Binnen de Rijksoverheid wordt veelal in ketens samengewerkt met vele partners. Een risico is dat de IT-ondersteuning voor een keten niet uniform en daardoor suboptimaal wordt ingericht, bijvoorbeeld omdat het ene onderdeel van een keten geen gebruik mag maken van public cloud terwijl dit voor een ander deel wel is toegestaan. Een tweede onderwerp is ‘sourcing’ van IT als het strategisch kiezen van externe dienstverleners (zoals bijvoorbeeld public cloud) om bepaalde IT-functies te realiseren. Een risico is dat het RPCB wordt gelezen als ‘cloudbeleid’ en niet als ‘public cloudbeleid’ waardoor alternatieven zoals het gebruik van een private cloud onvoldoende worden beschouwd. Aanbeveling is om deze twee onderwerpen toe te voegen aan het RPCB.

Effectiviteit en efficiëntie van proces van risicoafweging
Voor alle drie de diensten is een proces van risicoafweging op het gebied van privacy en informatiebeveiliging doorlopen. De wijze van uitvoering en vastlegging hiervan laat grote verschillen zien tussen de diensten. Ook is het beeld dat de risicoweging een fors beslag legt op beschikbare kennis en capaciteit en dat de inhoud van de risicoafwegingen inhoudelijk een aanzienlijke overlap vertonen en uitkomsten vergelijkbaar zijn. Inschatting is dat op het niveau van de Rijksoverheid significant dubbel werk wordt uitgevoerd. Het risico ligt aan de ene kant in de effectiviteit van de afweging: de grote verschillen in het proces zouden kunnen leiden tot verschillende uitkomsten en verschillen in risicoacceptatie. Aan de andere is efficiëntie relevant: het deels dubbel uitvoeren van het proces van risicoafweging door verschillende organisaties binnen de Rijksoverheid dient te worden voorkomen. De aanbeveling is om te onderzoeken op welke wijze (bijvoorbeeld door het bevorderen van samenwerking) de effectiviteit en efficiëntie van het proces van risicoafweging te versterken en de uitkomsten op te nemen in het RPCB.

Centraal inzicht informatie soevereiniteit en marktconcentratie
Uitgangspunt is dat departementen onder de voorwaarde 'gekend gebruik' hun materieel public cloudgebruik en de risico's daarvan rapporteren aan de CIO Rijk. Voor zover een overzicht is te vormen op basis van een deelwaarneming van drie diensten, is het beeld dat registratie van materieel public cloudgebruik binnen departementen in ontwikkeling is. In 2023 is nog geen rechtstreekse opgave van cloudgebruik aan CIO Rijk gedaan maar is wel informatie ter beschikking gesteld die in het kader van het onderzoek naar cloud door de Algemene Rekenkamer is verzameld. Risico van het (deels) ontbreken van centraal inzicht in het gebruik van public cloud is dat juist op onderwerpen die overzicht op het niveau van de Rijksoverheid als geheel vragen zoals soevereiniteit en marktconcentratie een afweging niet optimaal kan plaatsvinden.
De aanbeveling is om het rapportageproces conform RPCB te versterken. Houd hierbij wel rekening met de (te) hoge administratieve lastendruk op het gebied van verantwoording over IT die departementen aangeven te ervaren.

Continuïteit bedrijfsprocessen als belangrijk onderdeel exit strategie
De focus van het onderwerp exit strategie ligt in het RPCB op de afspraken met de public cloudprovider op het gebied van overdracht en vernietiging van data bij contractbeëindiging. In onderliggende documentatie voor het RPCB is de exit strategie breder gericht op onder meer de continuïteit van de bedrijfsprocessen die gebruik maken van public cloud IT-voorzieningen. In de praktijk zijn in de contracten van de drie onderzochte diensten cloudexit bepalingen opgenomen over de teruggave van data aan de Rijksoverheid en vervolgens de vernietiging van data bij de public cloudprovider. Een volledige uitwerking van een exit strategie gericht op de continuïteit van de ondersteunde bedrijfsprocessen is voor geen van de drie onderzochte diensten aangetroffen. Het risico is dat de huidige voorwaarden in het RPCB en onderliggende documenten niet leiden tot een uitwerking van een exit strategie op het gewenste niveau, waardoor bij een cloudexit de continuïteit van de ondersteunde bedrijfsprocessen van de Rijksoverheid niet voldoende is geborgd. De aanbeveling is om te onderzoeken op welke wijze het onderwerp exit strategie kan worden opgenomen in het RPCB zodanig dat (onderdelen van) departementen in staat zijn dit onderwerp voldoende effectief op te pakken. Ga hierbij ook na welke rijksbrede ondersteuning noodzakelijk is en of het wellicht mogelijk is om op dit onderwerp (deels) centraal binnen de Rijksoverheid samen te werken.

Digitale werkplek Rijksoverheid als voorbeeld grootschalig gebruik public cloud
Een belangrijke casus op het gebied van public cloud is de (digitale) werkplek voor de Rijksoverheid met functionaliteit zoals bijvoorbeeld tekstverwerking, e-mail, chat etc. Op het moment verkeert de Rijksoverheid in een transitiefase waarbij voor een groot deel stapsgewijs wordt overgegaan naar onder meer MS 365, de public cloudoplossing van Microsoft voor de werkplek. Hiermee wordt de on-premises werkplek van de Rijksoverheid verplaatst naar de public cloud. De eerder in deze samenvatting genoemde bevindingen, bijvoorbeeld op het gebied van soevereiniteit en marktconcentratie, zijn ook zeker relevant voor deze casus. Verder geldt voor algemene functionaliteit als de werkplek die alle onderdelen van de Rijksoverheid in principe gebruiken, een risico dat departementen in gelijke omstandigheden andere keuzes maken zowel op het gebied van risicomanagement als op het gebied van fundamentele technische inrichtingskeuzes. Aanvullend is de dreigingsaantrekkende werking van een werkplek op basis van MS 365 relevant. Deze komt voort uit het feit dat straks niet alleen (bijna) de volledige Rijksoverheid gebruik maakt van MS 365 maar ook vele buitenlandse overheden en bedrijven wereldwijd. Dit resulteert in een zeer grote verzameling vertrouwelijke data die bijvoorbeeld statelijke actoren een belangrijk motief geeft voor ontwikkeling van aanvalsmogelijkheden op MS 365. Een aanbeveling is om in het RPCB in te gaan op (het beheersen van) risico's van het gebruik van algemene IT functionaliteit uit de public cloud (zoals de werkplek) die (vrijwel) alle departementen inzetten.

Tot slot wordt opgemerkt dat de bevindingen uit dit onderzoek dienen te worden beschouwd als resultaten ten behoeve van een eerste evaluatie. Aanbeveling is om de evaluatie van het RPCB te herhalen op een moment dat dit volledig is ingevoerd of indien externe ontwikkelingen een eerdere evaluatie noodzakelijk maken.

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

Sinds 2006 hebben public clouddiensten zich wereldwijd in een hoog tempo ontwikkeld. De drijvende kracht achter de adoptie van public cloud ligt in meerdere factoren zoals schaalbaarheid, flexibiliteit en vermindering van kapitaalinvesteringen in eigen hardware. Ook de toegang tot vernieuwende technologieën en diensten en eenvoudige geografische spreiding van informatiesystemen in het kader van bedrijfscontinuïteit zijn potentiële voordelen van toepassing van public cloud. Uiteraard zijn er ook remmende factoren zoals bijvoorbeeld risico's op het gebied van gegevensbescherming en privacy mede in relatie tot naleving van de Algemene Verordening Gegevensbescherming. Ook de potentiële afhankelijkheid van een zeer beperkt aantal leveranciers van public clouddiensten met een specifieke geografische achtergrond levert belangrijke vragen op rond aspecten als een marktconcentratierisico en (Nederlandse) soevereiniteit. Voor de Rijksoverheid is een relevante achterliggende vraag in hoeverre zij bij grootschalige inzet van public cloud diensten voor het realiseren van essentiële overheidstaken zich in economische en geopolitieke zin (te) afhankelijk maakt van eerder genoemde leveranciers.

