Het Rijk in de cloud

Donkere wolken pakken samen

2025

Algemene Rekenkamer

Inhoud

Bijlagen | 62

1. Samenvatting

Aanleiding en doel
Het Rijk gebruikt steeds vaker de cloud (hardware, software en gegevens via internet). Dit doet het Rijk om beter te presteren en te functioneren. Cloud kan de dienstverlening van de overheid verbeteren en/of de bedrijfsvoering efficiënter maken. Maar het gebruik van cloud brengt ook risico's met zich mee voor soevereiniteit van de overheid, continuïteit van de overheidsdienstverlening en bescherming van gegevens van burgers en bedrijven. Bijvoorbeeld als gegevens bij de cloudaanbieder opgevraagd worden door andere staten of als een cloudaanbieder failliet gaat of gehackt wordt.

Een goed functionerende en presterende rijksoverheid vereist een verantwoorde inzet van cloud, waarbij de kansen benut worden en de risico's beheerst. Volgens de Algemene Rekenkamer is zicht op het gebruik van cloud hierbij cruciaal. Alleen als bekend is hoe het Rijk cloud gebruikt en wat de kansen en de risico's zijn, kunnen ministers en het parlement sturen op een verantwoorde inzet. Met dit onderzoek draagt de Algemene Rekenkamer hieraan bij.

In 2022 heeft de minister van BZK het Rijksbreed cloudbeleid herzien. Waar het gebruik van *public cloud* (zie kader) eerst niet was toegestaan, is dat binnen het Rijk nu onder voorwaarden mogelijk (BZK, 2022). Deze voorwaarden zijn bijvoorbeeld dat ministeries zicht hebben op hun cloudgebruik en dat zij risicoafwegingen maken. We hebben onderzocht of ministeries zich aan zulke voorwaarden houden.

Er zijn – zoals hierboven benoemd – bij het gebruik van cloud door het Rijk 3 principes belangrijk voor de dienstverlening van de overheid aan burgers en bedrijven: soevereiniteit, continuïteit en gegevensbescherming.

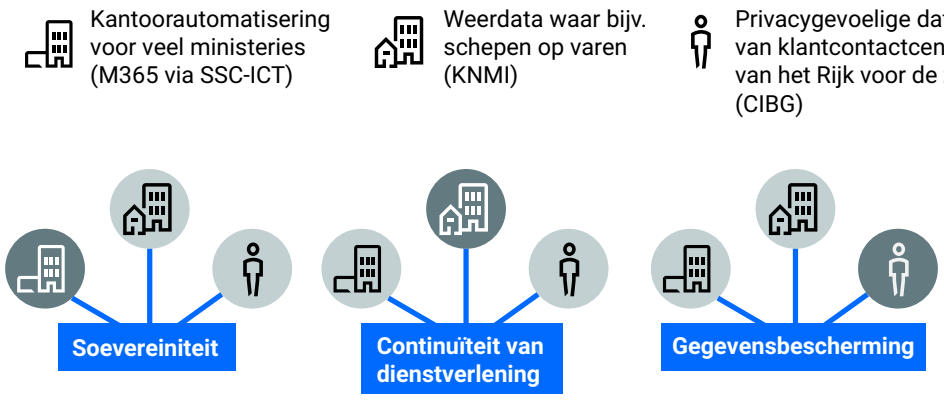
Wij hebben voor 3 public cloud-contracten onderzocht of deze principes voldoende zijn gewaarborgd.

We lichten in het volgende kader eerst het begrip cloud toe, voordat we onze conclusies en aanbevelingen samenvatten.

Wat is de cloud?

Cloudcomputing is het via het internet gebruikmaken van hardware, software en gegevens. De fysieke cloudomgeving (hardware) kan zich overal in de wereld bevinden. Wanneer de middelen in een cloud door één organisatie worden gebruikt, gaat het om private cloud. Een cloud die door meerdere partijen wordt gebruikt is een public cloud. Dit zijn IT-termen, die niet verward moeten worden met de Nederlandse aanduiding van publiek en privaat, bij-voorbeeld voor organisaties. Grote commerciële partijen – zoals Microsoft – bieden juist vaak public cloud aan en 'eigen' overheidsdienstencentra bieden juist vaak private cloud aan. Public cloud wordt bijvoorbeeld gebruikt bij kantoorautomatisering voor ministeries, systemen voor weerdata en systemen voor communicatie met burgers en bedrijven. Het borgen van soevereiniteit, continuïteit en gegevensbescherming is hierbij cruciaal.

Wat betekent cloud concreet voor burgers en bedrijven?



Concusies

In dit onderzoek trekken we de volgende belangrijkste conclusies:

1. Het Rijk heeft beperkt zicht op clouddiensten.
2. Het Rijk maakt onvoldoende strategische risicoafwegingen.
3. Het Rijk waarborgt onvoldoende de principes (digitale) soevereiniteit, continuïteit van de dienstverlening en de gegevensbescherming in 3 onderzochte public cloud-contracten.

Op basis van dit onderzoek concluderen we dat het Rijk ondoordacht cloud is gaan gebruiken en nu onvoldoende grip op heeft op zijn cloudgebruik. We beoordelen het cloudgebruik door het Rijk dan ook als **zorgelijk**. De dienstverlening aan burgers en bedrijven en de continuïteit van het functioneren van de overheid lopen immers te veel risico. De mogelijke schade van verstoorde overheidsdienstverlening kan ons land en onze maatschappij ontwrichten. Daarnaast kan cloudbeleid – en de uitvoering hiervan – niet los worden gezien van een context waarin geopolitieke ontwikkelingen verontrustend zijn.

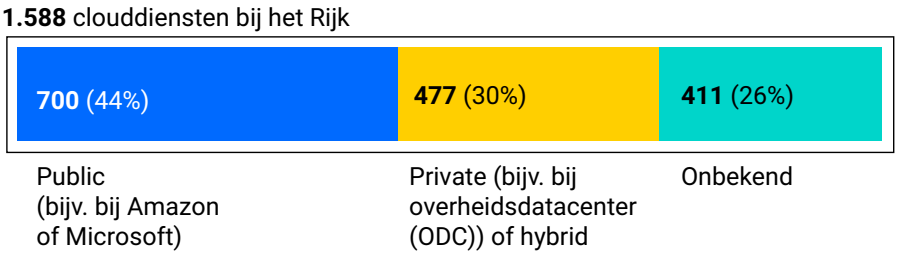
Conclusies deelonderzoek rijksbreed cloudgebruik

Het Rijk maakt volop gebruik van public cloud

Elk ministerie maakt gebruik van public cloud. Bijvoorbeeld bij Microsoft, Amazon en Google. Meer dan de helft van de materieel public cloud-diensten wordt bij deze 3 grote Amerikaanse bedrijven ingekocht.

Van de in totaal 1.588 clouddiensten bij het Rijk zijn 700 (44%) public cloud en 477 (30%) private cloud of hybrid cloud (mengvorm). Van 411 (26%) afgenomen clouddiensten is bij ministeries niet bekend of het om public cloud gaat, zie onderstaande figuur.

Van de door de ministeries gerapporteerde clouddiensten is van een kwart onbekend welke vorm het is



Beperkt zicht op clouddiensten

We concluderen dat ministeries beperkt zicht hebben op hun clouddiensten. Als een ministerie een adequaat overzicht heeft van zijn clouddiensten, kan het sturen op het voldoen aan wet- en regelgeving, het benutten van kansen, het beheersen van risico's en het voldoen aan informatieverplichtingen.

Bij twee derde clouddiensten geen risicoafweging

We concluderen dat ministeries onvoldoende strategische risicoafwegingen hebben gemaakt, voorafgaand aan de beslissing om public cloud te gaan gebruiken. Van de 700 public cloud-diensten zijn er 126 aangeduid als 'materieel' (voor de primaire taak van de organisatie, zoals belastinginning of visumverlening). Bij 84 (67%) van deze diensten is geen risicoafweging gemaakt. Hierdoor blijft bijvoorbeeld het risico bestaan dat gegevens niet goed beschermd zijn of dienstverlening ongewenst kan stoppen. Ook de staatssecretaris Digitalisering kan – via CIO-Rijk – moeilijk (bij) sturen op ministerie-overstijgende cloudrisico's.

Rijksbrede expertise en inkoopkracht onvoldoende gebruikt

We concluderen dat ministeries weinig contact opnemen met de verantwoordelijke partijen voor strategisch leveranciersmanagement (SLM), waardoor ze onvoldoende profiteren van rijksbrede expertise en bijvoorbeeld risicomitigerende maatregelen in SLM-afspraken met cloudleveranciers. Met SLM kan het Rijk zijn macht als grootste IT-afnemer in Nederland beter aanwenden.

Verschillend cloudbeleid

We concluderen dat de cloudstrategie en het cloudbeleid verschillen per ministerie. Door deze versnippering is het voor alle betrokken partijen lastig om eenduidige afspraken te maken, bijvoorbeeld afspraken tussen ministeries, overheidsdatacentra en cloudleveranciers.

Conclusies deelonderzoek 3 belangrijke public cloud-contracten

We hebben 3 materieel public cloud-contracten nader onderzocht. Het gaat om substantiële contracten voor belangrijke overheidsdienstverlening:

- Microsoft 365 bij het Shared Service Centrum-ICT (SSC-ICT);
- systemen bij het Koninklijk Nederlands Meteorologisch Instituut (KNMI);
- het klantcontactcentrumsysteem bij CIBG[1] (Centraal Informatiepunt Beroepen Gezondheidszorg).

Onvoldoende maatregelen voor borgen soevereiniteit, continuïteit en gegevensbescherming

We concluderen dat de betreffende ministeries onvoldoende maatregelen nemen om de soevereiniteit, continuïteit van dienstverlening en gegevensbescherming te waarborgen in public cloud-contracten. Dit betekent dat het Rijk risico's loopt, bijvoorbeeld als een cloudprovider failliet gaat. Het risico bestaat dat het Rijk producten of diensten voor burgers en bedrijven niet kan blijven leveren. Ook bestaat het risico dat gegevens van burgers en bedrijven onvoldoende beschermd zijn en kunnen worden misbruikt door kwaadwillenden en statelijke actoren.

Onvoldoende grip op contractuele afspraken public cloud-diensten
We concluderen dat de betreffende ministeries onvoldoende grip hebben op hun contractuele afspraken voor de public cloud-diensten. Het ontbreekt aan een volledig overzicht van en inzicht in alle contractuele afspraken. Er zijn vaak meerdere partijen bij een public cloud-dienst betrokken, bijvoorbeeld een sharedservice-organisatie (SSO) en onderaannemers. We constateren dat contractuele afspraken ingewikkeld zijn en in meerdere overeenkomsten zijn vastgelegd. Kennis over die afspraken is binnen de ministeries beperkt aanwezig. Dit is problematisch, want juist die contractuele voorwaarden zouden de risico's moeten beheersen.

Aanbevelingen

Onze hoofdaanbeveling aan alle ministers:
Om soevereine, continue en veilige overheidsdienstverlening te borgen is het zaak dat het Rijk richting de grote clouddienstverleners als één samenwerkende overheid kaders stelt, regels hanteert, risico's mitigeert en zijn positie ten opzichte van leveranciers en andere gebruikers van de cloud versterkt. Hiervoor is het nodig dat het Rijk beter zicht heeft op het eigen cloudgebruik en veel gerichter kansen, risico's en alternatieven afweegt voorafgaand aan, maar ook tijdens cloudgebruik.

De bijbehorende deelaanbevelingen zijn als volgt:

Aan de minister van BZK:
1. Maak het Rijksbreed cloudbeleid uniformer en concreter, en houd hier toezicht op:
    - Uniformer: door zo weinig mogelijk verschillen in departementaal beleid toe te staan en bijvoorbeeld ook de 'Handreiking risicobeheersing toepassing public cloud' verplicht te stellen. Onderzoek de mogelijkheid om het Rijksbreed cloudbeleid uit breiden naar decentrale overheden en zelfstandige bestuurs-organen (zbo's).
    - Concreter: door bijvoorbeeld ook nadrukkelijk enkele diensten van de overheid te noemen die onder geen beding naar de public cloud mogen.
2. Richt de handhaving van het Rijksbreed cloudbeleid beter in. Het voldoen aan het Rijksbreed cloudbeleid is nu te vrijblijvend. De staatssecretaris Digitalisering zou – via CIO-Rijk – deze rol steviger moeten pakken, in nauwe samenwerking met de departementale CIO's en verschillende expertises, zoals inkoop.
3. Zie bij alle ministeries toe op het verbeteren van het zicht op gebruikte cloud-diensten en het alsnog maken van risicoafwegingen voor materieel public clouddiensten waarvoor geen risicoafweging is gemaakt.

Aan alle ministers:

1. Het Rijk moet meer sturen op gezamenlijk inkopen, bedingen van voorwaarden en laten uitvoeren van audits. Een centrale partij voor strategisch leveranciers-management (SLM) kan een voortrekkersrol vervullen in het doelmatig afsluiten van cloudcontracten. In EU-verband zijn er kansen voor het Rijk om samen te werken voor standaardisatie, certificering en het afdwingen van AVG-voorwaarden. Overweeg als Rijk realistische EU-alternatieven in combinatie met een uitvoerbare exitstrategie.
2. Weeg voor elke nieuwe mogelijke clouddienst de kansen en risico's af en actualiseer risicoafwegingen van reeds gecontracteerde clouddiensten. De kansen en risico's kunnen namelijk per dienst verschillen. De afweging moet in ieder geval ingaan op de principes soevereiniteit, continuïteit van dienstverlening en gegevensbescherming. En daarnaast op andere aspecten zoals kosten, innovatie-kracht en vereiste kennis en kunde.
3. Verbeter het zicht op gebruikte clouddiensten en maak alsnog risicoafwegingen voor materieel public cloud-diensten waarvoor geen afweging is gemaakt. Neem maatregelen om de risico's te mitigeren. Bijvoorbeeld door extra contractuele voorwaarden af te spreken en te (laten) toetsen of deze worden nagekomen.

2. Over dit onderzoek

Dit hoofdstuk gaat in op de aanleiding en het doel van het onderzoek en de onderzoeksvragen en -activiteiten. We sluiten af met een leeswijzer.

2.1 Waarom dit onderzoek?

Het Rijk zet steeds meer in op cloud om beter te functioneren en te presteren. Cloud kan de dienstverlening van de overheid verbeteren of de bedrijfsvoering efficiënter maken. Maar het gebruik van cloud brengt ook risico's met zich mee voor soevereiniteit, continuïteit van de dienstverlening en bescherming van gegevens van burgers en bedrijven. Een goed functionerende en presterende rijksoverheid vereist een verantwoorde inzet van cloud, waarbij de kansen benut worden en de risico's beheerst. Zicht op het gebruik van cloud is hierbij cruciaal. Het doel van dit onderzoek is om inzicht bieden in het cloudgebruik door het Rijk en te toetsen of het Rijk zich aan de eigen voorwaarden houdt, bijvoorbeeld het maken van risico-afwegingen. Alleen als bekend is hoe het Rijk cloud gebruikt en wat de kansen en de risico's zijn, kunnen ministers en het parlement sturen op een verantwoorde inzet van cloud. Met dit onderzoek draagt de Algemene Rekenkamer hieraan bij.

2.1.1 Cloudontwikkelingen en rijksbreed beleid

Het gebruik van cloud bij het Rijk neemt toe. Cloud biedt mogelijke voordelen, zoals efficiëntie, flexibiliteit, schaalbaarheid en veiligheid. Dit kan de dienstverlening verbeteren of bedrijfsvoering efficiënter maken. Daarnaast duwen IT-ontwikkelingen gebruikers zoals het Rijk richting de cloud. Een bekend voorbeeld is de kantoor-applicatie Microsoft 365. Softwareontwikkelaars en IT-leveranciers investeren niet of minder in 'niet-cloud'-toepassingen. Mede daarom heeft de minister van BZK in

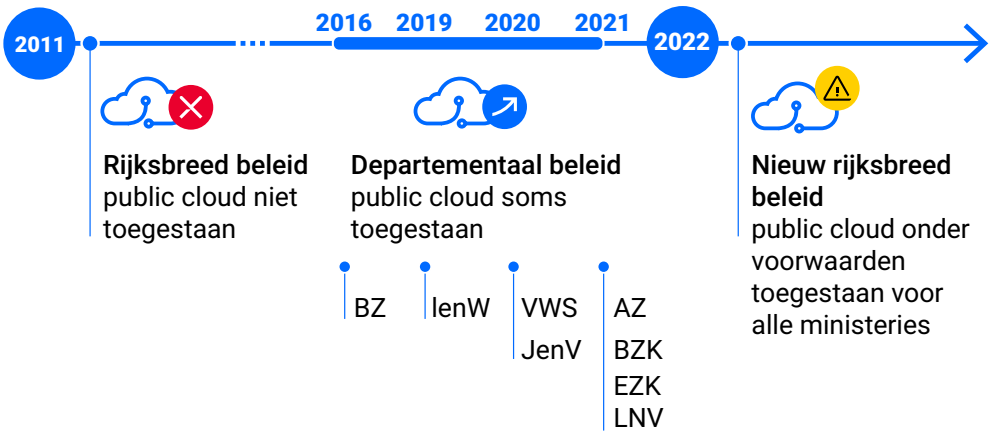
augustus 2022 het cloudbeleid van het Rijk herzien. Onder voorwaarden is het sindsdien ook toegestaan om public cloud te gebruiken, bijvoorbeeld bij Google, Amazon en Microsoft. De voorwaarden zijn onder meer dat ministeries departementaal beleid hebben, dat zij zicht hebben op hun cloudgebruik, dat zij steeds een risicoafweging maken en persoonsgegevens beschermen.

Public cloud-beleid: departementaal versus rijksbreed

Sinds augustus 2022 staat het Rijksbreed beleid het gebruik van public cloud toe. Vóór 2022 had echter al meer dan de helft van de ministeries departementaal cloudbeleid opgesteld, waarin het gebruik van public cloud werd toegestaan.

Figuur 1 *Tijdslijn beleid public cloud-gebruik*

Public cloud mocht eerst rijksbreed niet, vanaf 2022 wel



In ons onderzoek gaven meerdere ministeries als reden aan dat er eerder behoefte was aan de afname van public cloud-diensten en zij daarom zelfstandig beleid hebben opgesteld om dit beheerst mogelijk te maken. Vaak kwam deze behoefte voort uit noodzaak. Aanbieders stellen hun applicaties steeds vaker alleen beschikbaar via public cloud, bijvoorbeeld sommige SAP-applicaties (bedrijfsvoeringssoftware). Daardoor ervoeren de ministeries druk om van public cloud gebruik te gaan maken.

2.1.2 Belangrijke principes en risico's

Er zijn ook risico's bij cloudgebruik. Deze zijn er met name bij cruciale 'principes': soevereiniteit, continuïteit van dienstverlening en gegevensbescherming. Deze omschrijven we als volgt:[2]

- (Digitale) soevereiniteit: het Rijk dient eigenaar te zijn van zijn eigen data, inclusief die van burgers en bedrijven. Controle op dataverwerkende systemen moet uitgevoerd kunnen worden. Het moet inzichtelijk zijn wie toegang heeft tot data en op hoe de data worden gebruikt.
- Continuïteit van dienstverlening: de dienstverlening van het Rijk moet kunnen functioneren zonder (te) afhankelijk te zijn van bepaalde IT-leveranciers. Daarnaast moet er de mogelijkheid zijn voor alternatieven en/of overstappen.
- Gegevensbescherming: het Rijk moet kunnen garanderen dat de vertrouwelijke gegevens van rijksoverheid, burgers en bedrijven voldoende zijn beschermd bij leveranciers.

Bijlage 4 bevat een uitgebreidere, meer volledige definitie van deze principes.

De risico's bij deze principes zijn groot en reëel bij IT-gebruik door de overheid. Denk bijvoorbeeld aan de Chinese hack op Microsoft 365, waarbij 60.000 e-mails van het Amerikaanse ministerie van Buitenlandse Zaken werden gestolen in september 2023.[3] Of in Nederland de contactgegevens van alle 65.000 politiemedewerkers in september 2024.[4] Ook de continuïteit van grote IT-leveranciers is niet zeker. Een recent voorbeeld is een mogelijk faillissement van Atos, een IT-leverancier die een belangrijke rol speelt in diverse vitale overheidsprocessen.[5]

Verder waarschuwt de ADR in zijn evaluatie van het cloudbeleid voor een te grote afhankelijkheid van cloudleveranciers (ADR, 2024). Ook benoemt de ADR de dreigingsaantrekkende werking van Microsoft 365. Bijna de volledige rijksoverheid en veel buitenlandse overheden en bedrijven wereldwijd gebruiken deze werkplek-software. De zeer grote verzameling vertrouwelijke data is voor bijvoorbeeld statelijke actoren een belangrijk motief voor het ontwikkelen van aanvalsmogelijk-heden op Microsoft 365.

Risico's zijn er altijd bij uitbesteding van IT-diensten, maar de omvang van de risico's kan bij cloud anders zijn. Databases met gegevens van burgers en bedrijven staan soms volledig bij een cloudleverancier. Het is cruciaal om zicht te hebben op waar de data geografisch is, wie er precies bij de data kan en of deze nog overgezet kan worden als je naar een andere leverancier wilt. Hoe meer de IT op afstand staat (en dat is bij cloud het geval), hoe groter de risico's.

In dit onderzoek toetsen we heel concreet of er maatregelen zijn genomen om de genoemde principes te waarborgen bij essentiële dienstverlening van de overheid. We doen dat voor kantoorautomatisering voor ministeries, systemen voor weerdata en systemen voor communicatie met burgers en bedrijven.

Figuur 2 *Betekenis cloud voor burgers en bedrijven*

2.1.3 Het doel van ons onderzoek

Het doel van dit onderzoek is om inzicht bieden in het cloudgebruik door het Rijk en te toetsen of het Rijk zich aan de eigen voorwaarden houdt. Ook toetsen we of soevereiniteit, continuïteit en gegevensbescherming geborgd zijn bij het gebruik van public cloud door het Rijk. Voor het parlement is het essentieel om dit te weten. Zo kunnen ministers en het parlement sturen op een verantwoorde inzet van cloud door het Rijk.