In de jaren 2010/2011 is voor de Rijksoverheid voor het eerst expliciet de discussie gevoerd over de inzet van de verschillende vormen van cloudgebruik zoals public en private cloud. Dit heeft in 2011 geleid tot een Kamerbrief waarin het kabinet stelde dat de argumenten tegen het toepassen van public cloud op dat moment globaal zwaarder wogen dan de voordelen. In 2021/2022 is deze discussie hernieuwd met als uitkomst dat de staatssecretaris voor Koninkrijksrelaties en Digitalisering op 29 augustus 2022 het nieuwe rijksbrede public cloudbeleid 2022 (verder: 'het RPCB') per brief heeft gedeeld met de Tweede Kamer. Dit betreft een uitwerking van de nieuwe visie op het gebruik van public clouddiensten door de Rijksoverheid. Kort samengevat stelt deze nieuwe visie dat de mogelijkheden voor de inzet van public cloud door de Rijksoverheid significant worden vergroot. In haar brief doet zij verder de toezegging om extra aandacht te vragen van de departementen voor verantwoording over de risicoanalyses en bescherming van persoonsgegevens en om – als onderdeel van de controle op het beleid – vanaf 2023 te starten met evaluatie van dit beleid. In dit licht heeft de CIO Rijk aan de Auditdienst Rijk (ADR) verzocht om een gevraagd onderzoek uit te voeren naar het RPCB als een bouwsteen voor de invulling van deze toezegging.

1.2 Doelstelling en onderzoeksvragen

In het RPCB staan elf voorwaarden voor de Rijksoverheid (exclusief het Ministerie van Defensie) voor de inzet van public cloud. De doelstelling van dit onderzoek is om inzicht te bieden in de operationele toepasbaarheid van deze voorwaarden uit het cloudbeleid voor concrete public cloud programma's. Dit betreft programma's (of projecten) gericht op de invoering van public cloud voor een deel van de informatievoorziening van een departement of dienst hiervan. Ook zijn mede aan de hand van praktijkervaringen uit genoemde programma's en eigen observaties van ADR verbeterpunten in beeld gebracht. De uitkomsten van het onderzoek kunnen ten eerste door opdrachtgever worden gebruikt om het RPCB te versterken en ten tweede dienen als bron voor het invullen van de toezeggingen omtrent het RPCB aan de Tweede Kamer.

Teneinde invulling te geven aan de doelstelling van dit onderzoek zijn de volgende vragen beantwoord:

1. Welke bevindingen heeft ADR ten aanzien van de operationele toepasbaarheid van de elf voorwaarden uit het cloudbeleid in drie public cloud programma's?
2. Wat zijn de ervaringen binnen de drie programma's met het toepassen van het cloudbeleid met name op het gebied van eventuele ontbrekende voorwaarden?

1.3 Afbakening en definities

Het object van onderzoek betreft het rijksbrede public cloudbeleid[1] uit 2022 (RPCB). Dit is aangevuld met het Implementatiekader risicoafweging cloudgebruik[2] (verder: implementatiekader) en de Handreiking risicobeheersing public clouddiensten[3] (verder: handreiking). Hierbij ligt de focus op de operationele toepasbaarheid van de elf voorwaarden in het RPCB. Het kwaliteitscriterium 'operationele toepasbaarheid' houdt in dat een voorwaarde uit het cloudbeleid effectief en efficiënt kan worden toegepast binnen de activiteiten van een public cloud programma en bijdraagt aan de doelstellingen van dit programma als geheel. Waar in deze rapportage wordt verwezen naar het RPCB wordt in principe ook het onderliggende implementatiekader en handreiking bedoeld, tenzij expliciet ander beschreven. In het onderzoek wordt in het bijzonder de nadruk gelegd op onderwerpen als de naleving van wet- en regelgeving op het gebied van gegevensbescherming en privacy en de toepassing van risicoanalyse. Een public cloud programma is voor dit onderzoek gedefinieerd als een IT-programma of -project gericht op de invoering en toepassing van public cloud voor een deel van de informatievoorziening (bijvoorbeeld een informatiesysteem) van een departement of een onderdeel hiervan. In termen van het public cloudbeleid betreft het een dienst die voldoet aan de kenmerken van 'materieel public cloudgebruik'. Drie departementen hebben na een oproep in het CIO Beraad vrijwillig een public cloud programma aangemeld (verder aangeduid als 'de diensten') voor dit onderzoek.

Bij twee van de drie onderzochte diensten is een departement rechtstreeks eigenaar en daarmee ook rechtstreeks verantwoordelijk voor de afwegingen op het gebied van de voorwaarden uit het RPCB. Een van de drie aangemelde diensten wordt echter vanuit een aanbodbenadering geleverd door een interne IT-dienstenleverancier van de Rijksoverheid. In dit geval geldt aanvullend dat afstemming dient plaats te vinden tussen de leverancier en een departement als afnemer die gebruik maakt van de dienst, over de gemaakte afwegingen op de elf voorwaarden uit het cloudbeleid. Reden hiervoor is dat een departement als afnemer zelf verantwoordelijk blijft voor de naleving van deze voorwaarden. De wijze van afstemming is op hoofdlijnen in dit onderzoek meegenomen maar de afnemerzijde valt buiten dit onderzoek.

Bij het formuleren van de aanpak voor dit onderzoek is rekening gehouden met andere onderzoeken op het gebied van public cloud die gelijktijdig in de context van de Rijksoverheid worden uitgevoerd:

1. De Algemene Rekenkamer voert een doelmatigheidsonderzoek uit genaamd 'Het Rijk in de Cloud'. Het doel van dit onderzoek is om inzicht te bieden in de risicobeheersing van het cloudgebruik door het Rijk vanuit drie principes: soevereiniteit, continuïteit van dienstverlening en gegevensbescherming. Het eerste deel van dit onderzoek is uitgevoerd in de tweede helft van 2023 en heeft zich in de breedte op de public cloud ontwikkelingen bij de departementen gericht. Een tweede deel van dit onderzoek is in 2024 uitgevoerd en leidt naar verwachting in 2025 tot rapportage.

[1] Kamerbrief d.d. 29-09-22 Kamerbrief Rijksbreed cloudbeleid 2022
[2] Rapport 05-01-23 Implementatiekader risicoafweging cloudgebruik
[3] Handreiking risicobeheersing public clouddiensten

2. In het cloudbeleid is voorzien in een monitoringsrol van CIO Rijk op een aantal aspecten. Deze rol heeft deels een periodiek karakter en is verbonden aan de jaarlijkse cyclus van CIO gesprekken. Bij de start van dit onderzoek was de volledig beheercyclus zoals beschreven in het public cloudbeleid nog niet eenmaal volledig doorlopen.

Teneinde overlap van de werkzaamheden van de verschillende onderzoeken te voorkomen is in overleg met CIO Rijk als opdrachtgever voor dit onderzoek gekozen voor een scherpe afbakening: de identificatie van aandachts- en verbeterpunten in het cloudbeleid aan de hand van de concrete toepassing van dit beleid in drie public cloud trajecten (diensten) binnen de Rijksoverheid staat centraal. Verder wordt benadrukt dat het onderzoek zich heeft gericht op het cloudbeleid: bevindingen in deze rapportage zijn indicatief voor het toepassen van het cloudbeleid in het algemeen en geven geen gerichte informatie over de drie onderzochte diensten individueel.

De gebruikte begrippen in dit onderzoek volgen het RPCB.

1.4 Leeswijzer

In paragraaf 2.1 zijn de drie onderzochte diensten op hoofdlijnen beschreven. De beantwoording van de eerste onderzoeksvraag is opgenomen in paragraaf 2.2 en in paragraaf 2.3 de beantwoording van de tweede onderzoeksvraag. Tot slot wordt in paragraaf 2.4 een korte reflectie gegeven op de doelstelling voor dit onderzoek op basis van de beantwoorde onderzoeksvragen.

In hoofdstuk drie wordt op hoofdlijnen ingegaan op de uitgevoerde werkzaamheden, de gehanteerde standaard voor onderzoek en de beoogde verspreidingskring voor voorliggende rapportage.

Bijlage II bevat een infographic met een overzicht van de bevindingen van de eerste en tweede onderzoeksvraag.