Dit onderzoek levert verbeterpunten op voor beleid en uitvoering en biedt handvatten voor een betere risicobeheersing en verantwoorde inzet van cloudgebruik door het Rijk. Zodoende dragen we als Algemene Rekenkamer bij aan het leervermogen en daarmee verbeteren van het functioneren en presteren van de rijksoverheid.

In bijlage 1 zijn de onderzoeksvragen en onderzoeksactiviteiten opgenomen.

2.2 Het Rijksbreed cloudbeleid: actoren en scope

We lichten in deze paragraaf kort de actoren en scope van het Rijksbreed cloudbeleid toe. Dit is relevante informatie voor het kunnen plaatsen van de onderzoeks-bevindingen.

2.2.1 Relevante actoren voor cloudgebruik door het Rijk

De volgende actoren zijn bij het gebruik van clouddiensten door het Rijk belangrijk. Het merendeel van deze actoren wordt ook genoemd in het Rijksbreed cloudbeleid en bijbehorend implementatiekader. In lijn met dit beleid hebben de actoren verantwoordelijkheden. Een beknopte weergave hiervan in samenhang is te vinden in figuur 3. Na de figuur lichten we de actoren nader toe.

Figuur 3 *De taken en verantwoordelijkheden van CIO-Rijk, ministeries en SSO's bij cloud*

CIO-Rijk: directie Chief Information Office-Rijk, onderdeel van Directoraat-generaal Digitalisering en Overheidsorganisatie (DGDOO) van het ministerie van BZK. De directie CIO-Rijk bevordert de optimale vormgeving van de informatisering en ICT in het Rijk. De staatssecretaris Digitalisering en Koninkrijksrelaties (verder in dit rapport staatssecretaris Digitalisering) stelt kaders via CIO-Rijk en ziet daarop toe.

Strategisch leveranciersmanagement (SLM): de afdelingen binnen het Rijk die verantwoordelijk zijn voor strategisch leveranciersmanagement maken rijksbrede contractafspraken en inkoopvoorwaarden voor software en clouddienstverlening.

Deze afspraken landen in mantelovereenkomsten met IT-leveranciers. Ministeries en agentschappen mogen deze mantelovereenkomsten gebruiken, maar zijn hier niet toe verplicht.
Met SLM kan het Rijk zijn macht als grootste IT-afnemer in Nederland beter aanwenden. Er is niet één SLM-organisatie. Zo is bijvoorbeeld de minister van JenV verantwoordelijk voor de afspraken aangaande de clouddiensten van Microsoft, Google Cloud en Amazon Web Services. Voor Oracle is dit de minister van EZ (DICTU) en voor IBM is dit de minister van Financiën (Belastingdienst).[6]

Ministeries: ministeries (en agentschappen) zijn uiteindelijk de opdrachtgever voor uitbestedingen van IT-diensten, zoals cloud.

Sharedserviceorganisaties (SSO's) en overheidsdatacentra (ODC's): SSO's (bijvoorbeeld SSC-ICT en DICTU) en ODC's (bijvoorbeeld ODC-Noord of ODC-Belastingdienst) leveren IT- en clouddienstverlening aan ministeries. Zij bieden eigen (private) clouddienstverlening aan of zijn tussenpartij voor (public) clouddienstverlening van bijvoorbeeld Microsoft.

Clouddienstverlener: clouddiensten worden door veel verschillende partijen aangeboden. Zoals hierboven aangegeven leveren SSO's en ODC's clouddiensten. Het overgrote deel (67%) van clouddiensten wordt aangeboden door 3 grote partijen uit de Verenigde Staten: Amazon (Web Services), Microsoft (Azure) en Google (Cloud Platform).[7] Naast deze partijen zijn er Europese initiatieven, zoals in Duitsland (Delos Cloud) en Frankrijk (Bleu, OVHcloud). Ook in Nederland bieden dienstverleners cloudomgevingen aan. Er zijn meerdere aanbieders aangesloten bij de Dutch Cloud Community, een brancheverenigingvoor Nederlandse aanbieders van clouddiensten. Zo'n aanbieder is bijvoorbeeld Crayon, waar de minister van JenV een clouddienst van afneemt.

2.2.2 Scope van het Rijksbreed cloudbeleid

In het Rijksbreed cloudbeleid is het volgende opgenomen (p. 2):
"*Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit Rijksbeleid te volgen. Aan de departementen wordt gevraagd dit voor de onder hun minister vallende zbo's en eventueel andere organisaties te stimuleren.*"
Decentrale overheden en zbo's vallen dus niet onder dit beleid. Het Rijksbreed cloudbeleid geeft echter wel een beperking voor basisregistraties (in principe geen gebruikmaken van public cloud) die gevuld of beheerd worden door deze partijen.

Ook het ministerie van Defensie valt buiten de scope van dit beleid. Dit ministerie vindt het Rijksbreed cloudbeleid niet voldoende passend voor een veiligheids-organisatie. Wij hebben desalniettemin getoetst of het ministerie van Defensie beschikt over beleid en strategie, overzicht en risicoafwegingen. Een enkele specifieke norm die uit het Rijksbreed cloudbeleid komt (het raadplegen van strategisch leveranciersmanagement) hebben we bij Defensie niet getoetst.

Het Rijksbreed cloudbeleid is 'verplicht' voor de rijksoverheid, net als het Implementatiekader Risicobeheersing cloud (hierna Implementatiekader). In het Implementatiekader wordt melding gemaakt van een facultatieve handreiking (p. 4): "*Naast het cloudbeleid en het implementatiekader is er de (facultatieve) 'Handreiking risicobeheersing toepassing public cloud'. Deze geeft praktische handvatten voor het stapsgewijs beheersen van risico's. Deze wordt in het CIO-beraad vastgesteld en periodiek geactualiseerd.*"

2.3 Leeswijzer

We beginnen in hoofdstuk 3 met een inleiding in cloud, ter introductie op de thematiek en de kansen en risico's van cloud. Dit hoofdstuk is gebaseerd op vakliteratuur en expertinterviews. In de volgende 2 hoofdstukken beschrijven we de resultaten van ons onderzoek naar 'beleid, overzicht en afweging' en 3 specifieke cloudcontracten. We eindigen met conclusies en aanbevelingen. Hierna vindt u de reactie van de verantwoordelijke minister(s) en ons nawoord.

In dit rapport hanteren we de nieuwe naamgeving van de ministers en ministeries per 2 juli 2024. Sommige ministers hebben geen eigen afdeling die verantwoordelijk is voor IT-voorzieningen. Zij maken gebruik van onderdelen van andere ministeries. De minister van Asiel en Migratie (AenM) maakt gebruik van de bedrijfsvoering van het ministerie van Justitie en Veiligheid (JenV). De minister van Volkshuisvesting en Ruimtelijke Ordening (VRO) maakt gebruik van de bedrijfsvoering van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en de ministers van Klimaat en Groene Groei (KGG) en Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN) maken gebruik van de bedrijfsvoering van het ministerie van Economische Zaken (EZ). We hebben bevindingen bij 11 ministeries. Voor de bovengenoemde ministeries zijn meerdere ministers verantwoordelijk.

3. Een inleiding in cloud

We beschrijven in dit hoofdstuk een aantal aspecten van cloudcomputing die helpen om ons onderzoek goed te begrijpen. We beginnen met de ‘cloud push’, beschrijven de soorten cloud en kansen en risico’s. Daarna gaan we in op het begrip soevereiniteit.

3.1 De opmars van cloud: de ‘cloud push’

Cloudcomputing is het via het internet gebruikmaken van hardware, software en gegevens. Het gebruik van de cloud neemt om verschillende redenen toe. IT-ontwikkelingen duwen gebruikers zoals het Rijk richting de cloud. Sommige nieuwe producten, zoals brainstorm- of videovergadersoftware, zijn zelfs alleen maar via de cloud te gebruiken. Daarnaast ontwikkelen IT-leveranciers hun diensten door. Deze diensten worden vanaf een bepaald moment alleen nog maar via de cloud beschikbaar gesteld aan gebruikers(organisaties). Dit geldt bijvoorbeeld voor sommige SAP-applicaties die door ministeries worden gebruikt in de bedrijfsvoering. Een overheidsorganisatie heeft dan eigenlijk maar 2 opties: de dienstverlening niet (meer) gebruiken óf het gebruik van cloud accepteren. Voor alternatieve applicaties in de eigen IT-omgeving zijn soms geen leveranciers meer te vinden en voor het beheer is vaak geen personeel (meer) beschikbaar. Daarmee wordt een organisatie feitelijk gedwongen om gebruik te maken van de cloud.

Alhoewel deze zogenoemde *cloud push* niet moet worden onderschat, komt het ook voor dat soms te gemakkelijk voor de cloud wordt gekozen. De experts die wij hebben gesproken en Instituut Clingendael wijzen erop dat overheidsorganisaties

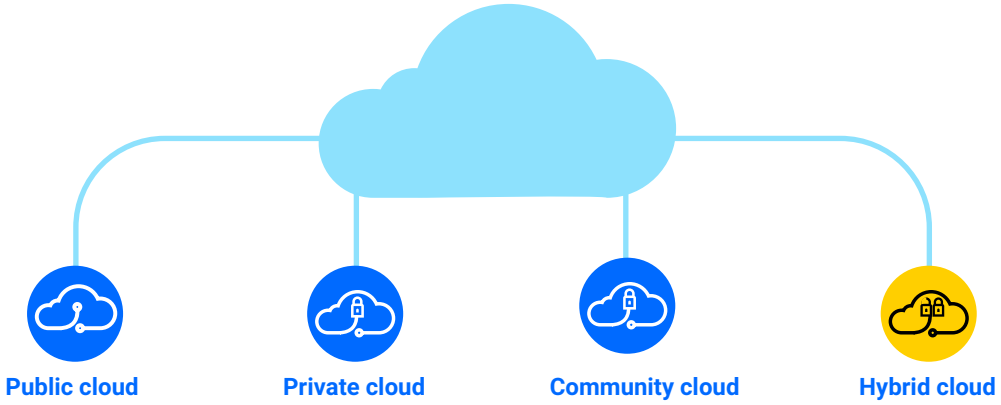
beperkt zoeken naar alternatieven voor clouddiensten (Clingendael, 2024a). Dit kan leiden tot onvoldoende doordacht cloudgebruik.

3.2 Soorten cloud

Bij cloud gebruikt een organisatie de IT-diensten van een cloudaanbieder via het internet en beheert de IT niet zelf. Cloud kent verschillende vormen.

Figuur 4 *Verschillende soort cloud*

Er zijn verschillende soorten cloud



De belangrijkste verschillen zijn:

- **Public cloud**: gebruik door meerdere partijen (in sommige gevallen door iedereen, zowel privé als zakelijk).
- **Private cloud**: exclusief gebruik door één organisatie.
- **Community cloud**: exclusief gebruik door een specifieke gemeenschap.
- **Hybrid cloud**: een mengvorm van de public en private (en/of community) cloud. Bij een hybrid cloud is de IT een samenstelling van 2 of meer IT-omgevingen (private, community of public) die met elkaar verbonden zijn.

Bijlage 4 bevat een uitgebreidere, meer volledige definitie van het begrip cloudcomputing en van de verschillende vormen van cloud. In dit rapport spreken we overigens verder niet over community cloud. Dit komt omdat deze vorm niet wordt genoemd in het Rijksbreed cloudbeleid.[8] Verder is hybrid cloud een mengvorm, deze vorm wordt in dit rapport vrijwel niet benoemd.

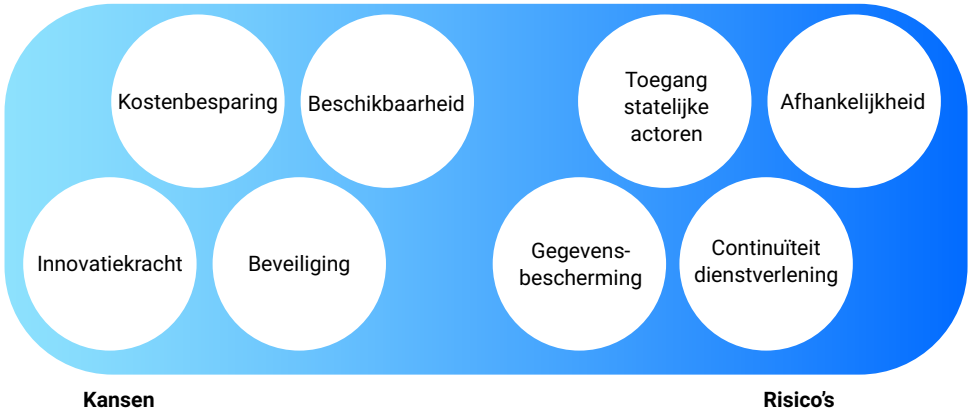
3.3 Kansen en risico's van cloud

Werken in de cloud biedt kansen, ook voor het Rijk. Denk hierbij aan kansen op kostenbesparing en efficiëntie, beschikbaarheid en toegankelijkheid, beveiliging en

privacy en innovatiekracht. Tegelijk bestaan er risico's op het gebied van soevereiniteit, continuïteit van dienstverlening en de bescherming van opgeslagen gegevens van burgers en bedrijven.

Of kansen in de praktijk worden waargemaakt, hangt af van de situatie. Ook kunnen kansen omslaan in risico's wanneer het Rijk de verkeerde afweging maakt. Een voorbeeld hiervan zijn de oplopende licentiekosten. Omgekeerd kan een risico ook een kans zijn: dat opgeslagen data niet op eigen grondgebied staat, kan in geval van oorlog bijdragen aan soevereiniteit. De beschreven kansen en risico's in de volgende paragrafen moeten met die nuance gelezen worden.

Figuur 5 *Beknopt overzicht kansen en risico's van cloud*



3.3.1 Kansen

Kostenbesparing en efficiëntie

Met name public cloud biedt de overheid de kans om digitale diensten sneller en goedkoper te verlenen. Met public cloud kan de overheid bijvoorbeeld eenvoudig en in korte tijd capaciteit opschalen wanneer dit nodig is, zonder dat hiervoor eigen servercapaciteit noodzakelijk is. Wanneer de vraag naar overheidsdiensten afneemt, verlaagt de overheid de af te nemen capaciteit bij de clouddienstverlener. Daarmee heeft de overheid geen kosten voor ongebruikte servercapaciteit. De eigen IT-infrastructuur kan met public cloud klein zijn, waardoor de eigen beheerkosten afnemen. Wel moet de overheid hierbij de abonnements- en/of licentiekosten goed in de gaten houden, alleen functionaliteiten afnemen die ook daadwerkelijk worden gebruikt en letten op prijsstijgingen.

Beschikbaarheid en toegankelijkheid
Een ander voordeel is de betere beschikbaarheid en toegankelijkheid van cloud-dienstverlening. Capaciteit en bandbreedte zijn eenvoudig en in sommige gevallen zelfs automatisch aan te passen, waardoor de kans dat een website of dienst-verlening offline gaat, kleiner is. Daarnaast vergemakkelijkt cloudgebruik samenwerkingsmogelijkheden, bijvoorbeeld interdepartementaal en internationaal.

Beveiliging en privacy
De Algemene Rekenkamer doet al zeker 10 jaar jaarlijks onderzoeken naar de IT-beveiliging en digitale privacy. Daaruit blijken voortdurend allerlei tekortkomingen: in de informatiebeveiliging, het IT-beheer, privacybescherming, enzovoorts. De ministeries zijn afhankelijk van beschikbare expertise binnen de eigen organisatie. Deze risico's doen zich ook bij cloud voor (zie AP 2022 en 2023; CSR 2021; ICTU 2024 en NCSC 2021), maar de experts (van o.a. NCSC en ODC-Noord) die we interviewden wezen erop dat het gebruik van public cloud de beveiliging van de dienstverlening juist kan verbeteren. Grotere technologiebedrijven hebben veel geïnvesteerd in expertise over de beveiliging van de IT. Zij kunnen expertise beter op peil houden vanwege hun schaalgrootte. Goede beveiliging is bovendien cruciaal vanuit commercieel oogpunt: grote cloudaanbieders kunnen het zich niet veroorloven om met bijvoorbeeld een groot datalek in de media te komen. Dit kost omzet.

Zoals hiervoor benoemd kunnen kansen ook omslaan in risico's. In § 2.1.2 noemden we de waarschuwing van de ADR dat de concentratie van informatie bij bijvoorbeeld Microsoft zorgt voor een verhoogde dreiging op inbreuken en daarmee diefstal van gegevens (ADR, 2024).

Innovatiekracht
Cloud biedt ook kans op het stimuleren van innovatiekracht voor organisaties. Veel huidige en toekomstige innovaties, zoals artificiële intelligentie (AI), zijn gebaseerd op cloudtechnologie. Door deze innovaties te gebruiken en kennis daarover te delen, kan de overheid effectiever worden.[9]

Kansen grotendeels gebaseerd op aannames
De hiervoor genoemde kansen zijn grotendeels gebaseerd op aannames. Organisaties zien de kansen als een gegeven of reden om gebruik te maken van public cloud. Ze hebben echter niet beoordeeld of de voordelen in het specifieke scenario en context daadwerkelijk zullen worden gerealiseerd. Het is lastig meetbaar te maken of deze kansen in de praktijk worden waargemaakt. Dit geldt met name voor de voordelen op de langere termijn en binnen een overheidscontext.

De opgedane ervaringen met kostenbesparingen in het bedrijfsleven zijn bijvoorbeeld niet zonder meer van toepassing bij de overheid. De overheid opereert immers in een andere context, met andere eisen en vanuit een andere startpositie. De Nederlandse overheid heeft bijvoorbeeld veel meer ervaring met en expertise over IT in eigen beheer dan met de externe clouddienstverlening.

3.3.2 Risico's

Het gebruik van cloud heeft naast kansen ook risico's voor overheidsorganisaties.

(Digitale) soevereiniteit: afhankelijkheid van leveranciers

Door steeds meer public cloud-diensten te gebruiken kan er een onwenselijk grote afhankelijkheid ontstaan van dominante en monopolistische leveranciers. Dit zijn bovendien meestal leveranciers van buiten de Europse Unie (EU)/Europese Economische Ruimte (EER). Er is sprake van een ongelijke machtsbalans tussen de clouddienstverleners en de overheden als afnemers. Dit komt ook omdat overheidsorganisaties niet altijd over voldoende capaciteit, expertise en professionaliteit beschikken om goed grip te hebben op de cloud en risico's te beperken.

(Digitale) soevereiniteit: toegang statelijke actoren

Cloudleveranciers uit de Verenigde Staten (VS) zijn verplicht om data te verstrekken aan de Amerikaanse overheid. Zie meer over dit risico in § 3.5.

Continuïteit dienstverlening

Anders dan bij veel andere producten die de overheid afneemt, is het bij cloud veel minder het geval dat de overheid kan overstappen naar een andere leverancier. Om een dergelijke 'vendor lock-in' te voorkomen is het van belang dat organisaties borgen dat gegevens uit de cloud van de ene provider ook te gebruiken zijn bij een andere cloudprovider.

Gegevensbescherming

Bij cloud staan gegevens bij de cloudleverancier, meer op afstand dan bij IT in eigen beheer. Zicht op autorisatiebeheer (wie er bij de gegevens kan) is daardoor nog belangrijker. Ongeautoriseerde toegang tot de gegevens kan ertoe leiden dat de gegevens worden gestolen, veranderd of verwijderd. Belangrijk is dat gegevens niet benaderd kunnen worden door andere klanten van de cloudleverancier en dat dit contractueel is vastgelegd. Overigens bestaat ook het risico dat persoonsgegevens onrechtmatig in de cloud staan, omdat niet alle organisaties zich afvragen of gegevens (überhaupt) wel in de cloud mogen staan.

Beperkte kennis en kunde

Cloudafnemers hebben volgens de geïnterviewde experts soms te weinig kennis. En dat geldt ook voor de overheid, die gewend is om taken uit te besteden en daarbij alleen een regierol vervult. Meer outsourcing betekent over het algemeen minder expertise in huis. Deze beperkte kennis kan leiden tot onvoldoende risicoanalyse en -beheersing.

3.4 Het begrip 'soevereiniteit'

Het begrip 'soevereiniteit' is een belangrijk begrip in dit rapport. Het wordt vaak gebruikt wanneer gediscussieerd wordt over cloud (Clingendael, 2024a; CSR, 2021; Moerel & Timmers, 2020).[10] Wanneer we het in dit rapport over soevereiniteit hebben, doelen we op digitale soevereiniteit. Hiervoor gebruiken we de volgende definitie:

Digitale soevereiniteit is het vermogen om autonoom te kunnen beslissen en handelen over de essentiële digitale aspecten in economie, maatschappij en democratie.[11]

Het gaat om het gebruik en inrichting van digitale systemen en de daarmee gegenereerde en opgeslagen data en gerelateerde werkprocessen. In ons normenkader hebben we dit begrip uitgewerkt in concrete normen, onder meer:

- *Datastromen en -locatie*: het is bekend waar de locatie van de data is.
- *Openbaarmaking van gegevens*: er zijn afspraken over de overdracht van gegevens naar landen buiten de Europese Economische Ruimte (EER).
- *Right to audit*: het recht om te auditen kan in de praktijk toegepast worden.
- *Interoperabiliteit*: het systeem kan samenwerken met andere IT-systemen, zodat data geautomatiseerd kan worden uitgewisseld en verder verwerkt.
- *Portabiliteit*: de data is altijd toegankelijk voor de afnemer (dus het Rijk), data kan overgezet worden naar een andere leverancier en er is een realistische exitstrategie. Zo voorkom je dat je (te) afhankelijk wordt van één leverancier.

Soevereiniteit wordt volgens experts vaak als reden gebruikt om aan te geven dat onze data op ons eigen (EU)grondgebied moet staan. En dat we geen gebruik meer moeten maken van cloudleveranciers uit de VS. Er zijn echter ook voorbeelden van landen die juist vanwege soevereiniteit, er bewust voor hebben gekozen om hun overheidsdata in datacentra in andere landen op te slaan, zie onderstaand kader.

Soeverein door de cloud, voorbeelden Estland en Oekraïne

Estland. Sinds 2015 gebruikt Estland de cloud om buiten zijn landsgrenzen staatsinformatie op te slaan. Door de 'data-ambassade' in Luxemburg verzekert Estland dat het - ook bij een fysieke inval op het land - een back-up heeft van kritieke overheidsdiensten en gevoelige staatsinformatie.[12]
Het gebruik van de cloud zorgt ervoor dat Estland als staat kan blijven functioneren, zelfs bij oorlog in het land.

Oekraïne. Net voordat Rusland Oekraïne binnenviel, heeft de regering al haar belangrijkste data gedownload en verplaatst naar de cloud. Tijdens de oorlog is het meermaals voorgekomen dat overheidsdatacentra zijn gebombardeerd of door cyberaanvallen zijn uitgeschakeld. Vanwege de beweging naar de cloud is geen kritieke informatie verloren gegaan. Nu wordt er actief ingezet om back-ups van overheidsdatabases in andere landen te hebben staan.
De publieke dienstverlening aan burgers kan door het gebruik van de cloud-diensten zelfs in oorlogstijd voortgezet worden.[13]

Bij deze voorbeelden merken wij overigens wel op dat de afhankelijkheid is verhoogd van de landen waar de data nu staat. Toch kozen Estland en Oekraïne hiervoor. Te maken keuzes voor meer (digitale) soevereiniteit lijken dus situatie-afhankelijk te zijn.

3.5 VS-wetgeving: toegang tot data

Een belangrijk soevereiniteitsrisico is het risico dat buitenlandse (veiligheids) diensten data opvragen wanneer de clouddienst door een buitenlands technologie-bedrijf wordt geleverd. Zo geeft de CLOUD Act de Amerikaanse overheid vergaande bevoegdheden om toegang te krijgen tot data van Europese burgers. Ook de Chinese overheid heeft wetgeving waarmee het toegang tot data bij bedrijven kan afdwingen. Dit brengt het risico met zich mee dat buitenlandse (geheime) diensten toegang krijgen tot (gevoelige) overheidsdata. Omdat het Rijk met name gebruikmaakt van cloudleveranciers uit de VS leggen we in deze paragraaf uit hoe dit voor de VS zit. De einduitkomst is dat de VS formeel toegang tot de data hebben, ook als de servers in Europa staan.

3.5.1 VS-wetgeving en EU-verdragen

Amerikaanse opsporings- en veiligheidsdiensten mogen op grond van de CLOUD Act gegevens vorderen van Amerikaanse providers van clouddiensten, zoals Microsoft,

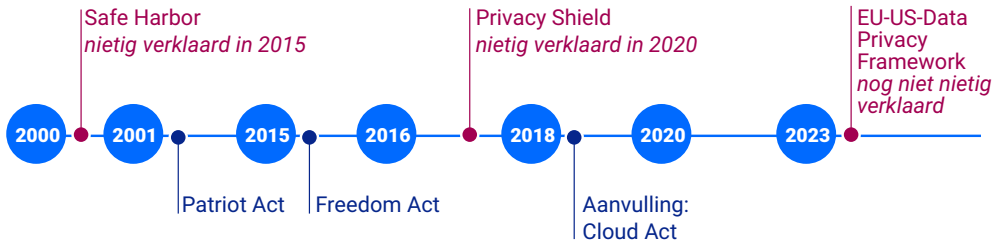
Google en Amazon. Dit geldt ook als die gegevens zijn opgeslagen op buitenlands grondgebied. De EU en de VS stellen steeds overeenkomsten op om dit risico te beheersen, maar het Europese Hof verklaart deze overeenkomsten steeds nietig. Zie ook het volgende kader, waar dit is uitgewerkt. De einduitkomst is dat de VS formeel toegang tot de data hebben, ook als de servers in Europa staan.

De rondedans 'VS-wetgeving – EU-verdragen' voor opvragen data

Over de jaren zijn er veel ontwikkelingen geweest in wet- en regelgeving voor cloud op internationaal vlak. Figuur 6 toont een tijdslijn voor de VS-wetgeving in verhouding tot EU-verdragen die betrekking hebben op cloud.[14]

Figuur 6 *Tijdslijn VS-wetgeving en EU-verdragen over databescherming*

De VS-wetgeving wordt gedempt door EU-verdragen, die nietig worden verklaard



VS-wetgeving

- *2001: de Patriot Act.* Dit was een Amerikaanse wet uit 2001, opgesteld naar aanleiding van de terroristische aanslagen van 11 september 2001. De wet breidt de bevoegdheden voor Amerikaanse autoriteiten uit voor het vorderen en verzamelen van gegevens.
- *2015: de Freedom Act.* In 2015 is de Patriot Act vervangen door de 'USA Freedom Act'. Onder de Freedom Act kunnen Amerikaanse autoriteiten bij Amerikaanse organisaties (die onder de Amerikaanse rechtsmacht vallen) data opvragen. Dit geldt ook voor data die is opgeslagen bij extern gevestigde organisaties die een band hebben met de Amerikaanse organisaties, en de bevoegdheid om daar apparatuur of software te installeren.
- *2018: de CLOUD Act*, een aanvulling op de Freedom Act. Via de CLOUD Act mogen Amerikaanse opsporings- en veiligheidsdiensten gegevens vorderen van Amerikaanse providers van clouddiensten (zoals Microsoft), ook als gegevens in het buitenland zijn opgeslagen. De CLOUD Act verschaft Amerikaanse inlichtingendiensten dus toegang tot Europese persoons-gegevens die verwerkt worden door Amerikaanse partijen.

EU-verdragen

- *2000: Safe Harbor.* In 2000 zijn de internationale Safe Harbor Privacy Principles opgesteld. Hiermee kregen Amerikaanse bedrijven de mogelijkheid om te verklaren dat ze voldeden aan EU-privacyregels. **Safe Harbor werd in 2015 nietig verklaard** door het Europese Gerechtshof vanwege zorgen over Amerikaanse surveillance.
- *2016: Privacy Shield.* Dit verving de Safe Harbor-principes. De bedoeling hiervan was om de rechten van Europeanen te beschermen en om data-uitwisseling tussen de EU en de VS te verbeteren. Het **Privacy Shield werd in 2020 nietig verklaard** door het Europese Gerechtshof, omdat het in strijd was met de AVG.
- *2023: EU-US-Data Privacy Framework*. Een nieuw kader om eerdere juridische bezwaren bij het *Privacy Shield* aan te pakken. Volgens het EU-US Data Privacy Framework moeten bedrijven voldoen aan strengere voorwaarden om te garanderen dat gegevens veilig worden behandeld. De nieuwe regels omvatten maatregelen zoals verbeterde transparantie en strengere controlemechanismen. Volgens Max Schrems (de initiator van de eerdere nietigverklaringen) is er niet veel veranderd ten opzichte van het Privacy Shield.[15]

3.5.2 Het 'toegang-VS'-risico in de praktijk

In opdracht van het Nationaal Cyber Security Centrum (NCSC) heeft een gespecialiseerd internationaal advocatenkantoor onderzocht hoe groot het risico is dat informatie in Europa wordt opgevraagd door de Amerikaanse overheid op basis van de CLOUD Act (NCSC, 2022). Aan 3 grote aanbieders van clouddiensten (Microsoft, IBM en Amazon) is gevraagd hoe vaak er gegevens van Europese inwoners zijn opgevraagd en verstrekt aan de Amerikaanse overheid. Volgens dit onderzoek zijn deze 3 aanbieders gezamenlijk groot genoeg om hier algemene conclusies aan te verbinden.

Volgens experts (CSR; NCSC) worden deze gegevens in de praktijk nauwelijks opgevraagd. Amazon heeft dergelijke verzoeken nooit ontvangen en IBM heeft er één ontvangen en verworpen. Microsoft heeft 12 verzoeken over gebruikers buiten Amerika gehonoreerd. Het is echter niet duidelijk of en in hoeveel gevallen dit Europeanen betrof. Het NCSC meldt op basis van dit onderzoek dat het risico dat de Amerikaanse overheid toegang krijgt tot Europese (persoons)gegevens, specifiek op basis van de CLOUD-act, weliswaar voorstelbaar, maar in de praktijk (heel) klein is.

Europese wetten zoals de AVG en afspraken tussen de VS en EU, zoals het EU-US Data Privacy Framework, bieden enige bescherming. Ook kunnen bedrijven juridische en technische maatregelen nemen om toegang tot data te bemoeilijken, bijvoorbeeld via encryptie.

Daarnaast zijn er andere routes voor bijvoorbeeld de National Security Agency (NSA) van de VS. Zij kunnen bijvoorbeeld direct contact leggen met de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Uit onze audits op Microsoft- en Amazon-clouddienstverlening blijkt niet dat 'persoonsgegevens openbaar gemaakt zijn door opvraging van wethandhavings-autoriteiten'. Het kan overigens ook zo zijn dat hier onvoldoende zicht op is bij de afnemende partijen. Zie hiervoor § 5.3.

3.5.3 Relevante EU-ontwikkelingen

Het komende Europese Cyberbeveiligingscertificeringssysteem voor clouddiensten (EUCS) zal verschillende controleniveaus (evaluatieniveaus) bieden die de lidstaten zullen helpen bij het nemen van beslissingen over cloud.[16] Welke aanbieder is er voor welke soort cloud en voor welke specifieke dienst? Er zal hierbij een trapsgewijze certificering komen met het oog op een bepaalde overheidsdienst en de bijbehorende gevoeligheid van gegevens.
De EU kan inzetten op het afdwingen van General Data Protection Regulation (GDPR) voorwaarden. Hier zouden EU-cloudleveranciers makkelijker aan kunnen voldoen, omdat zij bijvoorbeeld niet onder de Amerikaanse CLOUD Act vallen.

4. Toetsing uitvoering cloudbeleid

In dit hoofdstuk bespreken we de resultaten van ons deelonderzoek naar het rijksbreed handelen conform het Rijksbreed cloudbeleid en Implementatiekader cloud.[17] We toetsen of de aspecten departementaal cloudbeleid en -strategie, cloudoverzicht en risicoafweging voldoen aan de norm.

4.1 Conclusies

Het Rijk maakt volop gebruik van public cloud
Elk ministerie maakt gebruik van public cloud. Bijvoorbeeld bij Microsoft, Amazon en Google. Meer dan de helft van de materieel public cloud-diensten wordt bij deze 3 grote Amerikaanse bedrijven ingekocht.
Van de in totaal 1.588 clouddiensten bij het Rijk zijn 700 (44%) public cloud en 477 (30%) private cloud of hybrid cloud (mengvorm). Van 411 (26%) afgenomen cloud-diensten is bij ministeries niet bekend of het om public cloud gaat.

Beperkt zicht op clouddiensten
We concluderen dat ministeries beperkt zicht hebben op hun clouddiensten. Als een ministerie een adequaat overzicht heeft van zijn clouddiensten, kan het sturen op het voldoen aan wet- en regelgeving, het benutten van kansen, het beheersen van risico's en het voldoen aan informatieverplichtingen.

Bij twee derde clouddiensten geen risicoafweging
We concluderen dat ministeries onvoldoende strategische risicoafwegingen hebben gemaakt, voorafgaand aan de beslissing om public cloud te gaan gebruiken.

Van de 700 public cloud-diensten zijn er 126 aangeduid als ‘materieel’ (voor de primaire taak van de organisatie, zoals belastinginning of visumverlening). Bij 84 (67%) van deze diensten is geen risicoafweging gemaakt. Hierdoor blijft bijvoorbeeld het risico bestaan dat gegevens niet goed beschermd zijn of dienstverlening ongewenst kan stoppen. Ook de staatssecretaris Digitalisering kan – via CIO-Rijk – moeilijk (bij)sturen op ministerie-overstijgende cloudrisico’s.

Rijksbrede expertise en inkoopkracht onvoldoende gebruikt
We concluderen dat ministeries weinig contact opnemen met de verantwoordelijke partijen voor strategisch leveranciersmanagement (SLM), waardoor ze onvoldoende profiteren van rijksbrede expertise en bijvoorbeeld risicomitigerende maatregelen in SLM-afspraken met cloudleveranciers. Met SLM kan het Rijk zijn macht als grootste IT-afnemer in Nederland beter aanwenden.

Verschillend cloudbeleid
We concluderen dat cloudstrategie en cloudbeleid verschillen per ministerie. Door deze versnippering is het voor alle betrokken partijen lastig om eenduidige afspraken te maken, bijvoorbeeld afspraken tussen ministeries, overheidsdatacentra en cloudleveranciers.

4.2 Overzichten van cloudgebruik

In deze paragraaf bespreken we de resultaten van de door de departementen aangeleverde cloudoverzichten. Het Rijksbreed cloudbeleid schrijft voor dat ministeries zicht houden op hun clouddiensten. We hebben bij alle ministeries om een overzicht van cloudgebruik gevraagd, om te kunnen toetsen in hoeverre ministeries hier zicht op hebben. Dit overzicht is belangrijk voor het voldoen aan wet- en regelgeving, het benutten van kansen, het beheersen van risico’s en het voldoen aan informatieverplichtingen.

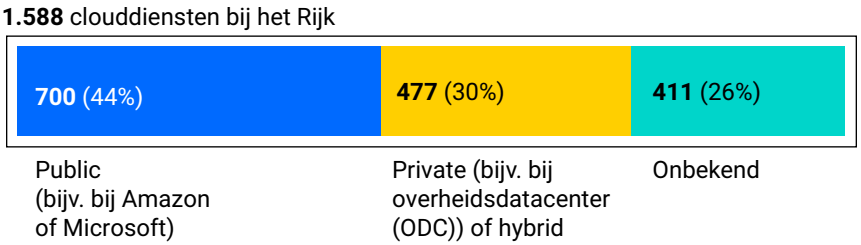
4.2.1 Rijkstotalen

We vroegen bij ministeries een overzicht van clouddiensten op. In Figuur 7 zijn de aantallen op rijksniveau weergegeven. Er zijn in totaal 1.588 clouddiensten opgegeven door de ministeries:

- bij 700 clouddiensten (44%) gaat het om public cloud;
- bij 477 diensten (30%) gaat het om private cloud of hybrid cloud (mengvorm);
- bij een aanzienlijk aantal van 411 clouddiensten (26%) is geen zicht op het type cloud.

Figuur 7 *Totaal aan opgegeven clouddiensten door het Rijk onderverdeeld naar soort*

Van de door de ministeries gerapporteerde clouddiensten is van een kwart onbekend welke vorm het is



4.2.2 Zicht op materieel public cloud per ministerie

Het Rijksbreed cloudbeleid geldt alleen voor materieel public cloud-gebruik. Van de 700 public cloud-diensten zijn er 126 aangeduid als 'materieel public cloud'. De ministeries hanteren verschillende definities van dit begrip. Het Rijksbreed cloudbeleid definieert materieel public cloud-gebruik als "*het gebruik van publieke clouddiensten ten behoeve van het uitvoeren van de primaire taak van de organisatie*". De clouddienst is voor de organisatie dan van wezenlijk belang.

Sommige ministeries hebben deze definitie overgenomen, andere hebben de definitie op verschillende manieren aangevuld, zoals:

- Wanneer de data die verwerkt wordt in de clouddienst gevoelig is, essentieel is, en niet eenvoudig vervangbaar is.
- Wanneer de clouddienst een significant deel van de gegevens in de bedrijfsvoering verwerkt.
- Wanneer de clouddienst digitale infrastructuur en panden beheert en monitort.
- Wanneer de clouddienst te beschermen belangen beveiligt.
- Wanneer de clouddienst noodzakelijk is voor essentiële secundaire processen.
- Wanneer de gevolgen voor burgers ernstig zijn indien de cloudapplicatie meerdere dagen niet beschikbaar is.
- Wanneer het ernstig is als gegevens in handen van derden vallen.

Het hanteren van verschillende definities door de ministeries betekent dat zij verschillend omgaan met materieel public cloud-diensten. Dat begint al met het bijhouden ervan, maar geldt ook, en dat is veel belangrijker, voor de beheersing van de bijbehorende risico's. Zoals eerder vermeld geldt het Rijksbreed cloudbeleid alleen voor materieel public cloud. De voorwaarden uit dit cloudbeleid (bijvoorbeeld op het gebied van risicoafweging en gegevensbescherming) zijn dus niet van toepassing als applicaties niet zijn geclassificeerd als materieel public cloud. Ook ontstaan verschillen in de rapportage van de ministeries aan CIO-Rijk.

Zo kan een onvolledig of vertekend beeld ontstaan van gerapporteerde risico's of een vertekend beeld, omdat sommige risico's onderbelicht blijven.

Vanwege de verschillende interpretaties van materieel public cloud-gebruik hebben we bij de ministeries een compleet overzicht opgevraagd: public, hybrid en private cloud, en zowel materieel als niet-materieel gebruik.[18] Dit om inzicht te krijgen in het totale gebruik van cloud door de ministeries. Op basis van het aangeleverde overzicht hebben we getoetst of het ministerie zicht heeft op materieel public cloud. In tabel 1 is van de clouddiensten op het aangeleverde overzicht opgenomen of voldoende bekend is of deze wel of niet materieel zijn én of deze public, private of hybrid zijn.

Zoals in § 2.3 benoemd, maken verschillende ministers gebruik van de bedrijfsvoering van andere ministeries. De minister van AenM maakt gebruik van de bedrijfsvoering van het ministerie van JenV. De minister van VRO maakt gebruik van de bedrijfsvoering van het ministerie van BZK en de ministers van KGG en LVVN maken gebruik van de bedrijfsvoering van het ministerie van EZ. We hebben bevindingen bij 11 ministeries. Voor de bovengenoemde ministeries zijn meerdere ministers verantwoordelijk. Dit geldt voor alle tabellen in dit hoofdstuk.

Tabel 1 *Zicht op materieel public cloud per ministerie*

	AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
Zicht op materieel public cloud	✓	✓	✓	✓	✗	✗	~	✓	✗	~	~

Voldoet aan de norm:
✓ ja ~ deels ✗ nee

Een aantal ministeries verbeterde het zicht op cloud in een half jaar

Het Rijksbreed cloudbeleid dateert van september 2022. Ministeries hebben tijd nodig om het beleid te implementeren. Als Algemene Rekenkamer hielden we daar rekening mee. We hebben voor alle ministeries de situatie in het najaar 2023 onderzocht. De bevindingen zijn met de ministeries besproken. Medio 2024 hebben we de situatie opnieuw onderzocht en was dit zicht bij een aantal ministeries verbeterd, onder meer bij de ministeries van BZ, BZK, Defensie en JenV.

4.2.3 Zicht op kenmerken materieel public cloud per ministerie

Het Rijksbreed cloudbeleid schrijft voor dat ministeries voor materieel public cloud-diensten tenminste de volgende kenmerken bijhouden:

- Organisatieonderdeel
- Bedrijfsproces
- Leverancier
- Risicoafweging gemaakt

We hebben in het aangeleverde overzicht door het ministerie bij de materieel public cloud-diensten getoetst of deze kenmerken bekend zijn. De uitkomsten zijn weergegeven in tabel 2.

Tabel 2 *Zicht op kenmerken van materieel public cloud per ministerie*

Voor de materieel public cloud-diensten zijn de kenmerken *organisatieonderdeel, bedrijfsproces, leverancier* en *risicoafweging gemaakt* ingevuld in het overzicht.

AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
✓	✓	✓	✓	~	✓	✓	~	~	✓	~

Voldoet aan de norm:
✓ ja ~ deels ✗ nee

Daar waar de clouddiensten als ‘materieel public’ zijn aangeduid, is bij 7 van de 11 ministeries bekend welk organisatieonderdeel, welk bedrijfsproces en welke leverancier het betreft en of er wel of geen risicoafweging is gemaakt. Dit is op basis van de zelfrapportage van de ministeries. Uit de aangeleverde overzichten blijkt onder andere dat meer dan de helft van de materieel public cloud-diensten bij 3 grote Amerikaanse bedrijven (Microsoft, Amazon en Google) wordt ingekocht. We hebben de informatie in de aangeleverde overzichten van de ministeries niet gecontroleerd voor organisatieonderdeel, bedrijfsproces en leverancier. Voor het kenmerk ‘risicoafweging gemaakt’ hebben we dit wel gedaan, zie hiervoor de volgende paragraaf.

Aanvullend op de 4 getoetste kenmerken, vroegen we er nog enkele uit, zoals geografische locatie en ingangs- en einddatum van de contracten. We constateren dat in de aangeleverde cloudoverzichten contractuele informatie over clouddiensten, zoals de ingangs- en einddatum van het contract, in veel gevallen niet is opgegeven. Daarnaast is niet van alle clouddiensten bekend wie de cloudprovider is. Ook is er niet altijd zicht op welke gegevens in de clouddienst worden opgenomen. Tot slot valt ook op dat bij veel clouddiensten de geografische locatie van de clouddienst

ontbreekt. Deze kenmerken zijn niet verplicht zijn volgens het Rijksbreed cloudbeleid, maar zijn wel van belang voor ministeries om grip te houden op cloud.

Ministeries hebben dus beperkt zicht op welke data bij welke partij en in welke geografische gebieden wordt opgeslagen en verwerkt. Dit is extra risicovol als data wordt verwerkt in landen waar statelijke actoren belangstelling hebben voor gegevens en wetgeving dit ook toelaat. Het veilig gebruik kunnen maken van cloud vraagt ook om inzicht in de leveranciersketen en hun veiligheidsoplossingen.[19]
We behandelen deze aspecten meer in de diepte in hoofdstuk 5 bij de toetsing van 3 materieel public cloud-contracten.

Goed voorbeeld departementaal overzicht: het ministerie van BZK

In 2022, voordat het onderzoek van de Algemene Rekenkamer van start ging, was het ministerie van BZK al proactief bezig met een cloudregister. Het door BZK aan ons aangeleverde cloudoverzicht volgt op een eerdere interne inventarisatie. Het cloudoverzicht bevat 156 clouddiensten, waarvan er 12 zijn gelabeld als materieel public cloud. Voor elke materieel public cloud-dienst zijn het organisatieonderdeel dat gebruikmaakt van de clouddienst, het bedrijfsproces en de leverancier van de clouddienst bekend. Verder zijn vrijwel alle overige kenmerken, zoals contractdatums en geografische locatie, bekend. De minister van BZK en de minister van VRO hebben dus een goed overzicht van de clouddiensten waar zij verantwoordelijk voor zijn.