2 Bevindingen

2.1 Beschrijving drie public clouddiensten

Zoals beschreven in paragraaf 1.3 'Afbakening en definities' zijn de volgende drie diensten door departementen vrijwillig aangemeld als basis voor een onderzoek naar het RPCB:

1. De eerste dienst betreft een applicatie ten behoeve van de bedrijfsvoering voor een uitvoerende dienst van een departement. De applicatie wordt geleverd in de vorm van een 'Software as a Service' (SaaS) oplossing ontwikkeld en beheerd door een klein Nederlands bedrijf als specialist op de benodigde functionaliteit. Voor het daadwerkelijk leveren van de betreffende applicatie wordt gebruik gemaakt van het platform dat wordt geboden door een grote Amerikaanse public cloudprovider. De uitvoerende dienst heeft een contract met het Nederlandse bedrijf. Dit bedrijf heeft vervolgens een contract met de public cloudprovider als platform voor het daadwerkelijk leveren van de dienst. Fysiek is de dienst primair geplaatst in een datacenter van de public cloudprovider op Nederlands grondgebied.

2. De tweede dienst betreft werkplekdienstverlening ten behoeve van ambtenaren van een aantal departementen, die op een aanbod gedreven wijze door een grote IT-dienstverlener binnen de Rijksoverheid wordt geleverd. In de huidige productiefase worden Office 365 licenties en MS Teams dienstverlening (functionaliteit zoals videoconferencing en chat) aangeboden op basis van het Microsoft (MS) 365 aanbod. In deze fase wordt nog geen data zoals gebruikersbestanden opgeslagen bij Microsoft maar wel worden gebruikersidentiteiten gedeeld ten behoeve van het technisch functioneren van de dienstverlening. Het betreft een hybride situatie waarbij de dienstverlening primair plaatsvindt middels een datacenter van de Rijksoverheid. Een volgende fase is op het moment in ontwikkeling (en deels in pilot) waarbij ook data zoals gebruikersbestanden wordt opgeslagen in de public cloud bij Microsoft (Onedrive). Voor deze dienst heeft de IT-dienstverlener een contract afgesloten met Microsoft op basis van de raamovereenkomst zoals beschikbaar gesteld door Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS (verder: SLM). Fysiek wordt de dienst primair geplaatst in een datacenter van Microsoft op Nederlands grondgebied.

3. De derde dienst betreft de gedeeltelijke verwerking van e-mail van een departement binnen de Rijksoverheid middels de Exchange Online dienstverlening zoals aangeboden door Microsoft. Dit betreft een vervolg op een eerder traject waarbij onder meer MS 365 inclusief MS Teams is ingevoerd. Het departement treedt hierbij op als opdrachtgever richting een interne IT-dienstverlening binnen de Rijksoverheid die op haar beurt voor haar dienstverlening gebruik maakt van Exchange Online als public clouddienst aangeboden door Microsoft. De ontwikkeling van deze dienst is inmiddels zover dat groepen gebruikers stapsgewijs worden overgezet. Ook voor deze dienst heeft de IT-dienstverlener een contract afgesloten met Microsoft op basis van de raamovereenkomst zoals beschikbaar gesteld door SLM. Ook deze dienst is fysiek primair geplaatst in een datacenter van de public cloudprovider op Nederlands grondgebied.

2.2 Onderzoeksvraag I: Bevindingen operationele toepasbaarheid voorwaarden public cloudbeleid

In de volgende paragrafen is per voorwaarde uit het public cloudbeleid een overzicht van de bevindingen opgenomen.

2.2.1 Opstellen departementaal beleid en strategie public cloud

Bestaande situatie als onderwerp opnemen in rijksbrede public cloudbeleid
Uitgangspunt in het RPCB is dat departementen hun eigen cloudbeleid en -strategie formuleren op basis van de voorwaarden uit het RPCB en onderliggende documenten. De drie onderzochte clouddiensten zijn gebaseerd op cloudbeleid en -strategie of vergelijkbare documentatie die is opgesteld voor het moment van publicatie van RPCB. Overigens is voor één betrokken organisatie zeer recent wel een nieuw cloudbeleid vastgesteld dat is gebaseerd op het RPCB. De onderzochte dienst is echter van eerdere datum en dus niet hierop gebaseerd. Een vaststelling is dat in het RPCB uitgegaan wordt van public cloud als onontgonnen terrein voor de Rijksoverheid. Er zijn geen bepalingen opgenomen over hoe om te gaan met bestaande initiatieven op het gebied van public cloud. Bijvoorbeeld een overgangstermijn ten aanzien van bestaand public cloudbeleid en diensten is niet bepaald. Een risico is dat departementen op verschillende wijze omgaan met het toepassen van het RPCB voor bestaande public cloud initiatieven en dat binnen de Rijksoverheid in vergelijkbare situaties dus verschillend wordt gehandeld.

Aanbeveling
Houd in een volgende versie van het RPCB rekening met de bestaande situatie op het gebied van public cloud en neem bijvoorbeeld expliciet een uiterste datum op voor het compliant zijn met het nieuwe RPCB.

Versterken samenwerking departementen en hergebruik producten
Het RPCB is feitelijk een beleidskader: het beschrijft een aantal voorwaarden waarmee rekening moet worden gehouden bij het opstellen van een departementaal cloudbeleid. Vaststelling is dat op dit moment het cloudbeleid en -strategie voor de drie onderzochte diensten significant van elkaar verschillen in structuur en inhoud. Op zich is dit verklaarbaar aangezien dit beleid zonder gemeenschappelijke basis tot stand is gekomen. Voor het cloudbeleid dat wel mede op basis van het RPCB tot stand is gekomen, geldt dat aanvullende onderwerpen zijn opgenomen die niet standaard in het RPCB zijn benoemd. Mede op basis van dit voorbeeld is de risicoinschatting dat verschillende departementen op basis van het RPCB tot een significant verschillende uitwerking van nieuw public cloudbeleid en -strategie gaan komen op zowel structuur en inhoud. Mogelijk gevolg is dat (niet noodzakelijke) verschillen in structuur en inhoud tussen public cloudbeleid en -strategie van verschillende departementen een eventuele samenwerking van departementen op het gebied van public cloud bemoeilijken en hergebruik van producten zoals bijvoorbeeld risicoanalyses niet faciliteren.

Aanbeveling
Beschrijf in het RPCB als beleidskader de minimale verplichte inhoudsopgave aangevuld met facultatieve onderwerpen en een standaard uitwerking als basis voor het opstellen van een departementaal cloudbeleid en -strategie teneinde samenwerking tussen departementen en hergebruik van producten te faciliteren.

Benoem criteria voor het verplicht opstellen van eigen public cloudbeleid door onderdelen Rijksoverheid
Een verschil tussen het RPCB en het bijbehorende implementatiekader is dat het RPCB voorschrijft dat er op het niveau van een departement beleid wordt opgesteld terwijl het kader spreekt over 'alle onderdelen van de Rijksdienst'. In deze context is relevant dat een van de deelnemers aan het onderzoek een shared service organisatie (SSO) binnen de Rijksoverheid betreft die gebruik maakt van het departementale public cloudbeleid zoals opgesteld voor het kerndepartement als eigenaar van deze SSO. Risico is dat de beleidseisen op het gebied van public cloud voor een kerndepartement en een grote IT-dienstverlener binnen de Rijksoverheid zodanig van elkaar verschillen dat de IT-leverancier middels dit beleid niet effectief worden gefaciliteerd.

Aanbeveling
Benoem in het RPCB criteria voor wanneer een onderdeel van de Rijksoverheid een eigen public cloudbeleid en -strategie moet opstellen. Ga bijvoorbeeld in op de positie van de grote IT-leveranciers binnen de Rijksoverheid.

2.2.2 Risicoafweging

Versterk effectiviteit en efficiëntie van proces van risicoafweging
In het RPCB is opgenomen dat voor het gebruik van een public clouddienst een risicoafweging (inclusief risicoanalyse) moet worden uitgevoerd op het gebied van privacy en informatiebeveiliging. Voor de drie onderzochte clouddiensten is het beeld op hoofdlijnen dat een aanzienlijke inspanning op dit gebied is gepleegd. Uit een beknopte analyse van de uitgevoerde werkzaamheden en uitkomsten komen de volgende punten naar voren:

1. Het proces van de uitvoering van de risicoafweging en de wijze van vastlegging laat grote verschillen tussen de drie onderzochte diensten zien. Dit varieert van de uitbesteding van (onderdelen van) de risicoafweging aan de markt, inzet van een formele risicomanagementmethodiek al dan niet gefaciliteerd door externe medewerkers tot een meer praktische aanpak gebaseerd op de kennis en kunde van direct betrokkenen. Een van de betrokken organisaties ontwikkelt geautomatiseerde ondersteuning voor dit proces wat mogelijkheden biedt voor hergebruik.
2. In alle onderzochte gevallen is het beeld dat het proces van risicoafweging een fors beslag legt op beschikbare kennis en capaciteit. Vraag is hierbij in hoeverre uitvoering van de risicoafweging in de toekomst voldoende schaalbaar is als meer IT-diensten naar de public cloud worden gebracht.
3. Beeld op basis van de inhoud van de risicoafwegingen is dat deze inhoudelijk een forse overlap vertonen en dat uitkomsten vergelijkbaar zijn. Inschatting is dat op het niveau van de Rijksoverheid significant dubbel werk wordt uitgevoerd. Een aantal restrisico's komst consistent naar voren.