4.3 Risicoafwegingen

4.3.1 Methodiek en gemaakte risicoafwegingen

In deze paragraaf bespreken we onze onderzoeksresultaten over risicoafwegingen bij materieel public cloud-gebruik. Als een overheidsorganisatie bijvoorbeeld een nieuw systeem voor het klantcontactcentrum nodig heeft, kan ze kiezen uit een systeem in eigen beheer of in de cloud. De kansen en risico's (zie onder meer § 3.3) van beide opties moeten dan afgewogen worden.
Het Rijksbreed cloudbeleid stelt dat een methodiek aanwezig moet zijn om risico's af te wegen. Wij vinden ook belangrijk dat dit gestructureerd gebeurt. Dus toetsten we of er een methodiek aanwezig en vastgesteld is op de ministeries.[20] Vervolgens hebben we getoetst of deze methodiek is toegepast bij materieel public cloud-contracten. Als de risicoafweging niet volgens de methodiek is gedaan, vinden we dat er op een andere manier een risicoafweging moet zijn gemaakt. In tabel 3 staan onze bevindingen of dit per ministerie het geval is geweest.

Tabel 3 *Risicoafwegingen materieel public cloud per ministerie*

	AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
Methodiek aanwezig	✓	✓	~	✓	✓	✓	✗	✓	✓	✓	✓
Methodiek vastgesteld	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓
Risicoafweging gemaakt (via methodiek of op andere manier)	~	~	~	~	~	~	~	~	~	✓	~

Voldoet aan de norm:
✓ ja ~ deels ✗ nee

Bij vrijwel alle ministeries zien we dat voor de materieel public cloud-contracten maar deels risicoafwegingen zijn gemaakt voorafgaand aan het gebruik van de clouddienst. Rijksbreed is er voor 42 van de 126 materieel public cloud-contracten documentatie voor risicoafwegingen aangeleverd. Van twee derde van de materieel public cloud-contracten is er dus geen risicoafweging. Alleen het ministerie van SZW heeft voor alle materieel public cloud-contracten risicoafwegingen gemaakt. De minister van SZW heeft dus voor alle materieel public cloud-contracten, zoals verwacht mag worden, een risico-afweging gemaakt.

Risicoafwegingen na een half jaar maar mondjesmaat verbeterd

Zoals eerder in dit hoofdstuk beschreven, bekeken we de situatie bij ministeries in het najaar 2023 en medio 2024. We kregen in dat halve jaar maar weinig extra risicoafwegingen. Qua methodiek zien we wel meer vooruitgang. Bij veel ministeries is deze nu aanwezig en vastgesteld. Als de methodiek wordt toegepast, worden risico's rondom cloud beter afgewogen.

Doordat ministeries deels risicoafwegingen maken, zijn risico's maar beperkt in beeld. Als risico's niet in beeld zijn, kunnen er geen mitigerende maatregelen genomen worden, waardoor het risico blijft bestaan. Bijvoorbeeld gegevens die niet goed beschermd zijn of dienstverlening die ongewenst kan stoppen. Op rijksniveau zijn risico's zo ook beperkt in beeld. Hierdoor kan de staatssecretaris Digitalisering – via CIO-Rijk – moeilijk (bij)sturen op risico's voor materieel public cloud-diensten, die ministerie-overstijgend zouden kunnen optreden.

4.3.2 Raadplegen strategisch leveranciersmanagement

In het Rijksbreed cloudbeleid staat dat SLM (strategisch leveranciersmanagement) geraadpleegd moet worden voor "hergebruik van eerdere analyses en waar mogelijk een gezamenlijke aanpak". Oftewel: de risicoafwegingen en andere analyses die SLM reeds heeft gemaakt kunnen ministeries zo hergebruiken. En als bekend is dat een

ministerie een bepaalde clouddienst wil gaan gebruiken, zou dit gezamenlijk aangepakt kunnen worden.

Tabel 4 *Raadplegen strategisch leveranciersmanagement (SLM)*

	AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
Strategisch leveranciersmanagement geraadpleegd	✗	✗	✗	●	✗	✗	~	✗	~	✗	✗

Voldoet aan de norm:
✓ ja ~ deels ✗ nee ● niet van toepassing

Slechts 2 ministeries lieten bij de opgegeven materieel public cloud-diensten zien dat SLM is geraadpleegd en dan ook nog eens bij slechts een deel van de opgegeven materieel public cloud-contracten. De andere ministeries hebben bij geen enkel contract SLM expliciet geraadpleegd.

Navraag bij SLM hierover leerde ons dat ministeries ook zonder expliciete raadpleging gebruikmaken van bijvoorbeeld mantelovereenkomsten die SLM sluit met onder andere Microsoft. Overigens maken niet álle ministeries of hun agentschappen gebruik van deze mantelovereenkomsten. Mogelijk heeft dat te maken met een situatie dat het uiteindelijke contract met een public cloud-aanbieder afgesloten is door een tussenpartij, waar het ministerie een contract mee heeft. Ook kan het zijn dat het contract al was afgesloten voordat er een mantelovereenkomst beschikbaar was. Het niet gebruikmaken van mantelovereenkomsten kan leiden tot duurdere dienstverlening en het niet voldoen aan rijksbreed gemaakte afspraken.

4.3.3 Kosten-batenafweging

Aanvullend op het Rijksbreed cloudbeleid, vinden we dat bij de afweging om wel of niet de public cloud te gebruiken ook de kosten en baten moeten worden betrokken. Zoals in § 3.3.1 benoemd, kán cloud kostenbesparend werken. Het Rijk moet de financiële aspecten en verschillende kostenstructuren (aankoop/licenties) bij cloudgebruik goed afwegen, voor zowel de korte als de lange termijn. Onvoldoende financieel inzicht kan leiden tot onvoldoende financiële dekking in de toekomst. Dit is een risico voor de continuïteit van overheidsdienstverlening.

Tabel 5 *Afweging kosten en baten*

	AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
Kosten en baten afgewogen	~	✗	✗	~	✗	✗	✗	✗	✗	✗	✗

Voldoet aan de norm:
✓ ja ~ deels ✗ nee

Het afwegen van kosten en baten vinden we bij vrijwel geen enkel ministerie terug. Uit tabel 5 blijkt dat alleen AZ en Defensie gedeeltelijk financiële aspecten meewegen bij materieel public cloud-contracten.

4.4 Beleid en strategie

In het implementatiekader van het Rijksbreed cloudbeleid is het volgende opgenomen: *"Alle onderdelen van de Rijksdienst formuleren hun eigen departementale cloudbeleid en -strategie binnen de kaders van het Rijksbreed cloudbeleid en dit Implementatiekader"*. Zonder beleid en strategie op de ministeries worden voor cloud ad-hocbeslissingen genomen, die mogelijk niet in lijn zijn met het Rijksbreed cloudbeleid en Implementatiekader. Verder moet het Rijksbreed beleid worden toegespitst op de uitvoeringspraktijk bij de ministeries en agentschappen. We toetsten of strategie en beleid aanwezig zijn of deze zijn vastgesteld, en of het Rijksbreed cloudbeleid is verwerkt. Onze bevindingen zijn opgenomen in tabel 6.

Tabel 6 *Departementaal beleid en strategie*

Departementaal beleid en strategie	AZ	BZ	BZK	DEF	EZ	FIN	IenW	JenV	OCW	SZW	VWS
Aanwezig	✓	✓	✓	✓	~	✓	~	✓	~	✓	✓
Vastgesteld	✓	✓	✓	✓	✓	~	✓	✓	✓	✓	✓
Rijksbreed cloudbeleid verwerkt in vastgestelde strategie en/of beleid	✓	✗	✗	●	✗	~	✓	✓	✓	✓	✓

Voldoet aan de norm:
✓ ja ~ deels ✗ nee ● niet van toepassing

8 van de 11 ministeries beschikken over cloudbeleid en -strategie. Bij 3 van de 11 is er óf beleid óf strategie, maar niet beide. De meeste ministeries stellen dit vervolgens ook vast. Bij Financiën is het beleid wel vastgesteld, maar de strategie niet (de conceptstrategie is van medio 2024).

Het Rijksbreed cloudbeleid is niet bij alle ministeries verwerkt in het departementale beleid of de strategie. Bij 6 van de 11 ministeries is dit wel het geval. Een reden die wordt genoemd voor het niet verwerken van het Rijksbreed cloudbeleid, is dat het departementale cloudbeleid al was vastgesteld voorafgaand aan het Rijksbreed cloudbeleid. Dit is bijvoorbeeld het geval bij het ministerie van BZK. Wij hebben niet getoetst of het cloudbeleid van de verschillende departementen ook inhoudelijk voldoet aan het Rijksbreed cloudbeleid.

Goed voorbeeld departementale cloudstrategie: de minister van Defensie

De inhoud van de cloudstrategie van de minister van Defensie is een goed voorbeeld. Deze strategie gaat onder andere in op de noodzaak, kansen en risico's, cloudambitie, strategische keuzes en afwegingscriteria, kaders, actielijnen en relevante ontwikkelingen binnen het Rijk. De strategie beschrijft dat de traditionele keuze voor afgeschermde IT in eigen datacentra niet meer passend is bij de huidige (markt)ontwikkelingen op het gebied van IT.
Om optimaal gebruik te kunnen maken van innovaties, werkt het ministerie geleidelijk toe naar een hybride IT-landschap: een IT-omgeving waarin ruimte is voor zowel private als public cloud. Daarnaast benadrukt het ministerie dat een beweging naar de cloud noodzakelijk is om Defensietaken te kunnen blijven ondersteunen. Hierin spelen ook geopolitieke ontwikkelingen een rol. Moderne technologie en conventionele slagkracht zijn nauw met elkaar verbonden in een militair conflict. De ontwikkelingen op gebied van cloud gaan snel. Om die ontwikkelingen binnen het ministerie te kunnen reguleren, heeft de minister van Defensie in de afgelopen jaren diverse beleidsdocumenten en een afwegingskader opgesteld.

Gedurende het onderzoek zijn bij verschillende ministeries positieve ontwikkelingen geweest op het gebied van cloudstrategie en -beleid. Zo had het ministerie van SZW in het najaar 2023 geen cloudbeleid of -strategie. Medio 2024 is er strategie en beleid vastgesteld waarin het rijksbrede beleid is verwerkt. Ook het ministerie van JenV heeft inmiddels een nieuwe cloudstrategie vastgesteld.

We constateren dat cloudstrategie en cloudbeleid verschillen per ministerie. Denk alleen al aan het in § 4.2.2 beschreven begrip 'materialiteit'. Door de verschillen is het voor alle betrokken partijen lastig om eenduidige afspraken te maken, bijvoorbeeld afspraken tussen ministeries, overheidsdatacentra en cloudleveranciers. Mogelijk geldt dit ook voor basisregistraties, waarbij het Rijk samenwerkt met decentrale overheden.

4.5 Rol staatssecretaris Digitalisering

CIO-Rijk monitort namens de staatssecretaris Digitalisering het gebruik van het Rijksbreed cloudbeleid en rapporteert hierover aan de Tweede Kamer. Dit gaat over het algemeen goed. De staatssecretaris Digitalisering kan – via CIO-Rijk – beter sturen op de informatieaanlevering door ministeries. De informatie die door ministeries aan CIO-Rijk wordt verstrekt is zeer verschillend van omvang en detail. Hierdoor is deze informatie beperkt bruikbaar om een volledig beeld te krijgen van het gebruik van het Rijksbreed cloudbeleid door de ministeries. Uit ons onderzoek blijkt dat de staatssecretaris Digitalisering – via CIO-Rijk – andere ministeries niet aanspreekt op volledige beantwoording van vragen over hun cloudbeleid en -gebruik in relatie tot het Rijksbreed cloudbeleid.

De staatssecretaris Digitalisering heeft de Auditdienst Rijk gevraagd een cloud-onderzoek uit te voeren (ADR, 2024). Het onderzoek geeft invulling aan het monitoren van het toepassen van het Rijksbreed cloudbeleid. De ADR deed onderzoek naar 3 public cloud-diensten die worden ingezet binnen het Rijk die vrijwillig door ministeries in overleg met CIO Rijk zijn aangemeld voor dit onderzoek. Samenvattend beeld is dat de invoering van het Rijksbreed cloudbeleid een proces in uitvoering is.

De staatssecretaris Digitalisering geeft periodiek updates inzake het Rijksbreed cloudbeleid aan de Tweede Kamer (BZK 2023d, 2024a en 2024b). Bij deze brieven wordt ook een overzicht gegeven van de stand van zaken van moties over cloud. Ook hebben ambtenaren van CIO-Rijk enkele technische briefings gegeven aan de Tweede Kamer.[21] Een recente Kamerbrief van de staatssecretaris Digitalisering gaat expliciet in op de evaluatie van het Rijksbreed cloudbeleid (BZK, 2024c). De genoemde onderwerpen bij de ‘hoofdlijnen van de inzichten’ sluiten aan bij onze bevindingen en conclusies.

5. Toetsing waarborgen principes in contracten

We hebben 3 belangrijke public cloud-contracten getoetst. In dit hoofdstuk staan onze conclusies en bevindingen over deze toetsing. We verwachten dat de betreffende ministers de contractuele afspraken begrijpen en grip hebben op soevereiniteit, continuïteit van dienstverlening en gegevensbescherming. We hebben de ministeries gevraagd om aan te tonen dat deze 3 principes zijn gewaarborgd door contractuele afspraken. Ook hebben we de ministeries gevraagd om aan te tonen dat de afspraken met de cloudleverancier in de praktijk worden nageleefd. Hiermee geven wij een beeld van hoe contracten op het gebied van public cloud door ministeries worden vormgegeven en nageleefd door de cloudaanbieders. Deze bevindingen zijn niet te generaliseren naar de gehele rijksoverheid, maar geven wel een indicatie van hoe soevereiniteit, continuïteit van dienstverlening en gegevens-bescherming zijn geborgd.

5.1 Conclusies

We hebben 3 materieel public cloud-contracten nader onderzocht. Het gaat om substantiële contracten voor belangrijke overheidsdienstverlening:

- Microsoft 365 bij het Shared Service Centrum-ICT (SSC-ICT);
- systemen bij het Koninklijk Nederlands Meteorologisch Instituut (KNMI);
- het klantcontactcentrumsysteem bij CIBG[22].

Onvoldoende maatregelen voor borgen soevereiniteit, continuïteit en gegevensbescherming

We concluderen dat de betreffende ministeries onvoldoende maatregelen nemen om de soevereiniteit, continuïteit van dienstverlening en gegevensbescherming te

waarborgen in public cloud-contracten. Dit betekent dat het Rijk risico's loopt, bijvoorbeeld als een cloudprovider failliet gaat. Het risico bestaat dat het Rijk producten of diensten voor burgers en bedrijven niet kan blijven leveren. Ook bestaat het risico dat gegevens van burgers en bedrijven onvoldoende beschermd zijn en kunnen worden misbruikt door kwaadwillenden en statelijke actoren.

Onvoldoende grip op contractuele afspraken public cloud-diensten

We concluderen dat de betreffende ministeries onvoldoende grip hebben op hun contractuele afspraken voor de public cloud-diensten. Het ontbreekt aan een volledig overzicht van en inzicht in alle contractuele afspraken. Er zijn vaak meerdere partijen bij een public cloud-dienst betrokken, bijvoorbeeld een sharedservice-organisatie (SSO) en onderaannemers. We constateren dat contractuele afspraken ingewikkeld zijn en in meerdere overeenkomsten zijn vastgelegd. Kennis over die afspraken is binnen de ministeries beperkt aanwezig. Dit is problematisch, want juist die contractuele voorwaarden zouden de risico's moeten beheersen.

Dit brengt de volgende risico's met zich mee voor de 3 principes soevereiniteit, continuïteit van dienstverlening en gegevensbescherming:

Soevereiniteit

Doordat het ministerie taken en verantwoordelijkheden heeft uitbesteed aan een derde partij (de cloudprovider) bestaat het risico dat het ministerie te weinig invloed heeft op keuzes en controle over:

- de inrichting en het gebruik van werkprocessen die gebruikmaken van eigen data;
- wie toegang heeft tot eigen data;
- hoe eigen data wordt gebruikt door de cloudprovider.

Dit betekent dat het ministerie mogelijk niet kan voldoen aan geldende Nederlandse of Europese wet- en regelgeving, zoals de AVG.

Eerder genoemd voorbeeld (in § 2.1.2) hierbij is de hack op e-mails van het ministerie van Buitenlandse Zaken van de VS. Via het apparaat van een Microsoft-ingenieur konden Chinese hackers binnendringen.[23]

Continuïteit van dienstverlening

Doordat het ministerie een grote afhankelijkheid heeft van een derde partij (de cloudprovider) bestaat het risico dat het – zonder plan B – geen producten of diensten kan blijven leveren op vooraf vastgestelde niveaus en de dienstverlening van het ministerie aan burgers en bedrijven in gevaar komt.

Een eerder genoemd voorbeeld hierbij is de bedreiging van het voortbestaan van Atos, een IT-leverancier die een belangrijke rol speelt in diverse vitale overheidsprocessen.[24]

Gegevensbescherming
Doordat het ministerie gegevens in de cloud laat opslaan, verwerken en transporteren, bestaat het risico dat gegevens van burgers en bedrijven onvoldoende zijn beschermd en zijn te misbruiken door kwaadwillenden.
Eerder genoemde voorbeelden hierbij zijn de buitgemaakte contactgegevens van alle politiemedewerkers in Nederland en e-mails van het Amerikaanse ministerie van Buitenlandse Zaken.[25]

Na een nadere beschrijving van de contracten die we hebben onderzocht geven we in de volgende paragrafen onze bevindingen per principe weer.

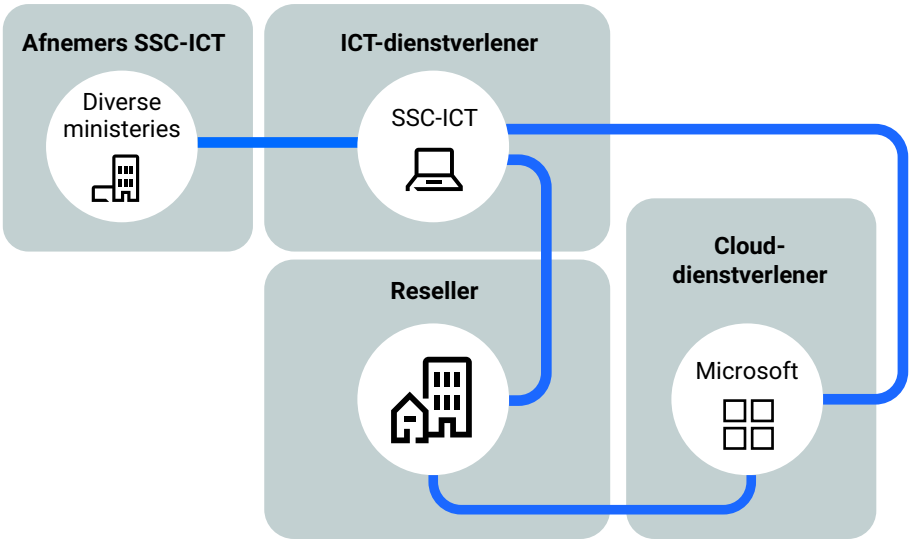
5.2 De contracten en leverancierskeketen

5.2.1 De leverancierskeketen

Vanuit de overzichten die ministeries hebben aangeleverd (zoals beschreven in § 4.2) hebben we 3 belangrijke materieel public cloud-contracten gekozen voor nader onderzoek.[26] We hebben die contracten gekozen die dienstverlening van de overheid richting burgers en bedrijven raakt. Omdat de leverancierskeketen een belangrijke factor is in de gekozen 3 contractaudits gaan we hier eerst wat dieper op in. IT-landschappen zijn vaak complex. Het is vrijwel nooit zo simpel dat één ministerie een contract afsluit met een cloudaanbieder. Vaak wordt een cloudcontract gezamenlijk met andere ministeries gesloten via een sharedserviceorganisatie (SSO). En die SSO sluit het contract vaak niet rechtstreeks af met de clouddienst-verlener, maar bij een zogenaamde ‘reseller’. Figuur 8 brengt de leverancierskeketen voor Microsoft 365 in beeld. Ministeries sluiten niet zelf een contract met Microsoft, maar nemen deze dienst af via de producten- en dienstencatalogus van SSC-ICT. Een reseller is door Microsoft gemachtigd om Microsoft-licenties te verkopen.

Figuur 8 *Een cloudleveranciersketen in beeld*

De leveranciersketen is complex



5.2.2 Contract SSC-ICT voor M365

Bij het ministerie van BZK heeft SSC-ICT de dienst 'Ontwikkeling M365 Cloud Omgeving (Microsoft)' gecontracteerd. SSC-ICT heeft op basis van het afgesloten contract een Rijkswerkomgeving/digitale werkomgeving voor zijn afnemers ingericht. Met ingang van 1 mei 2024 is dit contract van toepassing voor SSC-ICT zelf en alle afnemers van de Rijkswerkomgeving van SSC-ICT (ongeveer 40 in getal). SSC-ICT heeft een contract afgesloten met zowel Microsoft als een reseller. Zie ook Figuur 8.

De dienstverlening van SSC-ICT: SSC-ICT omschrijft zichzelf op zijn website als volgt: "*Wij zijn SSC-ICT, één van de grootste ICT-dienstverleners van en voor de Rijksoverheid. Met onze ICT-diensten zorgen wij ervoor dat ruim 57.000 rijkscollega's van 7 ministeries hun werk in dienst van de samenleving altijd, overal en veilig kunnen uitvoeren.*"[27]

Over Microsoft 365: Microsoft 365 is een verzameling van internetdiensten. Het is te vergelijken met het kantoorpakket Microsoft Office (onder meer tekstverwerking, spreadsheets, e-mailprogramma). In plaats van deze software op computers van of bij een organisatie te installeren, maakt Microsoft 365 gebruik van servers die door Microsoft worden geïnstalleerd en beheerd. Hierdoor draait Microsoft 365 als online dienst op ieder platform dat internet ondersteunt. Een public cloud-dienst dus.

5.2.3 Contract CIBG voor KLOPT

Bij het ministerie van VWS heeft het CIBG[28] (Centraal Informatiepunt Beroepen Gezondheidszorg) de dienst KLOPT gecontracteerd. Dit is het systeem voor het klantcontactcentrum van CIBG. De dienst verloopt via een hoofdaannemer en onderaannemer en wordt geleverd door cloudprovider Amazon Web Services (AWS).

De dienstverlening van CIBG: Het CIBG is een agentschap van het ministerie van VWS. Op de website geeft het als greep uit de taken en werkzaamheden:[29]

- *Wij registreren BIG (Beroepen in de Individuele Gezondheidszorg)-zorgverleners, keuzes van mensen over orgaandonatie, mensen met een diploma Sociale Hygiëne.*
- *Wij publiceren de jaarverantwoording (jaarverslag) van zorginstellingen.*
- *Wij toetsen topinkomens in de zorg en nieuwe zorgaanbieders.*
- *Wij stellen maximumprijzen van geneesmiddelen vast.*
- *Wij (laten) medicinale cannabis produceren.*
- *Wij erkennen weefselbanken en bloedbanken en buitenlandse diploma's voor beroepen in de zorgsector.*
- *Wij verstrekken toegangspassen aan zorgverleners voor inzage in digitale patiëntgegevens en beveiligd e-mailberichtenverkeer, vergunningen voor geneesmiddelen, vergunningen voor donortestlaboratoria, en opiumontheffingen.*

Over KLOPT: CIBG maakt gebruik van de applicatie KLOPT (Klant Optimaal) voor het klantcontactcentrum (KCC). Het KCC is het centrale klantenloket van het CIBG. Hier beantwoordt het CIBG de vragen van zijn klanten (burgers, professionals en organisaties). De klantvragen komen via diverse kanalen binnen en worden via diverse kanalen beantwoord (zoals telefoon, mail, balie, brief). Het KCC ontvangt klantvragen, meldingen en klachten over diverse producten zoals het Donorregister en CIBG-dienstverlening in het algemeen. Vervolgens legt het KCC de gegevens in KLOPT vast en handelt ze af, waar nodig met ondersteuning door de backoffice-medewerkers en Juridische Zaken. CIBG heeft een contract afgesloten met een hoofdaannemer die samen met een onderaannemer zorgt voor de levering van telefonie en de KCC-applicatie op het cloudplatform van AWS.

5.2.4 Contract KNMI voor kerncloudplatform AWS

Bij het ministerie van IenW gebruikt het Koninklijk Nederlands Meteorologisch Instituut (KNMI) de dienst '**Amazon AWS Cloud**' als kerncloudplatform. Het contract loopt via de lidmaatschapscoöperatie van SURF (zie kader hierna voor meer uitleg over SURF).

De dienstverlening van KNMI: Op de website van het KNMI staat het volgende omschreven: "*Het KNMI zorgt voor betrouwbare en consequente metingen, data en prognoses die aan de basis staan van belangrijke besluiten die Nederland veilig houden. Van een code rood voor het wegverkeer tot de klimaatscenario's voor het Deltaprogramma waar miljarden euro's mee zijn gemoeid. Voor een veilig Nederland dat voorbereid is op de invloed van weer, klimaat en aardbevingen.*"

Over Amazon AWS Cloud: KNMI beschrijft dit platform in de aangeleverde informatie als "*hét kerncloudplatform met vele operationele applicaties, van waarnemingen tot diensten voor de buitenwereld*".

Goed voorbeeld van samenwerking: KNMI en SURF

SURF is een afkorting van Samenwerkende Universitaire RekenFaciliteiten. Onder die naam werd de organisatie opgericht in 1986. Het is een vereniging van Nederlandse onderwijs- en onderzoeksinstellingen op het gebied van ICT. Leden van SURF hebben de mogelijkheid om te kiezen of ze clouddiensten willen gebruiken, hoe, en via welke dienstverlener dat gebeurt.
In onze contractaudit hebben we de keten van clouddienstverlening geanalyseerd. De eindklant (in dit geval KNMI) kan zelf bepalen welke cloud-dienst ze wil afnemen via SURF. SURF zorgt ervoor dat de dienst geleverd wordt. KNMI kan ook direct contact opnemen met AWS. De stap naar (public) clouddiensten gaat meer beheerst als overheidspartijen hun krachten bundelen.

5.3 Uitkomsten toetsing audit 3 public cloud-contracten

Onze audit op 3 belangrijke overheidscontracten laat zien dat de overheid risico's loopt met betrekking tot soevereiniteit, continuïteit van dienstverlening en gegevens-bescherming. De onderzochte organisaties hebben onvoldoende aandacht voor het beheersen van risico's.

We constateren dat contractuele afspraken ingewikkeld zijn en in meerdere overeen-komsten zijn vastgelegd. Kennis over die afspraken is binnen de ministeries beperkt aanwezig. Het ontbreekt aan een volledig overzicht van en inzicht in alle contractuele afspraken. Dit is problematisch, want juist die contractuele voorwaarden zouden de risico's moeten beheersen.

In tabel 7 zijn alle uitkomsten van de toetsingen van de normen voor de 3 principes

betreffende de 3 contracten opgenomen. In bijlage 2 zijn de uitgewerkte normen te vinden. Na de tabel is voor elk van de 3 principes een paragraaf met uitleg over de normen en bevindingen te vinden, met steeds een kader met een goed voorbeeld bij het principe.

Tabel 7 *Lijst met bevindingen als uitkomst van de audit van 3 public cloud-contracten*

Norm Nr.	Onderwerp	BZK - SSC-ICT		VWS - CIBG		IenW - KNMI	
		Opzet	Bestaan	Opzet	Bestaan	Opzet	Bestaan
	Soevereiniteit						
S1	Risicoafweging & contract afsluiten	~	~	✓	✓	✗	✗
S2	Interoperabiliteit & portabiliteit – rollen en verantwoordelijkheden	~	✗	~	✗	✓	✗
S3	Interoperabiliteit & portabiliteit – beëindiging contract	~	✗	~	✗	~	✗
S4	Interoperabiliteit & portabiliteit – overdraagbaarheid	✗	✗	✗	✗	~	✗
S5	Openbaarmaking van gegevens	✓	●	✗	✗	✓	●
S6	Datastromen en -locatie	~	✓	✓	✓	~	✓
S7	Right to audit	✓	✓	~	~	~	●
	Continuïteit dienstverlening						
C1	Continuïteit van bedrijfsvoering	~	~	✗	✗	✗	✗
C2	Back-up en datareplicatie	✓	✗	~	✗	~	✗
C3	Wijzigingen	✓	✓	~	~	~	✗
C4	Security-incidenten	✓	●	~	~	~	~
	Gegevensbescherming						
G1	Governance	~	✓	~	✗	~	✗
G2	Encryptie	~	~	✓	✓	~	✗
G3	Toegangsbeheer	✓	~	~	✗	✓	✗
G4	Toeleveringsketen	✗	✗	✗	✗	✗	✗
G5	Kwetsbaarheden	✗	✗	✓	~	~	✗
G6	Infrastructuurbeveiliging	✗	✓	✓	✓	✓	✓

Voldoet aan de norm:
✓ ja ~ deels ✗ nee ● niet voorgekomen

Opzet: 'op papier' – of de maatregel is vastgelegd in contracten, afspraken, processen of procedures.
Bestaan: 'in de praktijk' – of de maatregel in de praktijk aantoonbaar is aangetroffen.

5.3.1 (Digitale) soevereiniteit

Wij hebben onder andere getoetst of het ministerie voorafgaand aan het afsluiten van het contract een risicoafweging heeft opgesteld. Deze risicoafweging draagt bij aan het inventariseren en bespreken van eventuele cloudrisico's binnen de organisatie en het nemen van maatregelen om deze risico's te beperken. Ook hebben we getoetst of het ministerie maatregelen heeft getroffen om de overdraagbaarheid van gegevens naar een andere cloudprovider mogelijk te maken. Dit is met name belangrijk als het ministerie naar een andere cloudleverancier wil overstappen. Bijvoorbeeld in een noodsituatie, zoals bij een faillissement van de cloudleverancier.

De cloudinfrastructuur moet goed kunnen samenwerken met de andere systemen van een ministerie. We hebben daarom getoetst of het ministerie maatregelen heeft getroffen om deze samenwerking mogelijk te maken, zoals het kunnen uitwisselen van gegevens tussen de systemen.

Sommige statelijke actoren kunnen cloudleveranciers verzoeken om (persoons) gegevens, die zij namens hun klanten verwerken of opslaan, aan hen over te dragen. We hebben daarom getoetst of het ministerie maatregelen heeft getroffen die ervoor zorgen dat verzoeken om openbaarmaking van persoonsgegevens door wetshandhavingsautoriteiten alleen overeenkomstig de toepasselijke wet- en regelgeving plaatsvinden.

Een ministerie zou van een onafhankelijke partij – zoals een auditor – moeten willen horen of de cloudleverancier zijn afspraken nakomt. Wij hebben daarom getoetst of het ministerie het recht heeft bedongen op het kunnen uitvoeren van een audit bij de cloudleverancier. Zo'n auditor kan – maar hoeft niet – de Algemene Rekenkamer te zijn.

Goed voorbeeld risicoafweging voor afsluiten contract: CIBG

De uitvoeringsorganisatie CIBG van het ministerie van VWS heeft risico's goed afgewogen voorafgaand aan het afsluiten van het contract met AWS. Dit begon al bij de aanbesteding. Inschrijvers werd gevraagd aan te geven hoe zij specifieke cloudrisico's beperken, zoals misbruik van een datalek of een configuratiefout in de gedeelde cloudomgeving. Bij de aanbesteding voerde CIBG een zorgvuldigheidsonderzoek uit met een focus op beveiligings-maatregelen. Ook stelde CIBG de daadwerkelijke implementatie van deze beveiligingsmaatregelen vast door een bezoek ter plaatse. Verder liet CIBG toetsen op kwetsbaarheden (pentesten) uitvoeren. Deze kwetsbaarheden zijn vastgelegd in een Risico Acceptatie Document (RAD) en geaccepteerd door het directieteam van CIBG. De minister van VWS is verantwoordelijk voor het CIBG.

Bevindingen

Op basis van ons onderzoek komen we tot de bevinding dat de risico's die spelen bij het beëindigen van een cloudcontract niet goed beheerst worden bij alle 3 de contracten. Ook zien we onvoldoende afspraken in de contracten over hoe gegevens behouden kunnen blijven of over te dragen zijn naar andere systemen.[30] Het Rijk loopt hiermee risico's, bijvoorbeeld als een cloudprovider failliet gaat. Dat dit risico reëel is, blijkt uit recente berichtgeving over de bedreiging van het voortbestaan van Atos, een belangrijke IT-leverancier voor de overheid.[31] Uit ons onderzoek blijkt verder dat de rollen en verantwoordelijkheden onvoldoende duidelijk zijn verdeeld tussen ministerie en cloudprovider.

5.3.2 Continuïteit van dienstverlening

Wij hebben onder andere getoetst of het ministerie maatregelen heeft genomen om ervoor te zorgen dat het ministerie zijn kritieke diensten kan blijven leveren in het geval van een calamiteit. Tevens hebben we getoetst of de calamiteitsplannen die het ministerie met de cloudleverancier afspreekt in de praktijk worden getest.

Als een cloudleverancier wijzigingen in de cloudinfrastructuur doorvoert zonder het ministerie hiervan tijdig op de hoogte te stellen, kan dit leiden tot uitval van de dienstverlening van het ministerie. Wij hebben daarom getoetst of er duidelijke afspraken over het wijzigingenproces zijn gemaakt tussen het ministerie en de cloudleverancier en of deze afspraken in de praktijk worden toegepast.

Als de cloudleverancier en het ministerie geen goede afspraken hebben gemaakt over het melden van security-incidenten, kunnen beide partijen niet tijdig de

benodigde maatregelen nemen. Dit heeft mogelijk negatieve gevolgen voor de dienstverlening van het ministerie. Wij hebben daarom getoetst of er duidelijke afspraken zijn gemaakt over het melden van security-incidenten.

Goed voorbeeld wijzigingsbeheer en beveiligingsincidenten: SSC-ICT

SSC-ICT is een uitvoeringsorganisatie die valt onder het ministerie van BZK. SSC-ICT heeft wijzigingsbeheer en beveiligingsincidenten goed opgenomen in het contract met Microsoft. De contractuele voorwaarden beschrijven op welke wijze Microsoft de klant (SSC-ICT) informeert over belangrijke wijzigingen en welke verantwoordelijkheid de klant heeft. De contractuele voorwaarden bevatten ook bepalingen over hoe Microsoft omgaat met beveiligingsincidenten en wie welke verantwoordelijkheid heeft. De minister van BZK is verantwoordelijk voor wijzigingsbeheer en beveiligingsincidenten voor het contract met Microsoft dat naar onze bevinding voor deze aspecten op orde is.

Bevindingen

Op basis van ons onderzoek komen we tot de bevinding dat de continuïteit van dienstverlening slechts deels gewaarborgd is. SSC-ICT heeft ten opzichte van KNMI en CIBG hiervoor de meeste waarborgen getroffen. Geen van de 3 onderzochte cloudcontracten bevat duidelijke waarborgen voor de continuïteit van de bedrijfsvoering. We verwachten dat in de cloudcontracten afspraken staan voor een plan om in geval van een ramp kritieke diensten te kunnen blijven leveren. Ook verwachten we dat afspraken zijn gemaakt over verschillende locaties om de dienstverlening van het ministerie te kunnen hervatten als een bepaalde locatie van de cloudleverancier uitvalt.

5.3.3 Gegevensbescherming

Wij hebben onder andere getoetst of het ministerie en de cloudleverancier duidelijke afspraken hebben gemaakt over de rollen en verantwoordelijkheden voor gegevensbeheer. Onduidelijke afspraken hebben mogelijk tot gevolg dat niet alle (beveiligings)maatregelen worden genomen die nodig zijn om de gegevens, van het ministerie en de burgers en bedrijven aan wie zij diensten verlenen, goed te beschermen.

Ongeautoriseerde toegang tot de gegevens kan ertoe leiden dat de gegevens van het ministerie worden gestolen, veranderd of verwijderd. Wij hebben daarom ook getoetst of het ministerie en de cloudleverancier afspraken hebben gemaakt over de wijze waarop toegang verkregen kan worden tot gegevens van het ministerie.

Verder hebben we getoetst of de cloudleverancier voldoende maatregelen heeft getroffen om te voorkomen dat de gegevens van het ministerie benaderd kunnen worden door andere klanten van de cloudleverancier.

Goed voorbeeld beveiliging van IT-infrastructuur: CIBG

De minister van VWS heeft het beveiligen van de IT-infrastructuur bij CIBG goed geregeld in het contract met AWS. De cloudapplicatie draait op een gedeelde fysieke IT-infrastructuur. Een gunningscriterium bij de aanbesteding was dat data gescheiden moet worden van klanten die gebruikmaken van dezelfde cloud. Dit betekent dat de data van een klant altijd alléén voor deze klant beschikbaar is. En dat dus niet een andere klant tóch bij de data kan. CIBG heeft middels een bezoek op locatie geverifieerd dat dit ook daadwerkelijk zo is.

Bevindingen

Op basis van ons onderzoek komen we tot de bevinding dat ook het principe gegevensbescherming onvoldoende is gewaarborgd. Voor alle 3 contracten geldt dat er in de leveranciersketen geen goede controle is op de gegevensbescherming. Ook is bijvoorbeeld toegangsbeheer niet op orde. Hierdoor is het risico groter dat onbevoegde medewerkers bij de gegevens kunnen.

6. Conclusies en aanbevelingen

In dit hoofdstuk geven we de hoofdconclusies van ons onderzoek weer en doen we aanbevelingen op basis van ons onderzoek.

6.1 Conclusies

Op basis van onze bevindingen in dit onderzoek concluderen we het volgende:

Kansen en risico's
Cloudcomputing biedt het Rijk kansen op kostenbesparing en efficiëntie, beschikbaarheid en toegankelijkheid, beveiliging en privacy, en innovatiekracht. Tegelijk bestaan er risico's op het gebied van (digitale) soevereiniteit, continuïteit van dienstverlening en gegevensbescherming.

Conclusies deelonderzoek rijksbreed cloudgebruik
Wij hebben bij alle ministeries het volgende onderzocht: zicht op het gebruik van cloud, het maken van risicoafwegingen en beleid en strategie.

Het Rijk maakt volop gebruik van public cloud
Elk ministerie maakt gebruik van public cloud. Bijvoorbeeld bij Microsoft, Amazon en Google. Meer dan de helft van de materieel public cloud-diensten wordt bij deze 3 grote Amerikaanse bedrijven ingekocht.
Van de in totaal 1.588 clouddiensten bij het Rijk zijn 700 (44%) public cloud en 477 (30%) private cloud of hybrid cloud (mengvorm). Van 411 (26%) afgenomen clouddiensten is bij ministeries niet bekend of het om public cloud gaat.

Beperkt zicht op clouddiensten

We concluderen dat ministeries beperkt zicht hebben op hun clouddiensten. Als een ministerie een adequaat overzicht heeft van zijn clouddiensten, kan het sturen op het voldoen aan wet- en regelgeving, het benutten van kansen, het beheersen van risico's en het voldoen aan informatieverplichtingen.

Bij twee derde clouddiensten geen risicoafweging

We concluderen dat ministeries onvoldoende strategische risicoafwegingen hebben gemaakt, voorafgaand aan de beslissing om public cloud te gaan gebruiken. Van de 700 public cloud-diensten zijn er 126 aangeduid als 'materieel' (voor de primaire taak van de organisatie, zoals belastinginning of visumverlening). Bij 84 (67%) van deze diensten is geen risicoafweging gemaakt. Hierdoor blijft bijvoorbeeld het risico bestaan dat gegevens niet goed beschermd zijn of dienstverlening ongewenst kan stoppen. Ook de staatssecretaris Digitalisering kan – via CIO-Rijk – moeilijk (bij) sturen op ministerie-overstijgende cloudrisico's.

Rijksbrede expertise en inkoopkracht onvoldoende gebruikt

We concluderen dat ministeries weinig contact opnemen met de verantwoordelijke partijen voor strategisch leveranciersmanagement (SLM), waardoor ze onvoldoende profiteren van rijksbrede expertise en bijvoorbeeld risicomitigerende maatregelen in SLM-afspraken met cloudleveranciers. Met SLM kan het Rijk zijn macht als grootste IT-afnemer in Nederland beter aanwenden.

Verschillend cloudbeleid

We concluderen dat cloudstrategie en cloudbeleid verschillen per ministerie. Door deze versnippering is het voor alle betrokken partijen lastig om eenduidige afspraken te maken, bijvoorbeeld afspraken tussen ministeries, overheidsdatacentra en cloudleveranciers.

Conclusies deelonderzoek 3 belangrijke public cloud-contracten

We hebben 3 materieel public cloud-contracten nader onderzocht. Het gaat om substantiële contracten voor belangrijke overheidsdienstverlening:

- Microsoft 365 bij het Shared Service Centrum-ICT (SSC-ICT);
- systemen bij het Koninklijk Nederlands Meteorologisch Instituut (KNMI);
- het klantcontactcentrumsysteem bij CIBG[32].

Onvoldoende maatregelen voor borgen soevereiniteit, continuïteit en gegevensbescherming

We concluderen dat de betreffende ministeries onvoldoende maatregelen nemen om de soevereiniteit, continuïteit van dienstverlening en gegevensbescherming te waarborgen in public cloud-contracten. Dit betekent dat het Rijk risico's loopt, bijvoorbeeld als een cloudprovider failliet gaat. Het risico bestaat dat het Rijk producten of diensten voor burgers en bedrijven niet kan blijven leveren. Ook bestaat het risico dat gegevens van burgers en bedrijven onvoldoende beschermd zijn en kunnen worden misbruikt door kwaadwillenden en statelijke actoren.

Onvoldoende grip op contractuele afspraken public cloud-diensten

We concluderen dat de betreffende ministeries onvoldoende grip hebben op hun contractuele afspraken voor de public cloud-diensten. Het ontbreekt aan een volledig overzicht van en inzicht in alle contractuele afspraken. Er zijn vaak meerdere partijen bij een public cloud-dienst betrokken, bijvoorbeeld een sharedservice-organisatie (SSO) en onderaannemers. We constateren dat contractuele afspraken ingewikkeld zijn en in meerdere overeenkomsten zijn vastgelegd. Kennis over die afspraken is binnen de ministeries beperkt aanwezig. Dit is problematisch, want juist die contractuele voorwaarden zouden de risico's moeten beheersen.

Belangrijkste conclusies en oordeel

In dit onderzoek hebben we getoetst in hoeverre het Rijk handelt conform het Rijksbreed cloudbeleid en of de principes (digitale) soevereiniteit, continuïteit van de dienstverlening en gegevensbescherming zijn gewaarborgd. We trekken de volgende belangrijkste conclusies:

1. Het Rijk heeft beperkt zicht op clouddiensten.
2. Het Rijk maakt onvoldoende strategische risicoafwegingen.
3. Het Rijk waarborgt onvoldoende de principes (digitale) soevereiniteit, continuïteit van de dienstverlening en de gegevensbescherming in 3 onderzochte public cloud-contracten.

Op basis van dit onderzoek concluderen we dat het Rijk ondoordacht cloud is gaan gebruiken en nu onvoldoende grip op heeft op zijn cloudgebruik.

Wij geven in onze onderzoeken over resultaten van het gevoerde beleid een oordeel. Dat doen wij met een vijfpuntsschaal: goed, toereikend, matig, zorgelijk of zeer zorgelijk.

Wij beoordelen het cloudgebruik door het Rijk als **zorgelijk**. De dienstverlening aan burgers en bedrijven en de continuïteit van het functioneren van de overheid lopen immers te veel risico. De mogelijke schade van verstoorde overheidsdienstverlening kan ons land en onze maatschappij ontwrichten. Daarnaast kan cloudbeleid – en de uitvoering hiervan – niet los worden gezien van een context waarin geopolitieke ontwikkelingen verontrustend zijn.