Het risico ligt aan de ene kant in de effectiviteit van de afweging: de grote verschillen in het proces zouden kunnen leiden tot verschillende uitkomsten en verschillen in risicoacceptatie. Aan de andere is efficiëntie relevant: het deels dubbel uitvoeren van het proces van risicoafweging door verschillende organisaties binnen de Rijksoverheid dient te worden voorkomen.

Aanbeveling
Onderzoek op welke wijze de effectiviteit en efficiëntie van het proces van risicoafweging voor public cloud diensten op het niveau van de Rijksoverheid kan worden bevorderd en adresseer dit in de volgende versie van het RPCB. Besteed hierbij bijvoorbeeld aandacht aan de mogelijkheden voor samenwerking binnen de Rijksoverheid, de geautomatiseerde ondersteuning die is ontwikkeld en hergebruik binnen de Rijksoverheid beschikbare succesvolle methoden voor bijvoorbeeld risicoanalyse voor public clouddiensten.

Meerdere voorwaarden uit RPCB komen samen in de voorwaarde risicoafweging
In de voorwaarden van het RPCB zijn enkele onderwerpen opgenomen die samenhangen met het uitvoeren van een risicoafweging maar die als losstaand onderwerp zijn benoemd. In aanvulling op het onderwerp risicoafweging betreft het in ieder geval de onderwerpen 'Toegespitste risicoanalyse', 'Cyberveiligheid' en 'Opslag en verwerking persoonsgegevens'. Risico is bijvoorbeeld dat deze onderwerpen onvoldoende in samenhang worden beschouwd.

Aanbeveling
Onderzoek op welke wijze de voorwaarden in het RPCB die raken aan het onderwerp risicoafweging kunnen worden samengevoegd opdat een effectiever en efficiënter risicomanagementproces mogelijk wordt.

2.2.3 Gekend gebruik

Uitgangspunt is dat departementen hun materieel public cloudgebruik en de risico's daarvan rapporteren aan de CIO Rijk. In het RPCB wordt hierbij de relatie gelegd met de verwerking van persoonsgegevens terwijl in het implementatiekader het onderwerp risicoanalyse ook nadrukkelijker naar voren komt. Van belang hierbij is uiteraard de definitie van materieel public cloudgebruik. De drie onderzochte diensten worden daarbij in ieder geval beschouwd als duidelijke voorbeelden aangezien het ondersteuning van bedrijfsprocessen betreft die van wezenlijk belang zijn voor primaire taken van departementen. Tijdens het onderzoek is wel aangegeven dat het begrip materieel public cloudgebruik mogelijk verschillend wordt geïnterpreteerd. Voor breed gebruikte diensten zoals een werkplek op basis van MS 365 zou hier rijksbreed een keuze in kunnen worden gemaakt teneinde ongefundeerde verschillen tussen departementen te voorkomen.

Op het gebied van inzicht in public cloudgebruik en het daadwerkelijk rapporteren hierover is het beeld op hoofdlijnen:

1. Voor zover wij dit hebben kunnen onderzoeken op basis van een deelwaarneming van drie diensten is het beeld dat registratie van materieel public cloudgebruik binnen departementen in ontwikkeling is.
2. In lijn met het voorgaande punt is de rapportage aan CIO Rijk ook in ontwikkeling. In 2023 is nog geen rechtstreekse opgave van cloudgebruik aan CIO Rijk gedaan. Wel is conform de afspraken in het CIO-beraad de informatie die in het kader van een onderzoek naar cloud van de Algemene Rekenkamer is verzameld ter beschikking gesteld aan CIO Rijk.
3. Departementen die wij hebben onderzocht geven aan een (te) hoge administratieve lastendruk op het gebied van verantwoording over IT in het algemeen en specifiek over informatiebeveiliging en privacy te ervaren.

Risico van het (deels) ontbreken van centraal inzicht in het gebruik van public cloud is dat juist op onderwerpen die overzicht op het niveau van de Rijksoverheid als geheel vragen zoals soevereiniteit en marktconcentratie een afweging niet optimaal kan plaatsvinden.

Aanbeveling
Versterk het rapportageproces voor centraal inzicht in informatie over onder meer soevereiniteit en marktconcentratie conform de in het RPCB en achterliggende Implementatiekader benoemde uitgangspunten. Als dit proces functioneert dan kan vervolgens op basis van de verzamelde informatie – naast een inhoudelijke analyse – onderzoek worden gedaan naar aspecten van het rapportageproces zelf:

- wordt bijvoorbeeld de definitie van materieel public cloudgebruik consistent en in lijn met de oorspronkelijk doelstelling gehanteerd over de departementen heen;
- in hoeverre levert de rapportageverplichting op de langere termijn (te) hoge administratieve lasten op, na initiële inrichting van het rapportageproces?

2.2.4 Exit strategie

Benoem continuïteit bedrijfsprocessen expliciet op hoogste niveau cloudbeleid
De focus van het onderwerp exit strategie ligt in het RPCB op de afspraken met de cloudprovider op het gebied van overdracht en vernietiging van data bij contractbeëindiging. In het onderliggende implementatiekader en handreiking risicobeheersing is de exit strategie breder gericht op onder meer de continuïteit van de bedrijfsprocessen die gebruik maken van IT-voorzieningen die gebaseerd zijn op de public cloud. Het risico is dat de gebruiker van het RPCB een te beperkt beeld krijgt van het onderwerp exit strategie en hierdoor dit onderwerp te smal aanpakt.

Aanbeveling
Breng het onderwerp exit strategie in het RPCB in lijn met onder meer het implementatiekader en richt dit expliciet op het borgen van de continuïteit van de door public cloudgebruik ondersteunde bedrijfsprocessen.

Versterk ondersteuning ontwikkeling exit strategie
In de praktijk van de drie onderzochte clouddiensten zijn conform het RPCB bepalingen in de contracten met de respectievelijke leveranciers opgenomen omtrent de teruggave van data aan de Rijksoverheid en vervolgens de vernietiging van data bij de cloudprovider in het geval van een cloudexit. Een volledige uitwerking van een exit strategie gericht op de continuïteit van de ondersteunde bedrijfsprocessen conform alle beschreven onderwerpen uit het implementatiekader en de handreiking is voor geen van de drie onderzochte diensten aangetroffen. Wel zijn gedurende het implementatietraject van betreffende diensten deels de hiermee samenhangende continuïteitsrisico's expliciet beschreven en geaccepteerd. Tijdens interviews bleek dat bij betrokkenen wel informeel is nagedacht over continuïteit van bedrijfsprocessen in het geval van een cloudexit. Voor uitvoering van de besproken strategie zou dan bijvoorbeeld wel een aanzienlijke hoeveelheid hardware moeten worden aangeschaft of delen van het bedrijfsproces zouden handmatig moeten worden uitgevoerd. Hierbij merken wij op dat migratie naar betreffende public clouddiensten recent heeft plaatsgevonden waardoor op dit moment nog ervaring is met on-premises uitvoering van diensten. De vraag is in hoeverre over een aantal jaren deze ervaring nog beschikbaar is, er nog capaciteit aanwezig is in datacenters onder beheer van de Rijksoverheid voor het plaatsen van extra hardware en of het überhaupt mogelijk is om snel hardware te verwerven in het geval er grootschalige problemen zijn met de dienstverlening van een of meer grote public cloudproviders. Het risico is dat de huidige bepalingen in RPCB en onderliggende documenten niet leiden tot een uitwerking van de exit strategie per dienst op het gewenste niveau waardoor bij een cloudexit de continuïteit van ondersteunde bedrijfsprocessen van de Rijksoverheid niet voldoende is geborgd.