Oordeel

Hierbij willen we benoemen dat verscheidene ministeries in de onderzoeksperiode vooruitgang hebben laten zien op diverse gebieden, zoals het verbeteren van zicht op hun clouddiensten en het vaststellen van departementaal beleid. Op andere gebieden (het maken van risicoafwegingen, het borgen van principes in contracten) is een flinke verbeterslag noodzakelijk.

6.2 Aanbevelingen

Onze hoofdaanbeveling, aan alle ministers:
Om soevereine, continue en veilige overheidsdienstverlening te borgen is het zaak dat het Rijk richting de grote clouddienstverleners als één samenwerkende overheid kaders stelt, regels hanteert, risico's mitigeert en zijn positie ten opzichte van leveranciers en andere gebruikers van de cloud versterkt. Hiervoor is het nodig dat het Rijk beter zicht heeft op het eigen cloudgebruik en veel gerichter kansen, risico's en alternatieven afweegt voorafgaand aan, maar ook tijdens cloudgebruik.

Deze hoofdaanbeveling werken we verder uit in de volgende deelaanbevelingen met na de aanbeveling steeds een toelichting:

Aan de minister van BZK

Deelaanbeveling 1

Maak het Rijksbreed cloudbeleid uniformer en concreter, en houd hier toezicht op:

- Uniformer: door zo weinig mogelijk verschillen in departementaal beleid toe te staan en bijvoorbeeld ook de 'Handreiking risicobeheersing toepassing public cloud' verplicht te stellen. Onderzoek de mogelijkheid om het Rijksbreed cloudbeleid uit breiden naar decentrale overheden en zelfstandige bestuurs-organen (zbo's).
- Concreter: door bijvoorbeeld ook nadrukkelijk enkele diensten van de overheid te noemen die onder geen beding naar de public cloud mogen.

Nadere toelichting: uit ons onderzoek blijkt dat de organisaties binnen het Rijk verschillend met cloud omgaan. We zien dat deze verschillen een negatieve invloed hebben op de risicobeheersing van cloud. Verder heeft het Rijksbreed cloudbeleid een beperkte scope binnen de overheid, omdat zbo's en decentrale overheden zijn uitgesloten. Het is wenselijk dat de gehele overheid hetzelfde cloudbeleid hanteert. In de gehele keten worden immers risico's gelopen. Een bekend voorbeeld van overheidsbreed beleid dat voor alle overheidsorganisaties geldt is de Baseline Informatiebeveiliging Overheid (BIO). Voor digitale veiligheid is de cloud ook van belang en daarmee is overheidsbreed beleid nodig.

Deelaanbeveling 2

Richt de handhaving van het Rijksbreed cloudbeleid beter in. Het voldoen aan het Rijksbreed cloudbeleid is nu te vrijblijvend. De staatssecretaris Digitalisering zou – via CIO-Rijk – deze rol steviger moeten pakken, in nauwe samenwerking met de departementale CIO's en verschillende expertises, zoals inkoop.

Deelaanbeveling 3

Zie bij alle ministeries toe op het verbeteren van het zicht op gebruikte clouddiensten en het alsnog maken van risicoafwegingen voor materieel public cloud-diensten waarvoor geen risicoafweging is gemaakt.

*Nadere toelichting***:** met ons onderzoek wordt duidelijk dat de ministeries nog maar beperkt voldoen aan de voorwaarden (bijvoorbeeld risicoafwegingen), zoals deze zijn gesteld in het Rijksbreed cloudbeleid. Daarnaast is de informatieverstrekking vanuit ministeries over cloud aan CIO-Rijk zeer verschillend van omvang en detail. Het onderwerp cloud loopt veelal via de informatiebeveiligingsexpert (CISO), terwijl cloud

vanuit meerdere expertises zou moeten worden benaderd, zoals strategische inkoop, leveranciersmanagement en privacy. De staatssecretaris Digitalisering zou – via CIO-Rijk – meer oog moeten hebben voor en meer moeten samenwerken met deze expertises.

Aan alle ministers

Deelaanbeveling 1
Het Rijk moet meer sturen op gezamenlijk inkopen, bedingen van voorwaarden en laten uitvoeren van audits. Een centrale partij voor strategisch leveranciers-management (SLM) kan een voortrekkersrol vervullen in het doelmatig afsluiten van cloudcontracten. In EU-verband zijn er kansen voor het Rijk om samen te werken voor standaardisatie, certificering en het afdwingen van AVG-voorwaarden. Overweeg als Rijk realistische EU-alternatieven in combinatie met een uitvoerbare exitstrategie.

Nadere toelichting: wanneer elk ministerie de makkelijkste en goedkoopste keuze maakt, wordt de afhankelijkheid van het Rijk van enkele grote cloudleveranciers steeds groter. Daarom moet het Rijk meer als één samenwerkende organisatie optrekken bij inkoop, bedingen van voorwaarden (zoals AVG-voorwaarden) en het beheersen van risico's. Vervolgens moet het Rijk zich ervan vergewissen dat de voorwaarden worden nageleefd door de cloudleveranciers. Dit kan met gezamenlijke audits.

Het Rijk moet zich voor cloud meer als één samenwerkende overheid opstellen naar de grote cloudleveranciers en minimaal gebruikmaken van de bestaande mantel-overeenkomsten die gemaakt worden door de verschillende afdelingen binnen het Rijk die zorgen voor strategisch leveranciersmanagement (SLM). Het Rijk kan zijn macht als grootste ICT-afnemer in Nederland op deze wijze beter aanwenden. Zoals in § 2.2.1 gemeld is ook het strategisch leveranciersmanagement versnipperd. Een centrale partij SLM voor IT-dienstverlening zou logischer zijn, ook om verschillende clouddiensten te vergelijken en generieke voorwaarden te bedingen.

In de discussies over cloud lijkt het soms wel dat alleen bedrijven in de VS en China cloud aanbieden. Er zijn echter ook Europese initiatieven, zoals genoemd in dit rapport. Verder zou de EU bijvoorbeeld kunnen standaardiseren en certificeren en op deze wijze een blok kunnen vormen om gezamenlijk inhoudelijke eisen te kunnen stellen. Een aanzet hiervoor wordt gedaan met het komende Europese Cyber-beveiligingscertificeringssysteem voor clouddiensten, zie ook § 3.5.3.

Deelaanbeveling 2

Weeg voor elke nieuwe mogelijke clouddienst de kansen en risico's af en update risicoafwegingen van reeds gecontracteerde clouddiensten. De kansen en risico's kunnen namelijk per dienst verschillen. De afweging moet in ieder geval ingaan op de principes soevereiniteit, continuïteit van dienstverlening en gegevensbescherming. En daarnaast op andere aspecten zoals kosten, innovatiekracht en vereiste kennis en kunde.

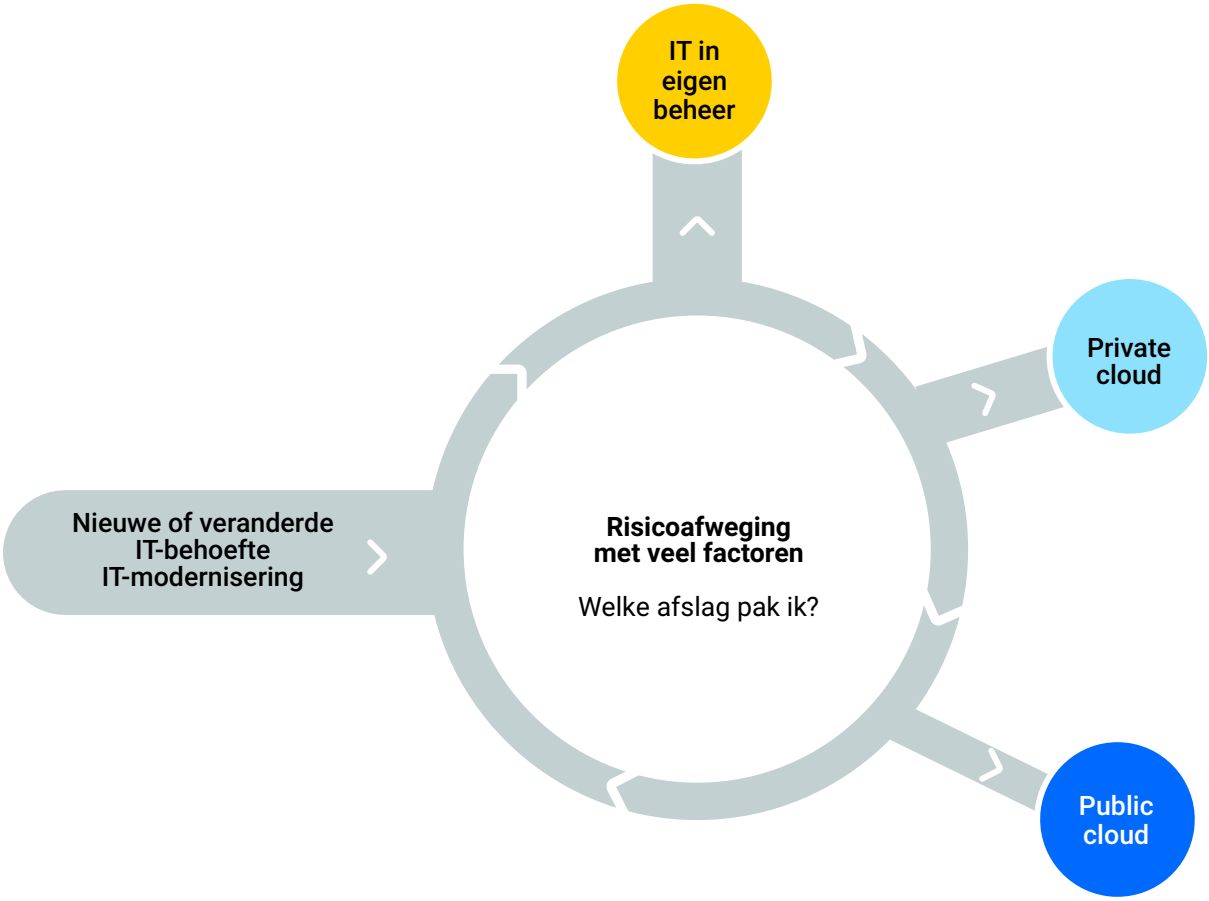
Deelaanbeveling 3

Verbeter het zicht op gebruikte clouddiensten en maak alsnog risicoafwegingen voor materieel public cloud-diensten waarvoor geen afweging is gemaakt. Neem maatregelen om de risico's te mitigeren. Bijvoorbeeld door extra contractuele voorwaarden af te spreken en te (laten) toetsen of deze worden nagekomen.

Nadere toelichting: het is essentieel om bewuste keuzes in het IT-landschap te maken. Wat kan wel en niet in de cloud en welke cloudvorm is dan het meest geschikt? Voor elke clouddienst kunnen de kansen en risico's verschillen. Deze moeten dus afgewogen worden. Dit wordt gevisualiseerd in Figuur 9. Dit is belangrijk voor nieuwe mogelijke clouddiensten én clouddiensten die al afgenomen worden maar waarbij zo'n afweging niet is gemaakt. De risico's zijn namelijk té groot, zoals geschetst in dit rapport.

Figuur 9 *Keuze van vorm van IT na risicoafwegig met veel factoren*

Het Rijk moet beter afwegen welke vorm van IT past



7. Reactie en nawoord

Op 9 december 2024 ontvingen we van de staatssecretaris Digitalisering een reactie op ons conceptrapport. Hieronder geven we het meest relevante deel uit zijn reactie weer. De volledige reactie staat op www.rekenkamer.nl. We sluiten af met ons nawoord.

7.1 Reactie staatssecretaris Digitalisering

De staatssecretaris Digitalisering bedankt ons in zijn reactie voor het rapport en geeft aan dat het hem belangrijke inzichten levert in de wijze waarop het Rijk de public cloud inzet en wat daarin verbeterd kan worden. Hij schrijft verder het volgende:

“Algemeen beeld
(...) Ik neem uw adviezen mee in de verbeteringen in en herzieningen van het Cloud-beleid en het implementatiekader, de besturing en de dagelijkse praktijk. Dit is een traject waarop ik centraal acties uitzet. Daarnaast moeten ook alle departementen en hun onderdelen met deze acties aan de slag gaan, onder aansturing van de eigen politieke en ambtelijke leiding.

Alle departementen en hun onderdelen: Verbetering operatie: meer inzicht en betere risicobeheersing
U constateert dat het inzicht in en de risicobeheersing van het cloudgebruik nog onvoldoende zijn. De inventarisaties door de departementen en hun onderdelen zijn nog niet volledig waardoor belangrijke inzichten ontbreken. Evenmin delen de onderdelen in alle gevallen deze inventarisaties met hun departement en

inventarisaties van materieel public cloudgebruik met CIO Rijk. Daarnaast ontbreken in veel gevallen vastgestelde risicoanalyses. Mede daardoor blijven de getroffen maatregelen achter.

De operationele beheersing valt onder de ministeriële verantwoordelijkheid van de desbetreffende departementen. U constateert dat tussen de twee meetmomenten al verbetering was opgetreden. Ik zal met mijn collega's actie nemen om de ingezette inhaalslag te versterken en zo het departementaal inzicht in het cloudgebruik te verbeteren en te komen tot betere departementale risicobeheersing. Ik zal dit centraal ondersteunen. Meer zicht op individuele risico's geeft ons vervolgens ook de mogelijkheid te sturen op departement-overstijgende risico's en dit bijvoorbeeld mee te nemen in het onderzoek naar digitale autonomie.

Uw bevindingen en aanbevelingen nemen we ook mee voor cloudgebruik dat in voorbereiding is. Dit geldt bijvoorbeeld voor de door u onderzochte werkplekdiensten van SSC-ICT: die zijn nu nog nagenoeg volledig on premises. SSC-ICT vernieuwt haar werkplekdiensten. Hierbij zullen geen onomkeerbare stappen worden gezet conform de afspraken met de Kamer hierover. Voor al het gepland cloudgebruik geldt steeds dat vooraf passende en formele risico-mitigatie plaatsvindt.
Invoering van de Algemene Beveiligingseisen Rijksoverheid Opdrachten (ABRO) zal ook bijdragen aan het beter mitigeren van risico's van cloudgebruik. Dit stelt standaard meer eisen aan de dienstverlening en de leverancier zelf en ook wordt standaard onderzocht of de dienstverlening en leverancier hieraan voldoen.

MinBZK en de departementen: Verbetering besturing en toezicht
Omdat de operationele beheersing achterblijft, adviseert u om minder vrijblijvend te sturen en beter toezicht te houden.

Ik onderschrijf dat de operationele verbetering ook meer besturing en toezicht vereisen. Om te sturen op de voortgang van de operationele verbetering heb ik maatregelen genomen om mij periodiek te laten informeren over de stand van zaken door CIO Rijk. Waar nodig zal ik samen met mijn collega's bijsturen.
Tevens zal ik inzetten op meer samenhang tussen onderdelen van de overheid waar dit nationale belangen of veiligheid raakt. CIO Rijk zal hierin een coördinerende en faciliterende rol vervullen zodat de CIO's binnen de rijksoverheid kunnen sturen op te nemen verbeterstappen.

MinBZK: Verbetering beleid en uitbreiding scope
Hoewel veel van voorgaande bevindingen opgelost worden door het volledig volgen van het cloudbeleid en implementatiekader, ziet u ook verbeteringsmogelijkheden in het beleid door het beleid uniformer en concreter te maken. De hoofdlijn daarin is om minder verschillen te laten ontstaan tussen de departementale cloudbeleidsstukken, de scope uit te breiden naar de gehele overheid, waaronder de medeoverheden en zbo's, en om bepaalde overheidsdiensten specifiek uit te sluiten van cloudgebruik.

Ik sta voor de één overheidsgedachte en ik wil de medeoverheden en zbo's betrekken in de vernieuwing van het cloudbeleid, en te komen tot één cloudbeleid voor de gehele overheid. Deze gedachte wordt ook meegenomen in de Nederlandse Digitaliseringsstrategie (NDS), welke momenteel uitgewerkt wordt.

Ik sta in beginsel positief tegenover het concreter en uniformer maken van het beleid. Dit sluit ook aan op mijn eigen evaluatie. In de komende herziening van het rijksbrede public cloudbeleid zal ik deze punten meenemen. Het beperken van verschillen tussen de departementale beleidstukken en het uitsluiten van specifieke diensten zijn waardevolle adviezen. Op strategisch beleidsniveau is veel uniformiteit mogelijk. Tegelijkertijd zijn er duidelijke operationele verschillen tussen de rijksorganisaties die leiden tot verschillende functionele behoeften in het cloudgebruik. Daarnaast zijn er meerdere manieren om operationeel goede risicobeheersing uit te voeren. Daar moet ruimte voor blijven. Een one-size-fits-all benadering kan passen op strategische niveau maar niet altijd op operationeel niveau. Het vinden van de juiste balans tussen blijft dus van belang.

MinBZK en departementen: Verbeteren samenwerking inkoop en contractbeheer
U constateert dat Strategisch Leveranciersmanagement (SLM) onvoldoende geraadpleegd wordt en dat de contractuele afspraken complex zijn. U adviseert om meer gezamenlijk in te kopen met daarbij een centrale rol voor SLM en hierbij ook samenwerking in EU-verband op te zoeken.

Ik onderschrijf het belang om meer samen te werken bij inkoop en daarbij de rol en positie van SLM te versterken met bijvoorbeeld een gedeeld expertisecentrum en (externe) specialistische dienstverlening. Dit leidt ook tot een set met formele afspraken, een logische opbouw en hiërarchie, minder contracten en dus minder complexiteit. Een gebalanceerde en dekkende maatregelenset (technisch, interne procedures, afspraken met toeleverancier etc.) draagt bij aan het beter borgen van de autonomie, continuïteit en gegevensbescherming. Samenwerken maakt het mogelijk om hierin effectiever in op te treden.

Met de EU is contact over samenwerking en die zullen we ook hiervoor inzetten. We werken op diverse gebieden samen, waaronder cloud en onderzoeken naar Europese cloudinitiatieven.

Ik nodig u graag uit om over de aanpak en opvolging van uw bevindingen in gesprek te gaan."

7.2 Nawoord

Wij waarderen dat de staatssecretaris Digitalisering in zijn reactie aangeeft dat hij onze hoofdconclusie deelt dat het cloudgebruik van het Rijk zorgelijk is en dat verbetering nodig is. Hij geeft aan dat inderdaad meer sturing en toezicht van zijn kant nodig is. We blijven graag ambtelijk en bestuurlijk in gesprek, zoals de staatssecretaris in zijn reactie aanbiedt. Wel geven we mee dat hij de verbetering op enkele punten concreter en met meer urgentie kan uitwerken.

Een begrijpelijke zorg vanuit de Tweede Kamer is de digitale soevereiniteit. Daarbij zou het passen om bepaalde diensten expliciet uit te sluiten van public cloud-gebruik. Staatsgeheime informatie is conform het Rijksbreed cloudbeleid al uitgesloten. Voor basisregistraties geldt 'nee, tenzij'. Per ministerie zouden diensten kunnen worden uitgesloten, denk aan kritieke fysieke infrastructuur. Dit kan de staatssecretaris bepalen op grond van het *Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst* en het *Besluit CIO-stelsel rijksdienst*. Het beperkt de ministeriële verantwoordelijkheid van vakministers niet. Op termijn zou een soevereine cloud – al dan niet met behulp van Europese cloudpartijen – hier mogelijk ook deels een oplossing kunnen bieden. De staatssecretaris zou verder bindend kunnen vastleggen wat materieel public cloud-gebruik is en zou het voortouw kunnen nemen bij het gezamenlijk inkopen van cloud.

Ons tweede en laatste punt betreft – met bovenstaande samenhangend – de invulling van de eigen rol van de staatssecretaris. Het is positief dat hij zijn collega's wil aanspreken. Maar daar gaat aan vooraf dat de staatssecretaris ambtelijk andere ministeries laat aanspreken op verplichtingen uit de niet-vrijblijvende rijksbrede kaders voor cloud. Bijvoorbeeld dat de reeds verplichte risicoafwegingen voor cloudgebruik alsnog moeten worden gemaakt binnen een bepaalde (korte) periode. Leidt dat niet tot verbetering, dan kan op grond van het hierboven genoemde Coördinatiebesluit worden geëscaleerd naar de ministerraad. Van dit mandaat van (de minister van) BZK wordt nog te weinig gebruik gemaakt. Daarnaast kan

transparantie over de stand van zaken per ministerie ook helpen om verbetering te bewerkstelligen. Het is immers onaanvaardbaar dat gevoelige informatie zonder risicoafweging in de cloud wordt gebracht. Misbruik van deze informatie door kwaadwillenden en statelijke actoren moet ten allen tijde worden voorkomen. Burgers en bedrijven mogen een meer zorgvuldige omgang met hun gegevens van het Rijk verwachten.

Bijlagen

Bijlage 1 Methodologische verantwoording

Wat hebben we onderzocht?

Wij voerden dit onderzoek uit aan de hand van 2 hoofdvragen. De eerste hoofdvraag heeft betrekking op het rijksbreed handelen op basis van het bestaande cloudbeleid en implementatiekader Rijk.

Hoofdvraag 1: In hoeverre handelen CIO-Rijk en de departementale CIO's conform het Rijksbreed beleid en Implementatiekader cloud voor bepaalde aspecten?

Deze 'bepaalde aspecten' staan in de volgende opsomming. Om het onderzoek uitvoerbaar te houden hebben we uit alle aspecten van het Rijksbreed cloudbeleid en Implementatiekader geselecteerd wat er volgens ons minimaal zou moeten zijn.
Wij onderzochten in hoeverre er sprake is van:

- departementaal cloudbeleid: in het cloudbeleid van CIO-Rijk staat dat elk ministerie over een eigen cloudbeleid moet beschikken;
- een cloudoverzicht: een ministerie moet inzicht hebben in welke clouddiensten in gebruik zijn en of hier contractuele afspraken over zijn vastgelegd;
- een vastgelegde afweging van voor- en nadelen (inclusief kosten) van public cloud-contracten: een ministerie moet een risicoafweging maken en zo mogelijk een businesscase hebben voor cloudcontracten.

Op basis van dit beeld toetsten we of een ministerie handelt conform onze onderzochte aspecten die als zodanig zijn opgenomen in het rijksbeleid en implementatiekader cloud. We toetsen het handelen van:

- de minister van BZK voor wat betreft de verantwoordelijkheden CIO-Rijk;
- de minister van BZK en de andere ministers voor wat betreft het handelen van de departementale CIO's.

In het normenkader in bijlage 2 is opgenomen hoe de aspecten zijn te relateren aan het rijksbeleid en implementatiekader cloud en welke verantwoordelijkheid die raken.

Het is goed om te weten dat we het cloudoverzicht in dit onderzoek breder hebben uitgevraagd, dan alleen materieel public cloud waar het Rijksbreed cloudbeleid betrekking op heeft. We hebben alle vormen van cloud uitgevraagd. Ook hebben wij het ministerie van Defensie onderzocht dat formeel niet onder het Rijksbreed cloudbeleid valt.

De tweede hoofdvraag heeft betrekking op het voldoen aan principes in de praktijk binnen het Rijk.

Hoofdvraag 2: In hoeverre zijn de soevereiniteit, de continuïteit van de dienstverlening en de gegevensbescherming gewaarborgd voor 3 geselecteerde public cloud-contracten?

Wij toetsten hiervoor een drietal cloudcontracten[33] vanuit onze inventarisatie bij hoofdvraag 1 waarbij (grotendeels) sprake is van public cloud en die het meest de dienstverlening van de overheid richting burgers en bedrijven raakt. Met deze deelwaarneming van 3 grote contracten bij 3 verschillende grote public cloud-aanbieders proberen wij een goede representatie te geven waarbij ook met een realistische onderzoekstijd rekening is gehouden. Het ministerie heeft ons moeten aantonen dat zij bij de clouddienstverlening voldoende beheersmaatregelen had getroffen om onze 3 gekozen principes (soevereiniteit, continuïteit van dienstverlening en gegevensbescherming), te waarborgen. Op basis van onze bevindingen doen we echter geen generaliserende uitspraken over alle cloudcontracten bij het Rijk. Wel geeft dit voldoende indicatie in hoeverre de principes worden nagestreefd, zodat het beleids- en implementatiekader aangescherpt kunnen worden.

Voor de te toetsen normen sloten we zoveel mogelijk aan bij het huidige beleids- en implementatiekader cloud van het Rijk. We vulden dit aan met ontbrekende normen, zoveel mogelijk gebruikmakend van bestaande wet- en regelgeving en richtlijnen.

Ook organiseerden we hier een workshop over met experts. Vervolgens scherpten we ons normenkader aan.

Voor de 3 public cloud-diensten hebben we het volgende concreet getoetst: we hebben de dienstverleningsafspraken getoetst die in contracten zijn vastgelegd of in documenten zoals gebruikersovereenkomsten en servicevoorwaarden. Meer specifiek:

- Voor de contractaudit betreffende SSC-ICT zijn het contract en dienstverlenings-afspraken met Microsoft getoetst.
- Voor de contractaudit betreffende CIBG geldt het volgende: CIBG heeft met een hoofdaannemer contractuele afspraken in een overeenkomst vastgelegd. In onderliggende documenten van de overeenkomst zoals de SLA (Service Level Agreement) en het DAP (Dossier Afspraken en Procedures) staan afspraken gemaakt over diensten die een onderaannemer voor KLOPT uitvoert. Voor het DAP geeft ook deze onderaannemer akkoord. Als we het in dit rapport hebben over het geselecteerde cloudcontract, dan bedoelen we dus de contractuele afspraken van VWS/CIBG met hoofdaannemer en onderaannemer.
- Voor de contractaudit betreffende KNMI hebben wij primair gekeken naar het contract tussen KNMI en SURF. Dit omdat KNMI contractuele afspraken met SURF heeft gemaakt in een raamovereenkomst. SURF is de opdrachtnemer in de uitbestedingsketen en door het KNMI aangewezen als reseller. SURF heeft op basis van afspraken in het contract met KNMI contracten afgesloten met andere organisaties (namens het KNMI) om de AWS-clouddienstverlening mogelijk te maken.

Context / kansen en risico's

Om een goed en evenwichtig beeld te krijgen van de kansen en risico's van cloud interviewden we relevante partijen als de Cyber Security Raad, cloudleveranciers, de Autoriteit Persoonsgegevens en beleidsverantwoordelijken bij de Europese Commissie.

Onderzoeksactiviteiten

- De onderzoeksperiode liep van mei 2023 tot en met augustus 2024.
- Bij de start hebben we het onderzoek toegelicht in de rijksbrede gremia; de CISO-raad, de CTO-raad en het CIO-beraad. Daarna voerden we de volgende acties uit:
- Opstellen cloudoverzicht template (te vinden in bijlage 2): voor de inventarisatie van clouddiensten bij alle 11 ministeries hebben wij een template opgesteld.

- Opvragen en analyseren van departementaal beleid en afwegingskaders, cloudoverzichten en (voor public cloud-contracten) risicoafwegingen. Dit is gedaan voor alle 11 ministeries.
- Startgesprekken en interviews met relevante functionarissen van alle ministeries over de aangeleverde informatie voor de cloudoverzichten.
- Opstellen normenkader contractaudit: op basis van input en onderzoek naar standaarden en belangrijke ontwikkelingen hebben wij ons normenkader voor cloudcontracten opgesteld.
- Workshop normenkader contractaudit: op 28 september 2023 organiseerden wij een workshop om ons onderzoek toe te lichten. Samen met de deelnemers hebben we ons gebogen over het te gebruiken normenkader. Bij de workshop waren 31 deelnemers aanwezig vanuit de meeste ministeries; specifiek ook auditors van de Auditdienst Rijk en adviseurs van strategisch leveranciers-management (SLM) en het Nationaal Cyber Security Centrum (NCSC). Het kader is vervolgens nog aangescherpt op basis van deze workshop en verder onderzoek.
- Opvragen en analyseren van contractdocumentatie en ingevulde normenkaders voor 3 geselecteerde public cloud-contracten.
- Startgesprekken en interviews met relevante functionarissen van de betrokken ministeries en uitvoeringsorganisaties over de aangeleverde informatie voor de contractaudit.
- Tijdens de onderzoeksperiode en rond de diverse gesprekken is relevante documentatie opgevraagd bij de gecontroleerden, die door ons is geanalyseerd.
- Expertinterviews: in de tweede helft van 2023 en de eerste helft van 2024 hebben wij diverse experts geïnterviewd van binnen en buiten de overheid op het gebied van cloudtechnologie. Er is onder andere gesproken met functionarissen van het NCSC, de European Union Agency for Cybersecurity (ENISA), SSO's en EY. De volledige lijst met gesprekspartners is te vinden in bijlage 3.
- Seminar cloud: voor het deelonderzoek naar beleid, overzicht en afweging hebben we per ministerie 2 nota's opgesteld: 1 voor de situatie eind 2023 en 1 voor de situatie medio 2024. Op 8 februari 2024 organiseerden we een seminar met de bevindingen van de situatie eind 2023, zodat ministeries in de maanden daarna nog verbeteringen konden doorvoeren.
- Uiteindelijk hebben we voor dit onderzoek 26 nota's van bevindingen opgesteld voor de verschillende deelonderwerpen en ministeries. Deze liggen ten grondslag aan dit rapport.

Bijlage 2 Normenkaders

Normenkader voor hoofdvraag 1

Hieronder is het normenkader opgenomen dat wij gebruiken in ons onderzoek om de onderzoeksvragen te beantwoorden. De kolom **Norm** bevat de norm betreffende de relevante hoofdvraag (onderzoeksvraag). De kolom **Risico** geeft aan dat als voldoende maatregelen zijn getroffen om aan de norm te voldoen, dat daarmee het gegeven risico wordt beheerst. De kolom **Bronnen** geeft een niet uitputtende lijst van mogelijke bronnen weer die maatregelen kunnen zijn om aan de norm te kunnen voldoen. De kolom **Referentie** geeft de afkomst aan van de norm en de kolom **Toelichting** een nadere specificatie van de concrete toetsing.

Hoofdvraag 1: *In hoeverre handelen CIO-Rijk en de departementale CIO's conform het Rijksbreed beleid en Implementatiekader cloud voor bepaalde aspecten?*

Norm 1	Risico	Bronnen	Referentie	Toelichting
CIO-Rijk monitort gebruik rijksbreed cloudbeleid en rapporteert aan de Tweede Kamer	Risico dat organisaties het Rijksbreed cloudbeleid niet goed interpreteren of zelfs helemaal niet bekend hiermee zijn waardoor de organisatie risico's loopt v.w.b. soevereiniteit, continuïteit dienstverlening en gegevensbescherming.	• Interviews CIO-Rijk • Communicatie omtrent rijksbreed cloudbeleid • Monitoring controles	Rijksbreed cloudbeleid 2022 voorwaarde 1: "(.) *monitort CIO Rijk de implementatie conform het Besluit CIO stelsel*." Implementatiekader Artikel 14. "De ontvangen rapportages, DPIA's en risicoanalyses gebruikt CIO Rijk conform het cloudbeleid en het CIO-stelsel, in de jaarlijkse cyclus van de CIO-gesprekken als onderdeel van haar monitorings- en adviesfunctie. (.) Op basis van de aangeleverde rapportages houdt CIO Rijk een totaaloverzicht bij van het materieel public cloudgebruik. Tevens rapporteert CIO Rijk conform het Cloudbeleid over de voortgang van de implementatie van het Cloudbeleid aan de Tweede Kamer."	We toetsen of CIO-Rijk: • de implementatie van het cloudbeleid monitort; • CIO-gesprekken houdt waarbij cloud wordt besproken; • monitorings-informatie analyseert en hieraan acties verbindt; • een totaaloverzicht materieel public cloud-gebruik bijhoudt; • over de voortgang van de implementatie van het cloudbeleid aan de Tweede Kamer rapporteert.

Hoofdvraag 1a: departementaal cloudbeleid

Norm 2	Risico	Bronnen	Referentie	Toelichting
Alle onderdelen van de Rijksdienst formuleren hun eigen departementale cloudbeleid en -strategie binnen de kaders van het Rijksbreed cloudbeleid en het Implementatiekader cloud.	Risico dat er geen cloudbeleid en -strategie is of niet in afstemming met rijksbreed cloudbeleid waardoor organisatie niet voldoet aan het Rijksbreed cloudbeleid waardoor de organisatie risico's loopt v.w.b. soevereiniteit, continuïteit dienstverlening en gegevensbescherming.	• Departementaal cloudbeleid en -strategie; • Andere departementale kaders gerelateerd aan cloudgebruik; • Interview per ministerie (gespreksverslag).	Implementatie-kader cloud: Art 1.b	We toetsen voor departementale cloudbeleid en -strategie: • Is het aanwezig? • Is het vastgesteld? • Is het Rijksbreed cloudbeleid hierin verwerkt? We toetsen hierbij niet of het departementale beleid. volledig overeenkomt met het Rijksbreed cloudbeleid en Implementatiekader.

Hoofdvraag 1b: een cloudoverzicht

Norm 3	Risico	Bronnen	Referentie	Toelichting
De departementen houden voor het materieel public cloudgebruik ten minste de volgende zaken bij: • Het organisatie-onderdeel; • Het bedrijfsproces; • Inzicht in de risico's; • De leverancier van de public cloud-dienst en de afgenomen clouddiensten	Door het ontbreken van een overzicht kan een organisatie niet sturen op het voldoen aan wet- en regelgeving, waaronder de beheersing van risico's en het voldoen aan informatie-verplichtingen.	• Aangeleverd cloud-overzicht van ministerie in Algemene Rekenkamer-template; • Overige documentatie die betrekking heeft op a, b, c en/of d; • Interview per ministerie (gespreksverslag).	Implementatie-kader cloud: Art 13.1	We toetsen hierbij of de departementen een overzicht hebben van hun cloudgebruik waarbij in ieder geval de materieel public cloud-diensten zijn opgenomen die zijn te herleiden naar een organisatie-onderdeel of bedrijfsproces; waarbij inzichtelijk is of een risicoafweging is gemaakt en de cloudleverancier inzichtelijk is. Waarop getoetst zal worden (de norm) is materieel public cloud-gebruik. Een overzicht van materieel public cloud moet er minimaal zijn.

Hoofdvraag 1c: een vastgelegde afweging van voor- en nadelen (incl. kosten)

Norm 4	Risico	Bronnen	Referentie	Toelichting
De departementen en hun onderdelen hebben conform de BIO een formeel vast-gestelde risicomanagement-methodiek. Voorafgaand aan het gebruik van public clouddiensten wordt conform die methodiek een risico-afweging gemaakt. Hierbij wordt conform cloudbeleid SLM geraadpleegd ten behoeve van hergebruik van eerdere analyses en waar mogelijk een gezamenlijke aanpak. In de afweging om een clouddienst af te nemen zijn ook de kosten en baten afgewogen.	Als er geen weloverwogen beslissing is genomen, bestaat het risico dat gegevens niet goed beschermd zijn, conti-nuïteit van dienstverlening gevaarloopt en de onafhankelijkheid van de organisatie niet goed is gewaarborgd. Het niet inzichtelijk maken van kosten en het niet gebruiken van mantel-overeenkomsten zorgt voor mogelijk duurdere dienstverlening en het niet voldoen aan rijksbrede afspraken.	• Documentatie die betrekking heeft op afwegingen, risico-management en/of financiële aspecten; • Interview per ministerie (gespreks-verslag).	Implementatie-kader cloud: Art 4.1 en 2; Toevoeging door Algemene Rekenkamer.	We toetsen de volgende elementen: • voor 'risicomanagement-methodiek': 1. is er een methodiek aanwezig: a. wordt hierbij een strategische afweging 'wel/niet naar de cloud gaan' gefaciliteerd, b. gaat de methodiek expliciet in op cloud? 2. is deze methodiek vastgesteld? • voor risicoafwegingen voor materieel public cloud-diensten: 1. zijn risicoafwegingen gemaakt a. via de eventuele methodiek of b. anderszins? (Een risico-afweging kan gemaakt zijn in een risicoanalyse). 2. is SLM-Rijk geraadpleegd? 3. zijn financiële aspecten (kosten/baten) meegenomen bij de afwegingen?

Normenkader voor hoofdvraag 2

Hieronder staat het gebruikte normenkader voor het deelonderzoek voor hoofdvraag 2. De kolom **Nr.** verwijst naar de unieke nummering van de normen zoals ook gebruikt in de hoofdstukken 4 t/m 6 inclusief verwijzing naar de 3 getoetste principes soevereiniteit (Sn), continuïteit (Cn) en gegevensbescherming (Gn).
De 3 getoetste principes zijn op het einde van deze bijlage ook nog gedefinieerd inclusief het risico. De kolom **Onderwerp** verwijst naar het onderwerp van de norm. Kolom **Bron + Control ID** geeft een verwijzing naar de oorsprong van de norm. Dit kan een rijkskader zijn of good practices op het gebied van cloud. Op het eind van deze bijlage is het overzicht hiervan opgenomen. Kolom **Norm** geeft vanzelfsprekend de norm. Kolom **Inspectiestappen** geeft onze toetsrichting aan met onderscheid in de opzet en het bestaan van beheersmaatregelen.

Hoofdvraag 2: *In hoeverre zijn de soevereiniteit, de continuïteit van de dienstverlening en de gegevensbescherming gewaarborgd voor 3 geselecteerde public cloud-contracten?*