Aanbeveling
Onderzoek op welke wijze het onderwerp exit strategie kan worden opgenomen in het RPCB zodanig dat (onderdelen van) departementen in staat zijn dit onderwerp voldoende effectief op te pakken. Ga hierbij ook na welke rijksbrede ondersteuning noodzakelijk is en of het wellicht mogelijk is om op dit onderwerp (deels) centraal binnen de Rijksoverheid samen te werken.

Ontwikkel een good practice voor exit strategie SaaS
Zoals eerder beschreven betreft een van de drie diensten de uitbesteding van een applicatie in de vorm van SaaS. Juridisch is deze dienstverlening zodanig ingericht dat de eigenaar van de dienst (een onderdeel van een departement) een contract heeft met de dienstverlener. Zoals eerder beschreven is dit een Nederlands bedrijf dat gespecialiseerd is in het ontwikkelen en beheren van een applicatie op een specifiek expertisegebied. Deze dienstverlener heeft vervolgens een eigen contract met een van de grote Amerikaanse public cloudproviders. De exitstrategie voor deze dienst richt zich echter volledig op de continuïteit van de Nederlandse dienstverlener (bijvoorbeeld in het geval van een faillissement) en gaat niet in op het exit vraagstuk van de achterliggende public cloudprovider. Het risico van deze constructie is dat een exit strategie op het door RPCB gewenste niveau niet is ingeregeld voor deze public cloudprovider.

Aanbeveling
Ontwikkel een ‘good practice’ voor een exit strategie bij het gebruik van een SaaS oplossing. Besteed hierbij zowel aandacht aan de exit strategie voor de directe leverancier als de achterliggende public cloudprovider en de continuïteit van het bedrijfsproces.

2.2.5 Voldoen aan eisen ICT-dienstverlening

Het RPCB stelt dat voor de public cloud dienst gedocumenteerd dient te worden op welke wijze wordt voldaan aan de bestaande voorwaarden voor ICT-dienstverlening. In de praktijk is voor de drie onderzochte diensten op verschillende wijze invulling gegeven aan deze voorwaarde. Waar voor de ene dienst een lijst van tientallen verwijzingen naar wet- en regelgeving is opgesteld, wordt dit voor een andere dienst beperkt tot de belangrijkste kaders zoals bijvoorbeeld de Baseline Informatiebeveiliging Overheid. In een toelichting wordt verder aangegeven dat betrokkenen deze voorwaarde als onduidelijk ervaren en dat het voor zich spreekt dat elke IT-dienst (public cloud of niet) moet voldoen aan alle relevante wet- en regelgeving. Met name wordt het risico genoemd dat de in de bijlage bij het RPCB gegeven overzicht van relevante wet- en regelgeving wordt beschouwd als limitatief terwijl dit slechts voorbeelden zijn. In de visie van ADR is het vraagstuk voor deze voorwaarde te vergelijken met de problematiek, risico’s en aanbevelingen zoals beschreven voor het proces van risicoafweging, zie aanbevelingen paragraaf 2.2.2.

2.2.6 Toegespitste risicoanalyse

De toegespitste risicoanalyse richt zich op specifieke onderwerpen zoals marktconcentratie en politieke en geografische spreiding van public clouddiensten. Voor dit onderwerp wordt in het algemeen verwezen naar paragraaf 2.1.2 aangezien deze onderwerpen in onze visie deel dienen uit te maken van een brede risicoanalyse. Wel worden aanvullend enkele specifieke bevindingen voor deze onderwerpen benoemd.

Aandacht voor locatie van opslag en verwerking van persoonsgegevens
Inhoudelijk is het beeld dat voor de drie diensten een afweging is gemaakt omtrent de locatie van opslag en verwerking van de betreffende persoonsgegevens. In vervolg hierop is in alle gevallen primair gekozen voor datacenters van grote Amerikaanse public cloudproviders in Nederland. Voor uitwijklocaties wordt gebruik gemaakt van datacenters in de EU. Het onderwerp geografische spreiding van public clouddiensten komt zowel bij deze voorwaarde als bij de voorwaarde 'opslag en verwerking persoonsgegevens' aan de orde. Risico is dat deze voorwaarden onvoldoende in samenhang worden beschouwd.

Aanbeveling
Onderzoek of beide voorwaarden (toegespitste risicoanalyse en opslag en verwerking van persoonsgegevens) kunnen worden samengenomen als onderdeel van de versterking van het proces van risicoweging (zie paragraaf 2.2.2).

Onderzoek het optimale beschouwingsniveau voor strategische risico's
Voor risico's op het gebied van marktconcentratie en soevereiniteit is minder aandacht in de gemaakte risicoafwegingen. Uitzondering zijn de risico's die samenhangen met (Amerikaanse) wet- en regelgeving zoals de Cloud-act al wordt het restrisico dat hiermee samenhangt uiteindelijk wel geaccepteerd voor de onderzochte diensten. Hierbij is onze indruk dat op het niveau van individuele organisaties binnen de Rijksoverheid praktische afwegingen doorslaggevend zijn zoals het kunnen gebruiken van specifieke, alleen nog in de public cloud aangeboden functionaliteit of bijvoorbeeld het mitigeren van het risico van verouderde IT bij een interne IT-dienstverlener van de Rijksoverheid. Het risico is dat op het beschouwingsniveau van individuele organisaties binnen de Rijksoverheid de veronderstelde praktische voordelen van public cloud al snel groter zijn dan de strategische risico's (met kleine kansen maar grote gevolgen) op het gebied van marktconcentratie en soevereiniteit waardoor deze in de meeste gevallen geaccepteerd worden.

Aanbeveling
Onderzoek op welk niveau van de Rijksoverheid de meer strategische risico's op het gebied van marktconcentratie en soevereiniteit voor public cloud optimaal kunnen worden beschouwd en leg dit vast in het RPCB in aanvulling op de informatie die al in de handreiking is opgenomen.

2.2.7 Cyberveiligheid

De voorwaarde cyberveiligheid richt zich op het uitvoeren van een risicobeoordeling op basis van de C2000 criteria. Deze criteria geven richtlijnen om risico's van public cloudgebruik ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere derde partijen af te wegen. Een schriftelijke vastlegging van een beoordeling van deze criteria is voor de drie onderzochte diensten niet aangetroffen. Mondeling is toegelicht dat de inschatting is gemaakt dat toepassing van deze criteria niet nodig is voor de betreffende dienstverlening. Het niet expliciet documenteren van de risicobeoordeling van de C2000 criteria brengt risico's met zich mee zoals bijvoorbeeld:

- het verantwoordelijk management wordt niet in staat gesteld om eventuele restrisico's te accepteren;
- het is niet mogelijk om op een later moment verantwoording af te leggen over gemaakte afwegingen;
- voor dit onderdeel ontbreekt een startpunt voor onderhoud en doorontwikkeling van de dienst.

Aanbeveling
Borg als onderdeel van de uitvoering van de in paragraaf 2.2.2 opgenomen aanbevelingen over het proces van risicoafweging dat de C2000 criteria expliciet worden meegenomen.

2.2.8 Openbaarheid

De voorwaarde openbaarheid richt zich vanuit Wet Open Overheid (WOO) op de openbaarmaking van de besluitvorming over de DPIA en indien van toepassing, adviezen van de Privacy Adviseur Rijk (PAR) binnen drie maanden na ingebruikname van betreffende public cloud dienst. Voor alle drie de diensten geldt dat openbaarmaking niet heeft plaatsgevonden. In gesprek hierover zijn de volgende punten naar voren gekomen:

- Voor twee van de drie onderzochte diensten geldt dat de privacy relevante data die wordt verwerkt als onderdeel van de dienst grotendeels betrekking heeft op rijksambtenaren. Verschillende geïnterviewden geven aan dat het niet duidelijk is in hoeverre de publicatieplicht in dit geval geldt.
- Voor alle drie de diensten beschrijft de DPIA in detail de inrichting van de dienst, eventuele misbruikscenario's en andere informatie die relevant is vanuit cyber security perspectief. Deze informatie zou eventuele kwaadwillende actoren een uitstekende basis voor een cyberaanval bieden. Mede vanuit deze overweging is afgezien van publicatie. Het opstellen van een 'externe' publicatieversie met minder details zou een optie zijn maar dit zou hoge administratieve lasten met zich meebrengen en de informatiewaarde zou beperkt zijn.
- De tekst van de voorwaarde zoals opgenomen in het RPCB wordt niet eenduidig uitgelegd. Er staat dat openbaarmaking de 'besluitvorming' betreft maar gebruikers lezen de voorwaarde alsof onder meer de DPIA's openbaar moeten worden gemaakt.

Samenvattend beeld is dat door de gebruikers van het RPCB voor uitvoering van deze voorwaarde in de huidige vorm aanzienlijke cyber security risico's worden gezien. Ook is de formulering van deze voorwaarde naar inschatting van ADR onvoldoende helder. Risico is echter ook dat onvoldoende invulling wordt gegeven aan de eisen die de WOO stelt.

Aanbeveling
Voer voor deze voorwaarde een aanvullende beleidsanalyse uit waarbij deze voorwaarde wordt herzien op basis van genoemde punten en in overleg met onder meer de gebruikers van het RPCB en WOO en privacy juristen.

2.2.9 Opslag en verwerking van persoonsgegevens

In de visie van ADR is het vraagstuk voor deze voorwaarde te vergelijken met de problematiek, risico's en aanbevelingen zoals beschreven voor toegespitste risicoanalyse onder 'Aandacht voor locatie van opslag en verwerking van persoonsgegevens'. Zie voor aanbevelingen paragraaf 2.2.6.

2.2.10 *Bijzondere persoonsgegevens*

De drie onderzochte diensten zijn niet bedoeld voor de verwerking van bijzondere persoonsgegeven zoals bedoeld in de AVG. Op basis van onderzoek van deze diensten hebben wij dan ook geen bevindingen voor deze voorwaarde. Wel is de tekst van deze voorwaarde in de visie van ADR niet helder: er staat dat indien aan eis 9.c wordt voldaan of in alle andere situaties, de explain die minimaal de uitgevoerde (pre-scan of formele) DPIA bevat zo spoedig mogelijk na vaststelling aan CIO Rijk wordt toegezonden. Het is niet duidelijk of met 'alle andere situaties' naar eis 9.a en 9.b verwezen wordt of naar andere niet nader genoemde situaties. Risico is dat verschillende organisaties dit bepaling op verschillende wijze uitleggen en toepassen.

Aanbeveling
Onderzoek op welke wijze het onderdeel 'alle andere situaties' kan worden verduidelijkt en pas het RPCB hierop aan.

2.2.11 *Basisregistraties*

Ook de voorwaarde 'basisregistraties' is niet relevant voor de drie onderzochte diensten en onderzoek op dit punt leidt dus niet tot bevindingen. Uit een van de interviews komt wel de volgende bevinding naar voren. Het RPCB stelt in voorwaarde 11 onder meer dat ook bronnen van basisregistraties in principe geen gebruik mogen maken van public cloudvoorzieningen. Deze voorwaarde wordt in de praktijk als onduidelijk ervaren: 'Wat is bijvoorbeeld een bron?'. Risico is dat de voorwaarde op het gebied van basisregistraties door departementen op verschillende manieren wordt uitgelegd en toegepast.

Aanbeveling
Onderzoek op welke wijze het onderdeel 'bronnen van basisregistraties' kan worden verduidelijkt en pas het RPCB hierop aan.

2.3 Onderzoeksvraag II: Ervaringen en versterking rijksbrede public cloudbeleid

2.3.1 *Versterk public cloudbeleid op onderwerpen buiten informatiebeveiliging en privacy*

De voorwaarden zoals beschreven in het RPCB hebben met name betrekking op privacy en informatiebeveiliging. Voor wat betreft privacy wordt qua wetgeving met name de naleving van de Algemene Verordening Gegevensbescherming (AVG) ondersteund. Gesignaleerd wordt dat ook buiten de onderwerpen privacy en informatiebeveiliging behoefte is aan strategische richting voor de inzet van public cloud. De volgende aandachtspunten in en mogelijkheden voor versterking van het RPCB zijn benoemd:

1. Een van de drie onderzochte public clouddiensten valt niet onder de AVG maar onder de uitwerking van een EU-richtlijn in nationale (uitvoerings-) regelgeving in combinatie met sectorale regelgeving. Doordat het RPCB zich met name richt op AVG, wordt aangegeven dat het RPCB voor deze organisatie niet optimaal ondersteuning biedt voor de inzet van public cloud.

   Aanbeveling
   Neem in (bijlagen bij) het RPCB ook voor andere relevante wetgeving een uitwerking op.

2. Binnen de Rijksoverheid wordt veelal in ketens samengewerkt met vele partners. Deze complexiteit wordt ook weerspiegeld in de IT-ondersteuning van (delen van) ketens waarbij mogelijk gebruik wordt gemaakt van public clouddiensten. Gesignaleerd wordt dat het RPCB het onderwerp ketens niet benoemd als aandachtspunt voor het departementaal cloudbeleid. Een risico is dat de IT-ondersteuning voor een keten niet uniform en daardoor suboptimaal wordt ingericht, bijvoorbeeld omdat het ene onderdeel van een keten geen gebruik mag maken van public cloud terwijl dit voor een ander deel wel is toegestaan.

Aanbeveling
Neem het onderwerp ketenregie op in het RPCB als aandachtspunt voor departementaal cloudbeleid.

3. De 'sourcing' van IT als het strategisch kiezen van externe dienstverleners (zoals bijvoorbeeld public cloud) om bepaalde IT-functies te realiseren is een belangrijke stap bij het ontwikkelen of herzien van IT-dienstverlening. Een observatie is dat een van de onderzochte organisaties vanuit haar behoefte het onderwerp sourcing heeft toegevoegd aan het ontwikkelde public cloudbeleid gebaseerd op het RPCB. Een risico is dat het RPCB wordt gelezen als 'cloudbeleid' en niet als 'public cloudbeleid' waardoor alternatieven zoals het gebruik van een private cloud onvoldoende worden beschouwd.

Aanbeveling
Neem het onderwerp sourcing als voorwaarde op in het RPCB. In de uitwerking hiervan in departementaal beleid kan vervolgens worden verwezen naar departementaal sourcing beleid waarin staat beschreven op welke wijze bijvoorbeeld per applicatie een rationele afweging kan worden gemaakt tussen inzet van private of public cloud.

2.3.2 Gebruik rijksbrede contracten public cloud en dienstverlening SLM

Aandacht noodzakelijk voor rijksbrede afspraken en voorwaarden cloud bij Saas
Bij het Ministerie van Justitie & Veiligheid is Strategische Leveranciersmanagement Microsoft, Google Cloud en AWS ondergebracht (verder: SLM). SLM is initiatiefnemer van rijksbrede contractafspraken en inkoopvoorwaarden met onder meer de grote Amerikaanse public cloudproviders zoals Microsoft, Amazon Web Services en Google cloud. Rijksoverheidsorganisaties kunnen gebruik maken van deze rijksbrede contractafspraken en inkoopvoorwaarden als basis voor een eigen contract voor het gebruik van public cloud. Deze aanvullende afspraken en voorwaarden bieden een aantal voordelen ten aanzien van een standaard contract, met bijvoorbeeld afspraken die gericht zijn op het mogelijk maken van een AVG-compliant gebruik, een bepaling over het van toepassing zijn van Nederlands recht en een afspraak over een 'right to audit'. Dit betekent dat de Rijksoverheid een onderzoek mag laten uitvoeren bij de betreffende cloudprovider naar bijvoorbeeld de privacy en informatiebeveiligingsaspecten.
Zoals beschreven in paragraaf 2.2.4 sluit een Rijksoverheidsorganisatie in het geval van inzet van een SaaS oplossing veelal een overeenkomst af met een gespecialiseerde derde partij die op haar beurt een contract heeft met een van de grote public cloudproviders als platform voor levering van de dienst. In dit geval zijn de aanvullende afspraken en voorwaarden die gelden voor een rechtstreeks contract tussen een Rijksoverheidsorganisatie en een grote public cloudprovider niet van toepassing. Theoretisch zou dit per SaaS contract kunnen worden geregeld maar in de praktijk is er een aanzienlijke kans dat dit niet haalbaar is, bijvoorbeeld vanwege de geringe schaalgrootte van de derde partij. Het risico is dat als een

Rijksoverheidsorganisatie veel gebruik maakt van SaaS oplossingen via derde partijen, zij uiteindelijk via grote aantallen standaardcontracten (waarin de aanvullende Rijksoverheidsafspraken en voorwaarden niet zijn opgenomen) diensten afneemt van de grote public cloudproviders. Op het moment zegt het RPCB niets over dit vraagstuk.

Aanbeveling
Onderzoek op welke wijze rijksbrede contractafspraken en inkoopvoorwaarden zoals afgesproken door SLM met grote public cloudproviders kunnen worden gebruikt in de context van toepassing van SaaS diensten. Behandel dit onderwerp vervolgens in het RPCB.

Verduidelijk op welke momenten raadpleging van SLM plaatsvindt
In het RPCB en het Implementatiekader wordt op een aantal plaatsen beschreven dat SLM wordt geraadpleegd, bijvoorbeeld bij het uitvoeren van een risicoafweging ten aanzien van het gebruik van public cloud door een departement. Beeld is dat deze mogelijkheid in de praktijk weinig wordt benut. Het risico hiervan is dat er onvoldoende gebruik wordt gemaakt van de kennis en ervaring die bij SLM aanwezig is.

Aanbeveling
Beschrijf in het RPCB duidelijker op welke momenten raadpleging van SLM dient plaats te vinden.

2.3.3 Beschouw algemeen gebruikte IT functionaliteit in de public cloud op niveau RPCB

Met uitzondering van de voorwaarde op het gebied van basisregistraties gaat het RPCB niet in op het gebruik van specifieke public cloudfunctionaliteit. Als belangrijke casus op dit gebied is de werkplek voor de Rijksoverheid genoemd. Vanwege de relevantie wordt deze casus hier (op hoofdlijnen) geschetst.

Sinds eind jaren negentig van de vorige eeuw wordt voor de verschillende werkplekken van de Rijksoverheid veelal gebruik gemaakt van Microsoft software zoals MS Office en MS Windows die vervolgens on-premises bij de Rijksoverheid worden toegepast. Op het moment verkeert de Rijksoverheid in een transitiefase waarbij voor een groot deel stapsgewijs wordt overgegaan naar MS 365, de public cloudoplossing van Microsoft voor de werkplek. Hiermee wordt de on-premises werkplek van de Rijksoverheid verplaatst naar de public cloud. Twee van de drie diensten die wij hebben onderzocht, betreffen voorbeelden van deze transitie. Een relevante vraag die in meerdere interviews naar voren is gekomen, is in hoeverre risico's op het gebied van marktconcentratie en soevereiniteit significant veranderen als gevolg van deze ontwikkeling (zie ook paragraaf 2.2.6). Hierbij zijn meerdere visies naar voren gekomen:

1. In een eerste visie wordt gesteld dat risico's op het gebied van marktconcentratie en soevereiniteit ook in de bestaande situatie bij on-premises gebruik van Microsoft producten al significant aanwezig was: als voor software bijvoorbeeld geen beveiligingsupdates meer worden ontvangen dan worden deze al snel praktisch onbruikbaar. In deze visie verandert de orde van grootte van risico's niet significant bij de overgang van de werkplek naar de public cloud.
2. In de tweede visie wordt gesteld dat bij on-premises gebruik er nog altijd veel meer mogelijkheden zijn voor het treffen van aanvullende beveiligingsmaatregelen en dat bij overgang naar de cloud de risico's wel significant veranderen, zeker als gebruikersdata ook in de public cloud wordt opgeslagen.

Deze verschillen in visies maken in ieder geval zichtbaar dat bij gelijke feiten en omstandigheden voor een vergelijkbaar object andere risicowegingen worden gemaakt binnen de Rijksoverheid. Voor dit soort algemene functionaliteit als de werkplek die ieder departement in principe gebruikt is een risico dat departementen in gelijke omstandigheden andere keuzes maken zowel op het gebied van risicomanagement als op het gebied van fundamentele technische inrichtingskeuzes.

Aanvullend is in enkele interviews de zorg benoemd voor de dreigingsaantrekkende werking van een werkplek op basis van MS 365. Deze komt voort uit het feit dat straks niet alleen (bijna) de volledige Rijksoverheid gebruik maakt van MS 365 maar dat dit ook geldt voor vele buitenlandse overheden en bedrijven wereldwijd. Dit resulteert in een zeer grote verzameling vertrouwelijke data die bijvoorbeeld statelijke actoren een belangrijk motief geeft voor ontwikkeling van aanvalsmogelijkheden op MS 365.

Aanbeveling
Ga in het RPCB in op onder meer belangrijke risico's voor algemene IT functionaliteit uit de public cloud (zoals de werkplek) die (vrijwel) alle departementen inzetten. Ga hierbij ook specifiek in op de dreigingsaantrekkende werking door sterke concentratie van vertrouwelijke data in MS 365. Ook zou kunnen worden onderzocht op welke wijze voor fundamentele technische inrichtingskeuzes best practices kunnen worden gedeeld tussen departementen.

Een aandachtspunt op het gebied van privacy is het aanbieden van video conferencing op de werkplek. Zoals in een van de ontvangen risico- en privacy-analyses wordt aangeven, kan de beeldinformatie uit een videoverbinding strikt genomen worden beschouwd als een bijzonder persoonsgegeven, bijvoorbeeld op het aspect biometrische informatie. Ook voor dit soort vraagstukken is een gezamenlijke risicoweging op het niveau van de Rijksoverheid opportuun in lijn met de voorgaande aanbeveling.

Naast algemene IT-functionaliteit zoals de werkplek waarbij er nog on-premises alternatieven denkbaar zijn, is er ook een tweetal ontwikkelingen die eigenlijk alleen via de public cloud worden aangeboden: kunstmatige intelligentie en (wat verder weg in de tijd) quantum computing. Ook hier is het risico weer dat onderdelen van de Rijksoverheid hier verschillend mee omgaan.

Aanbeveling
Ga in het RPCB ook in op IT-functionaliteit zoals toepassing van kunstmatige intelligentie en quantum computing die uitsluitend via de public cloud wordt aangeboden.

2.3.4 Verantwoording over voorwaarden RPCB bij aanbodsturing interne IT-dienstverlener

Bij een van de drie onderzochte diensten biedt een IT-dienstverlener binnen de Rijksoverheid zelfstandig in dit geval een werkplekdienst aan (MS 365 / MS Teams) aan op basis van een contract met een public cloudprovider (Microsoft). Een departement kan deze dienst vervolgens afnemen. In deze situatie blijft het departement wel verantwoordelijk voor het voldoen aan de voorwaarden uit het RPCB maar is hiervoor deels afhankelijk van de IT-dienstverlener. In de praktijk zijn hiervoor beheersmaatregelen getroffen om departementen te betrekken: met name overleg met betrokken CISO's. In het RPCB wordt op dit governance vraagstuk niet ingegaan. Het risico is dat een departement uiteindelijk de verantwoordelijkheid voor naleving van de voorwaarden uit het RPCB niet in voldoende mate kan dragen.

Aanbeveling
Onderzoek op welke wijze de verantwoording door een interne IT-dienstverlener binnen de Rijksoverheid over de voorwaarden uit het RPCB bij aanbod gedreven IT-diensten op basis van public cloud waar nodig kan worden versterkt en borg dit vervolgens in het RPCB.

2.3.5 Overige bevindingen

De volgende overige bevindingen zijn significant om te melden:

1. Naast het RPCB en onderliggende Implementatiekader en Handreiking is er ook nog de BIO Thema-uitwerking Clouddiensten (maart 2023, versie 2.2) opgesteld door het Centrum informatiebeveiliging en privacybescherming beschikbaar. Vraag is in hoeverre deze kaders onderling consistent zijn. Ook moet de gebruiker van deze kaders zelf vaststellen welke voorwaarden uit de kaders al (deels) worden afgedekt bij het gebruik van standaardcontracten van SLM. Risico is dat de samenhang tussen deze kaders voor de doelgroep binnen de Rijksoverheid onduidelijk is en de kaders hierdoor doelmatig en doeltreffend werken niet bevorderen.

   Aanbeveling
   Draag in elk geval binnen de (Rijks-)overheid zorg voor een consistente en overzichtelijke verzameling kaders op het gebied van cloud. Geef hierbij bijvoorbeeld ook aan welke voorwaarden (deels) al worden afgedekt bij gebruik van standaardcontracten van SLM.

2. In enkele interviews is een trend gesignaleerd dat logging en monitoring voor detectie van informatiebeveiligingsincidenten bij public cloudgebruik steeds belangrijker en complexer wordt. Risico is dat dit leidt tot hogere beheerskosten waardoor bijvoorbeeld de business case voor public cloudgebruik zou kunnen veranderen.

   Aanbeveling
   Onderzoek in welke mate versterking van logging en monitoring bij gebruik van public cloud in de context van de Rijksoverheid noodzakelijk is en welke invloed dit heeft op de kosten van public cloudgebruik.

2.4 Realisatie doelstelling onderzoek en synthese uitkomsten

Met de beantwoording van de onderzoeksvragen in paragraaf 2.2 en 2.3 is invulling gegeven aan de doelstelling van dit onderzoek. Voor het RPCB zijn aandachts- en verbeterpunten geïdentificeerd aan de hand van onderzoek van drie concrete diensten. Ook zijn risico's en aanbevelingen geformuleerd als basis voor versterking van het RPCB.

Tot slot wordt opgemerkt dat de invoering van het RPCB een proces in uitvoering is. Het RPCB is nog maar deels verwerkt in departementaal beleid en de drie onderzochte diensten zijn gebaseerd op beleid en strategie dat dateert van voor het RPCB. Bij de implementatie van deze diensten is op onderdelen al wel gebruik gemaakt van het RPCB. De bevindingen uit dit onderzoek dienen dan ook te worden beschouwd als resultaten ten behoeve van een eerste evaluatie. Aanbeveling is om de evaluatie van het RPCB te herhalen op een moment dat dit volledig is ingevoerd of indien externe ontwikkelingen een eerdere evaluatie noodzakelijk maken.

3 Verantwoording onderzoek

3.1 Werkzaamheden

Het onderzoek is uitgevoerd in de periode januari t/m mei 2024. Voor beantwoording van de onderzoeksvragen is per dienst documentatie opgevraagd met betrekking tot de verschillende voorwaarden uit het RPCB. Ook zijn per dienst de belangrijkste betrokkenen geïnterviewd (circa 5 per dienst) zoals de verantwoordelijke CIO, CISO, CTO, COO en inhoudelijk materiedeskundige en/of andere adviseurs. Ook is een interview gehouden met de plv. Strategisch Leveranciersmanager Microsoft, Google Cloud en AWS Rijk. De ontvangen informatie is voor de eerste onderzoeksvraag verwerkt aan de hand van een referentiekader per dienst. Dit kader is gebaseerd op de elf voorwaarden uit het RPCB. De drie referentiekaders per dienst zijn vervolgens op hoofdlijnen vergeleken en hebben geresulteerd in de bevindingen die in deze rapportage zijn opgenomen.

Aangezien de tweede onderzoeksvraag een verkennend en inventariserend karakter heeft, is hiervoor geen expliciet referentiekader gehanteerd. Deze vraag is met name beantwoord op basis van de inhoud van gehouden interviews op enkele onderdelen aangevuld met observaties van ADR zelf.

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

3.3 Verspreiding rapport

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor CIO Rijk als de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

4 Ondertekening

Den Haag, 3 juli 2024

auditmanager IT

Auditdienst Rijk

Bijlage 1: Infographic

Auditdienst Rijk
Ministerie van Financiën

Resultaten evaluatie public cloudbeleid Rijksoverheid

In 2024 heeft de Auditdienst Rijk een evaluatie uitgevoerd van het Rijksbrede public cloudbeleid. De doelstelling van dit onderzoek was om inzicht te bieden in de operationele toepasbaarheid van de 11 voorwaarden uit het cloudbeleid voor concrete public cloud programma's. Dit betreft programma's (of projecten) gericht op de invoering van public cloud voor een deel van de informatievoorziening van een departement of dienst hiervan. Ook zijn mede aan de hand van praktijkervaringen uit genoemde programma's en eigen observaties van ADR verbeterpunten in beeld gebracht. De uitkomsten van het onderzoek kunnen door opdrachtgever worden gebruikt om het beleid te versterken. Zie voor een toelichting op de hieronder beschreven aanbevelingen de rest van het onderzoeksrapport.

Bevindingen operationele toepasbaarheid voorwaarden public cloudbeleid

Departementaal beleid en strategie public cloud
- Houd rekening met de bestaande situatie op het gebied van public cloud
- Beschrijf de minimale verplichte inhoudsopgave aangevuld met facultatieve onderwerpen en een standaard uitwerking
- Benoem criteria voor wanneer een onderdeel van de Rijksoverheid een eigen beleid en strategie moet opstellen

Risicoafweging
- Onderzoek op welke wijze de effectiviteit en efficiëntie van het proces van risicoafweging op het niveau van de Rijksoverheid kan worden bevorderd
- Onderzoek op welke wijze de voorwaarden die raken aan het onderwerp risicoafweging kunnen worden samengevoegd

Gekend gebruik
- Versterk het rapportageproces voor centraal inzicht conform de benoemde uitgangspunten en onderzoek hierna aspecten van het rapportageproces zelf

Exit strategie
- Breng het onderwerp exit strategie in lijn met het implementatiekader en richt dit expliciet op het borgen van de continuïteit van de ondersteunde bedrijfsprocessen
- Onderzoek op welke wijze het onderwerp kan worden opgenomen zodat (onderdelen van) departementen in staat zijn dit onderwerp voldoende effectief op te pakken
- Ontwikkel een 'good practice' voor een exit strategie bij het gebruik van een SaaS oplossing

Voldoen aan eisen ICT-dienstverlening
- In de visie van ADR is het vraagstuk voor deze voorwaarde te vergelijken met de problematiek, risico's en aanbevelingen zoals beschreven voor het proces van risicoafweging

Toegespitste risicoanalyse
- Onderzoek of toegespitste risicoanalyse en opslag en verwerking van persoonsgegevens kunnen worden samengenomen als onderdeel van de versterking van het proces van risicoweging
- Onderzoek op welk niveau van de Rijksoverheid de meer strategische risico's op het gebied van marktconcentratie en soevereiniteit voor public cloud optimaal kunnen worden beschouwd en leg dit vast.

Cyberveiligheid
- Borg als onderdeel van de uitvoering van de opgenomen aanbevelingen over het proces van risicoafweging dat de C2000 criteria expliciet worden meegenomen

Openbaarheid
- Voer voor deze voorwaarde een aanvullende beleidsanalyse uit waarbij deze voorwaarde wordt herzien op basis van genoemde punten en in overleg met onder meer de gebruikers van het Rijksbrede public cloudbeleid en WOO en privacy juristen

Opslag en verwerking van persoonsgegevens
- Onderzoek of toegespitste risicoanalyse en opslag en verwerking van persoonsgegevens kunnen worden samengenomen als onderdeel van de versterking van het proces van risicoweging

Bijzondere persoonsgegevens
- Onderzoek op welke wijze het onderdeel 'alle andere situaties' kan worden verduidelijkt en pas het Rijksbrede public cloudbeleid hierop aan.

Basisregistraties
- Onderzoek op welke wijze het onderdeel 'bronnen van basisregistraties' kan worden verduidelijkt en pas het Rijksbrede public cloudbeleid hierop aan.

Ervaringen en versterking Rijksbrede public cloudbeleid

Verbreding behandelde onderwerpen
- Neem ook voor andere relevante wetgeving een uitwerking op
- Neem ketenregie op als aandachtspunt voor departementaal cloudbeleid
- Neem het onderwerp sourcing als voorwaarde op

Rijksbrede contracten public cloud en dienstverlening SLM
- Behandel het gebruik van Rijksbrede contractafspraken en inkoopvoorwaarden bij de toepassing van SaaS diensten
- Beschrijf duidelijker op welke momenten raadpleging van SLM dient plaats te vinden.

Algemeen gebruikte IT functionaliteit in de public cloud
- Ga in op belangrijke risico's voor algemene IT functionaliteit uit de public cloud (zoals de werkplek) die (vrijwel) alle departementen inzetten
- Ga in op IT-functionaliteit zoals kunstmatige intelligentie en quantum computing die uitsluitend via de public cloud wordt aangeboden

Verantwoording voorwaarden aanbodsturing interne IT-dienstverlener
- Onderzoek op welke wijze de verantwoording door een interne IT-dienstverlener binnen de Rijksoverheid over de voorwaarden uit het beleid bij aanbod gedreven IT-diensten op basis van public cloud waar nodig kan worden versterkt en borg dit in het Rijksbrede public cloudbeleid

Overig
- Draag zorg voor een consistente en overzichtelijke verzameling kaders op het gebied van cloud
- Onderzoek in welke mate versterking van logging en monitoring bij gebruik van public cloud noodzakelijk is en welke invloed dit heeft op de kosten van public cloudgebruik

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