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
S1	Afsluiten contract	BZK Implementatiekader cloud	Het afsluiten van het contract is voorafgegaan door een risico-afweging. In het contract is opgenomen welke functionarissen van de CSC en de CSP verantwoordelijk zijn voor het beheer van het contract.	**Opzet** 1. Stel vast dat de CSC een risico-afweging heeft opgesteld voor de af te nemen clouddienst. 2. Stel vast dat de CSC de keten van betrokken partijen voor de dienst-verlening tot en met de CSP inzichtelijk heeft. 3. Stel vast dat in de contractuele afspraken de rollen en verantwoorde-lijkheden van de CSC, CSP en andere ketenpartijen over het beheer van het contract zijn opgenomen. **Bestaan** 1. Stel vast dat de CSC heeft vastgesteld dat voor de belangrijkste risico's in het contract maatregelen zijn opgenomen. 2. Stel vast dat eventuele wijzigingen in het contract zijn plaatsgevonden conform de afgesproken rollen en verantwoordelijkheden.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
S2	Interoperability & Portability	CCM IPY-01	Interoperabiliteit en portabiliteit zijn opgenomen in de cloud service-overeenkomst, waarbij afspraken zijn opgesteld voor: a. Rollen en verantwoordelijkheden van de CSP en de CSC over interoperabiliteit en portabiliteit; b. Interoperabiliteit van gegevens-uitwisseling en -verwerking; c. Portabiliteit van cloudsystemen.	**Opzet** 1. Stel vast dat de contractuele afspraken rondom rollen en verantwoordelijkheden van de CSP en de CSC over interoperabiliteit en portabiliteit zijn vastgelegd. 2. Stel vast dat in het contract is vastgelegd op welke wijze inter-operabiliteit van gegevens-uitwisseling en -verwerking is gewaarborgd. 3. Stel vast dat in het contract is vastgelegd op welke wijze porta-biliteit van cloudsystemen is gewaarborgd. **Bestaan** 1. Stel vast dat de CSP periodiek rapporteert aan de CSC over status en wijzigingen over interoperabiliteit en portabiliteit. 2. Stel vast dat de CSC periodiek de interoperabiliteit van gegevens-uitwisseling en -verwerking test. 3. Stel vast dat de CSC periodiek de portabiliteit van cloudsystemen test.
S3	Interoperability & Portability	CCM IPY-04; SWIPO CCCDPCSS 4.4; SWIPO CCCDPCSS 5.7; SWIPO CCCDPCSS 5.16	Toegang van CSCs tot gegevens bij beëindiging van het contract zijn opgenomen in de cloud service-overeenkomst en omvatten: a. Gegevensformaat conform Open Standaarden; b. Tijdsperiode waarin gegevens worden opgeslagen; c. Scope van de gegevens die worden bewaard en ter beschikking gesteld van de CSCs; d. Beleid voor het verwijderen van gegevens; e. Versleuteling van het export-bestand.	**Opzet** 1. Stel vast dat in het contract afspraken zijn vastgelegd over toegang van de CSC tot gegevens bij beëindiging van het contract, met tenminste afspraken over a t/m e uit de norm. **Bestaan** 1. Stel vast dat de CSC vaststelt dat de CSP periodiek aantoont dat aan de afspraken a t/m e is voldaan.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
S4	Interoperability & Portability	EDPS	De CSP moet waarborgen en aantonen dat de gegevens van de CSC vanuit zijn systemen en elk subverwerkend systeem binnen de in de cloud serviceovereenkomst afgesproken tijd en formaat overdraagbaar zijn naar andere CSPs, naar de keuze van de CSC.	**Opzet** 1. Stel vast dat in het contract afspraken, inzake tijd en formaat, zijn vastgelegd over het overdragen van gegevens van de CSC naar andere CSPs. **Bestaan** 1. Stel vast dat de CSC vaststelt dat de CSP periodiek aantoont dat aan de afspraken over tijd en formaat is voldaan. 2. Stel vast dat de CSC vaststelt dat de gegevens overdraagbaar zijn naar een andere CSP.
S5	Disclosure notification	CCM DSP-18	De procedure om verzoeken om openbaarmaking van persoonsgegevens door wetshandhavingsautoriteiten te beheren en te beantwoorden overeenkomstig de toepasselijke wet- en regelgeving is door de CSP opgesteld en aan de CSC gecommuniceerd. De CSP belicht daarbij de kennisgevingsprocedure aan geïnteresseerde CSCs, tenzij anderszins verboden, zoals een verbod op grond van het strafrecht om de vertrouwelijkheid van een rechtshandhavingsonderzoek te bewaren.	**Opzet** 1. Stel vast dat de rollen en verantwoordelijkheden van de CSP en de CSC over verzoeken om openbaarmaking van persoonsgegevens door wethandhavingsautoriteiten in het contract zijn vastgelegd. 2. Stel vast dat de kennisgevingsprocedures aangaande openbaarmaking van persoonsgegevens in het contract zijn vastgelegd. **Bestaan** 1. Stel vast dat in het geval van openbaarmaking van persoonsgegevens door wetshandhavingsautoriteiten de kennisgevingsprocedures zijn nageleefd.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
S6	Data Location en Data Flow	CCF 79; CCM DSP-19; CCF 114; CCM DSP-05	- De CSC identificeert geografische gebieden met risico's op het gebied van wet- en regelgeving, zoals landen onder embargo. - De CSP heeft procedures en maatregelen gedefinieerd om de fysieke locaties van gegevens te specificeren en te documenteren, inclusief locaties waar gegevens worden verwerkt of geback-upt. - De CSP draagt alleen gegevens van de CSC over naar een land buiten de Europese Economische Ruimte (EER), indien dit is overeengekomen als onderdeel van de Cloud Serviceovereenkomst. - Documentatie over gegevensstromen zijn aanwezig om te bepalen welke gegevens waar worden verwerkt, opgeslagen of verzonden.	**Opzet** 1. Stel vast dat de CSC de geografische risicogebieden heeft geïdentificeerd voor gegevensverwerking en -opslag. 2. Stel vast dat in het contract de fysieke locaties van gegevensverwerking, -opslag en back-ups zijn gedocumenteerd. 3. Stel vast dat in het contract afspraken zijn gemaakt over de overdracht van gegevens van de CSC naar landen buiten de EER. 4. Stel vast dat de CSC de gegevensstromen (verzending, verwerking en opslag) heeft gedocumenteerd. **Bestaan** 1. Stel vast dat de CSC vaststelt dat gegevensverwerking, -opslag en back-ups alleen op de gedocumenteerde fysieke locaties plaatsvindt.
S7	Right to audit	CCF 3; DEDPS	Procedures met betrekking tot audits op verzoek van de CSC zijn gedefinieerd, gedocumenteerd en transparant gecommuniceerd naar de CSC en, indien van toepassing, de gemandateerde auditor.	**Opzet** 1. Stel vast dat het right to audit bij de CSP en mogelijke subverwerkers en de voorwaarden waaronder kosten en termijn in het contract zijn opgenomen. **Bestaan** 1. Stel vast dat het right to audit in de praktijk toegepast kan worden.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
C1	Business Continuity Management and Operational Resilience en Multi-Location Strategy	CCM BCR-01 CCM BCR-02 CCM BCR-03 CCM BCR-04 CCM BCR-06 CCM BCR-09 CCM BCR-10 CCF 19	De CSC en CSP hebben procedures en maatregelen gedefinieerd voor business continuity management en omvatten: - een risicoanalyse ten grondslag aan de procedure; - een business continuity plan; - business continuity testen; - disaster recovery plan; - disaster recovery testen. De cloud serviceovereenkomst omvat afspraken over een multi-locatie- of regiostrategie voor productieomgevingen om de activiteiten op andere CSP-faciliteiten te kunnen hervatten indien een faciliteit uitvalt.	**Opzet** 1. Stel vast dat de rollen en verantwoordelijkheden van de CSP en de CSC over BCM in het contract zijn vastgelegd. 2. Stel vast dat in het contract de procedures en maatregelen over BCM zijn vastgelegd, waaronder: risicoanalyse, business continuity plan en testen, disaster recovery plan en testen en multi-locatie- of regiostrategie een onderdeel zijn van BCM. **Bestaan** 1. Stel vast dat de CSC een risicoanalyse voor BCM hebben opgesteld. 2. Stel vast dat de BCP is vastgesteld, gecommuniceerd en periodiek wordt geëvalueerd en bijgesteld. 3. Stel vast dat business continuity testen het afgelopen jaar hebben plaatsgevonden. Tijdens de test zijn de locaties uit de multi-locatie strategie meegenomen. 4. Stel vast dat het disaster recovery plan is vastgesteld, gecommuniceerd en periodiek wordt geëvalueerd en bijgesteld. 5. Stel vast dat disaster recovery testen het afgelopen jaar hebben plaatsgevonden. 6. Stel vast dat de multi-locatie- of regiostrategie periodiek worden getest tijdens BCM-testen, disaster recovery testen en back-up testen.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
C2	Back-up en data replicatie	CCM BCR-08 en CCF 23	De cloud serviceovereenkomst omvat afspraken over verantwoordelijkheden ten aanzien van het maken van regelmatige back-ups van gegevens die in de cloud zijn opgeslagen. De cloud serviceovereenkomst omvat afspraken over replicatie naar een secundaire databank of datacenter	**Opzet** 1. Stel vast dat in de cloud service-overeenkomst de rollen en verantwoordelijken voor het maken van regelmatige back-up van gegevens zijn vastgelegd. 2. Stel vast dat in de cloud service-overeenkomst is vastgelegd op welke wijze periodiek het herstel van gegevens vanuit de back-up wordt getest. 3. Stel vast dat in de cloud service-overeenkomst is vastgelegd op welke wijze data replicatie naar een secundaire databank of datacenter plaatsvindt. **Bestaan** 1. Stel vast dat de CSC vaststelt dat back-up door de CSP zijn gemaakt conform de afspraken. 2. Stel vast dat de CSC het herstel van gegevens via een back-up periodiek test. 3. Stel vast dat de CSC vaststelt dat data replicatie heeft plaatsgevonden naar een secundaire databank of datacenter.
C3	Change management	CCM CCC-01 BIO 12.1.2	De cloud serviceovereenkomst omvat afspraken over het toepassen van wijzigingen op bedrijfsmiddelen, waaronder applicaties, systemen, infrastructuur, configuratie, enz. Daarbij zijn verantwoordelijkheden expliciet gemaakt.	**Opzet** 1. Stel vast dat de rollen en verantwoordelijkheden van de CSP en de CSC aangaande change management in het contract zijn vastgelegd. 2. Stel vast dat in het contract het change management proces is beschreven. **Bestaan** 1. Stel voor een aantal wijzigingen vast dat deze wijzigingen conform de rollen, verantwoordelijkheden en proces heeft plaatsgevonden.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
C4	Security Incident Management, E-Discovery, & Cloud Forensics	CCM SEF-03	De klant en CSP hebben procedures en maatregelen gedefinieerd voor security incident respons en omvatten: - betrokken partijen; - relevante bedrijfskritische relaties (zoals toeleveringsketen) die kunnen worden geraakt.	**Opzet** 1. Stel vast dat de rollen en verantwoordelijkheden van de CSP en de CSC aangaande security incident en event management in het contract zijn vastgelegd. 2. Stel vast dat in het contract het security incident en event management proces is beschreven. **Bestaan** 1. Stel voor een aantal incidenten vast dat deze incidenten conform de rollen, verantwoordelijkheden en proces heeft plaatsgevonden.
G1	Governance Management	CCF 115 CCM STA-01	De cloud serviceovereenkomst omvat afspraken over de rollen en verantwoordelijkheden van CSP en de CSC. In de overeenkomst zijn definities opgenomen, inclusief maar niet beperkt tot: - rollen en verantwoordelijkheden voor het verlenen van toegang en goedkeuring; - gebruik door (sub)leveranciers.	**Opzet** 1. Stel vast dat de rollen en verantwoordelijkheden van de CSP en de CSC aangaande gegevensbescherming in het contract zijn vastgelegd, betreffende; rollen en verantwoordelijkheden voor het verlenen van toegang en goedkeuring en gebruik door (sub) leveranciers. **Bestaan** 1. Stel vast dat conform de afgesproken rollen en verantwoordelijkheden toegang wordt verleend voor gegevens.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
G2	Cryptography, Encryption & Key Management - encryption algorithm	CCM CEK-03; CCM CEK-04 CCF 89	De cloud serviceovereenkomst omvat afspraken over versleutelings-algoritmen en sleutelbeheer die geschikt zijn voor gegevens-bescherming, rekening houdend met de classificatie van gegevens. De cloud serviceovereenkomst omvat afspraken over crypto-grafische bescherming voor 'data at rest' , 'data in motion' en 'data in use', met behulp van cryptografische bibliotheken die zijn gecertificeerd volgens goedgekeurde standaarden.	**Opzet** 1. Stel vast dat in het contract de classificatie van de gegevens is vastgelegd. 2. Stel vast dat in het contract afspraken zijn vastgelegd over het versleutelingsalgoritmen, versleutelingsstandaarden en sleutelbeheer, afgestemd op de classificatie van de gegevens. Stel vast dat dit zowel is vastgelegd voor 'data at rest' , 'data in motion' als 'data in use'. **Bestaan** 1. Stel vast dat CSC heeft vast-gesteld dat een versleutelings-algoritme/encryptietechnologie wordt toegepast, in overeen-stemming met het contract. 2. Stel vast dat de CSC heeft vastgesteld dat sleutelbeheer plaatsvindt in overeenstemming met de afspraken in het contract.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
G3	Identity & Access Management	CCM IAM-01 CCM IAM-02 CCM IAM-08 CCF 164 BIO 9.2.2 BIO 9.2.3 BIO 9.4.3	De cloud serviceovereenkomst omvat afspraken over taken, rollen, bevoegdheden en verantwoordelijkheden aangaande toegangsbeheer bij de klant en CSP. De cloud service overeenkomst en omvat tevens afspraken over: - identificatie en authenticatie; - wachtwoordbeleid; - 'least privilege' en functiescheiding; - speciale toegangsrechten, waaronder hoog geprivilegieerde accounts: - toegang en gebruik van leveranciersaccounts uitsluitend gedurende de periode die nodig is en monitoring tijdens gebruik.	**Opzet** 1. Stel vast dat in het contract afspraken zijn vastgelegd over taken, rollen, bevoegdheden en verantwoordelijkheden over toegangsbeheer bij de CSC en CSP. 2. Stel vast dat in het contract afspraken zijn vastgelegd over minimaal: - identificatie en authenticatie; - wachtwoordbeleid; - 'least privilege' en functiescheiding; - Speciale toegangsrechten, waaronder hoog geprivilegieerde accounts; - toegang en gebruik van leveranciersaccounts uitsluitend gedurende de periode die nodig is en monitoring tijdens gebruik. **Bestaan** 1. Stel vast dat door de CSC en CSP toegangsbeheer is uitgevoerd conform de in het contract vastgelegde afspraken over taken, rollen, bevoegdheden en verantwoordelijkheden. 2. Stel vast dat de CSC vaststelt dat in de praktijk aan de contractvoorwaarden wordt voldaan, waaronder identificatie en authenticatie, wachtwoordbeleid, least privilege en functiescheidingen, speciale toegangsrechten met hoog geprivilegieerde accounts en toegang en gebruik van leveranciersaccounts uitsluitend gedurende de periode die nodig is en monitoring tijdens gebruik.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
G4	Supply Chain Management, Transparency, and Accountability	CCM STA-08	Het cloud contract omvat afspraken over het periodiek beoordelen van risicofactoren gerelateerd aan de organisaties binnen de toeleverings-keten.	**Opzet** 1. Stel vast dat in het contract is vastgelegd op welke wijze en door wie een periodieke beoordeling plaatsvindt van risicofactoren gerelateerd aan de organisaties binnen de toeleveringsketen. Dit vindt tenminste iedere 3 jaar plaats of bij wezenlijke wijzigingen in de clouddienstverlening of risico-factoren. **Bestaan** 1. Stel vast dat de CSC een periodieke beoordeling heeft uitgevoerd van risicofactoren gerelateerd aan de organisaties binnen de toeleveringsketen. 2. Stel vast dat de periodieke beoordeling binnen 3 jaar heeft plaatsgevonden of bij wezenlijke wijzigingen in de clouddienst-verlening of risicofactoren.
G5	Threat & Vulnerability Management	CCM TVM-01	Het cloud contract omvat afspraken over vulnerability management: - detect vulnerability; - assess the risk; - prioritize remediation; - confirm remediation.	**Opzet** 1. Stel vast dat in het cloud contract afspraken zijn vastgelegd over taken, rollen, bevoegdheden en verantwoordelijkheden aangaande vulnerability management. **Bestaan** 1. Stel vast dat de CSC vaststelt dat kwetsbaarheden van de cloud omgeving periodiek worden gemonitord en dat de geïdentifi-ceerde kwetsbaarheden en verbetermaatregelen adequaat worden opgevolgd.

Nr.	Onderwerp	Bron + Control ID	Norm	Auditstappen
G6	Infrastructure & Virtualization Security	CCM IVS-06	Het cloud contract omvat afspraken over de inrichting van applicaties en infrastructuur, waarbij toegang van de verschillende klanten tot services en resources binnen een cloud-omgeving: - op de juiste manier zijn gesegmenteerd en gescheiden; - worden gemonitord; - niet toegankelijk is vanuit andere klanten.	**Opzet** 1. Stel vast dat in het cloud contract afspraken zijn vastgelegd over de inrichting van applicaties en infrastructuur, waarbij toegang van de verschillende klanten tot services en resources binnen een cloud-omgeving: - op de juiste manier zijn gesegmenteerd en gescheiden; - worden gemonitord; - niet toegankelijk is vanuit andere klanten. **Bestaan** 1. Stel vast dat de CSC vaststelt dat de cloudomgeving is gesegmenteerd en gescheiden voor verschillende klanten. 2. Stel vast dat is gemonitord dat klanten alleen toegang hebben gekregen hebben tot services en resources in de voor hen bestemde cloudomgeving. 3. Stel vast dat andere klanten geen toegang hebben tot services en resources die niet voor hen bestemd zijn (= doorbreking segmentering).

Uitwerking kolom Bron + Control ID

Bij dit normenkader hebben we gebruikgemaakt van verschillende bronnen, met waar mogelijk de specifieke verwijzing naar het kenmerk (control ID):

- CCM: Cloud Control Matrix (CCM, versie 4.0.7).
  Bron: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.
- CCF: Cisco Cloud Controls Framework (CCF, Public Release V2.0). Bron: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html
- SWIPO: Converged Code of Conduct for Data Portability and Cloud Service Switching (versie 2023 - v.1) SWIPO, Switching Cloud Providers and Porting Data is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes). Bron: https://swipo.eu/wp-content/uploads/2023/06/SWIPO_AISBL_ConvergedCode-v1._29.03.2023_For-publication_Final.pdf
- BIO: Baseline Informatiebeveiliging Overheid (BIO versie 1.04);
- BZK implementatiekader Cloud 2022;
- European Data Protection Supervisor - Guidelines on the use of cloud computing services.

Gebruikte afkortingen in het normenkader

- CSC: Cloud service consumer. De afnemer van de clouddienstverlening, in dit geval het verantwoordelijke ministerie.
- CSP: Cloud service provider. In dit geval de aanbieder van de onderliggende cloud-dienst, de hyperscalers.
- Keten: Met de keten bedoelen wij de CSC, CSP en mogelijke tussenpartijen en resellers (die ook als deel-CSP's zijn te zien).

Bijlage 3 Lijst geïnterviewde organisaties

Naast het houden van interviews op alle ministeries en bij enkele gecontroleerde uitvoeringsorganisaties, spraken wij met functionarissen met cloudexpertise van de volgende partijen. Vanwege privacy-redenen worden de namen van de functionarissen niet genoemd, anders dan bij 2.

In alfabetische volgorde:

1. Autoriteit Persoonsgegevens
2. Bert Hubert (entrepreneur & software developer, zie https://berthub.eu/)
3. Cyber Security Raad (CSR)
4. Dictu
5. European Commission, Directorate-General Communications Networks, Content and Technology (DG CNET)
6. European Data Protection Board (EDPB)
7. European Union Agency for Cybersecurity (ENISA)
8. EY
9. Forum Standaardisatie
10. Nationaal Bureau voor Verbindingsbeveiliging (NBV).
11. Nationaal Cyber Security Centrum (NCSC)
12. ODC-Noord
13. SSC-ICT
14. Thales

Bijlage 4 Begrippen en afkortingenlijst

In deze bijlage hebben wij begrippen en afkortingen die in dit rapport voorkomen, omschreven en nader toegelicht. Ook is de bron weergegeven van de omschrijving.

AWS – Amazon Web Services (AWS) is een bedrijfsonderdeel van het Amerikaanse bedrijf Amazon.com dat voorziet in webdiensten en cloudcomputing. Bron: Wikipedia

Azure – Microsoft Azure Platform is een cloudcomputingplatform van het Amerikaanse bedrijf Microsoft waarmee een aantal internetdiensten aangeboden kan worden via het internet of binnen de omgeving van de organisatie. Bron: Wikipedia

Business continuity management – Business continuity management (BCM) (bedrijfscontinuïteitsbeheer) is het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de uitwerking op de operatie van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. BCM biedt een kader om tegen deze bedreigingen weerstand te bieden onder andere door effectief te kunnen reageren. Bron: Wikipedia

Change management – De procedure die beschrijft hoe de afhandeling, dus het indienen, de analyse en de besluitvorming, van wijzigingsvoorstellen wordt geborgd. Dit kunnen wijzigingen zijn op het gebied van de applicatie of het platform of infrastructuur. Bron: Internet

Cloudcomputing – Cloudcomputing is een model voor alomtegenwoordige, gemakkelijke, on-demand netwerktoegang tot een gedeelde pool van configureerbare computerbronnen (bijv. netwerken, servers, opslag, toepassingen en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale beheerinspanning of interactie met de serviceprovider. Bron: NIST

Cloud service consumer (CSC) – De afnemer van de clouddienstverlening, in dit geval het verantwoordelijke ministerie. Bron: Algemene Rekenkamer

Cloud servicemodellen – De 3 belangrijkste servicemodellen voor de cloud zijn Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). Elk servicemodel voorziet in de behoeften van verschillende gebruikers en organisaties en biedt een verschillende mate van controle, beveiliging en schaalbaarheid.

Zie ook de definities van de specifieke servicemodellen, Community cloud en Hybrid cloud. Bron: Internet

Cloud service provider (CSP) – De aanbieder van de onderliggende clouddienst, in dit geval de hyperscalers. 2 bekende hyperscalers zijn AWS en Azure. Zie ook: AWS, Azure en hyperscaler. Bron: Algemene Rekenkamer

Community cloud – De cloudinfrastructuur wordt geleverd voor exclusief gebruik door een specifieke gemeenschap van afnemers van organisaties die gemeenschappelijke belangen hebben (bijv. missie, beveiligingsvereisten, beleid en nalevingsoverwegingen). De infrastructuur kan eigendom zijn van, beheerd en geëxploiteerd worden door een of meer organisaties in de gemeenschap, een derde partij of een combinatie daarvan, en kan zich op of buiten de locatie bevinden.
Zie ook: Cloud servicemodellen en Hybrid cloud. Bron: NIST

Continuïteit van dienstverlening – Het aanbieden van diensten aan de maatschappij komt niet in gevaar. 2 belangrijke begrippen die hieronder vallen:

- *Interoperabiliteit*. Dit is het vermogen van IT-systemen om samen te werken met andere IT-systemen, waardoor data kan worden uitgewisseld en verder kan worden verwerkt. Gebruik van open standaarden en open source zijn hierbij belangrijk.
- Voorkomen van *vendor lock-in*: het (te) afhankelijk worden van 1 leverancier. Belangrijk hierbij is portabiliteit; data kan worden overgezet naar een andere leverancier en een realistische exitstrategie is aanwezig.

Bron: Algemene Rekenkamer

Cryptografie – Cryptografie wordt gebruikt om gegevens over te dragen die niet leesbaar mogen zijn door andere partijen. Alleen de ontvanger – en eventueel ook de zender – beschikt over de juiste sleutel om de te ontcijferen gegevens in hun originele vorm te herstellen. Bron: Wikipedia

Dienstaanbieder – Organisatie die een cloudapplicatie aanbiedt. Bron: Algemene Rekenkamer

Disclosure notification – Kennisgeving van openbaarmaking door cloud service provider. Procedures voor kennisgeving van openbaarmaking zijn relevant wanneer:

- wetshandhavingsinstanties toegang vragen tot persoonlijke gegevens die in de cloud zijn opgeslagen;

- juridische procedures of officiële onderzoeken de openbaarmaking van klantgegevens vereisen;
- dagvaardingen of gerechtelijke bevelen de clouddienstverlener dwingen gegevens te verstrekken aan bevoegde partijen.

Bron: Internet

Europese Economische Ruimte (EER) – Bij de Europese Economische Ruimte (EER) horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland. Bron: Internet

Gegevensbescherming – Voldoende bescherming van de gegevens. Bij de public cloud ligt het eigenaarschap van software en hardware en soms ook gegevens meestal niet bij de overheidsorganisatie zelf. Beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens zijn dan belangrijk. Bron: Algemene Rekenkamer

Hybrid cloud – Een hybrid cloud is een samenstelling van 2 of meer afzonderlijke cloudinfrastructuren (private, community of public). Deze blijven unieke entiteiten, maar zijn met elkaar verbonden door gestandaardiseerde of bedrijfseigen technologie die overdraagbaarheid van gegevens en toepassingen mogelijk maakt (bijv. cloud bursting voor het verdelen van de belasting tussen clouds). Zie ook: Cloud servicemodellen en Community cloud. Bron: NIST

Hyperscaler – Bedrijf dat hyperscale computing aanbiedt. Hyperscale computing is nodig om een robuust en schaalbaar cloud-, big data-, map reduce- of gedistribueerd opslagsysteem te bouwen en wordt vaak geassocieerd met de infrastructuur die nodig is om grote gedistribueerde sites zoals Google, Facebook, Twitter, Amazon, Microsoft, IBM Cloud of Oracle te laten draaien. Zie ook: Cloud service provider (CSP). Bron: Wikipedia

Identity & access management – Identity and Access Management (IAM) is het beheer om ervoor te zorgen dat de juiste 'identiteiten' (denk daarbij vooral aan personen of computers), voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten. Bron: NORA

Infrastructure as a Service (IaaS) – Type cloud servicemodel. De mogelijkheid die aan de afnemer wordt geboden is het beschikbaar stellen van verwerkings-, opslag-, netwerk- en andere fundamentele computerbronnen waar de afnemer willekeurige software kan implementeren en uitvoeren, waaronder besturingssystemen en toepassingen. De afnemer beheert of controleert de onderliggende cloud-infrastructuur niet, maar heeft controle over besturingssystemen, opslag en

ingezette toepassingen; en mogelijk beperkte controle over bepaalde netwerk-componenten (bijv. host firewalls). Zie ook: Cloud servicemodellen. Bron: NIST

Leveranciersketen (supply chain) – Een supply chain is de keten van diensten, materialen en informatie van leveranciers via een bedrijf naar zijn klanten. In deze keten wordt van een grondstof door meerdere bedrijven een product gemaakt en/of diensten geleverd. Als onderdeel van de keten verstaan wij de cloud service consumer (CSC), cloud service provider (CSP) en mogelijke tussenpartijen en resellers (die ook als deel-CSPs zijn te zien). Bronnen: Internet en Algemene Rekenkamer

Materieel cloudgebruik – Materieel public cloudgebruik is gebruik van public cloud-diensten voor het uitvoeren van de primaire taak van een organisatie. Met andere woorden, voor de organisatie is die (cloud)dienst van wezenlijk belang. Hieronder vallen ook de daarbij ondersteunende bedrijfsvoeringsprocessen, voor zover deze van wezenlijk belang zijn voor de primaire taken. Bron: BZK

Onderaannemer (subcontractor) – Een onderaannemer is een persoon of bedrijf die zich ertoe verbindt om een deel van of alle verplichtingen van een contract van een ander uit te voeren. Een onderaannemingscontract is een contract dat een deel van een bestaand contract aan een onderaannemer toewijst. Bron: Wikipedia

On-premise – On-premise software wordt geïnstalleerd en draait op de eigen hardware-infrastructuur van een organisatie en wordt lokaal gehost. Cloud software wordt daarentegen opgeslagen en beheerd op de servers van de provider en is toegankelijk via een webbrowser of een andere interface. Bron: Internet

Pentest – Een penetratietest of pentest is een toets van een of meer computer-systemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken.
Kenmerk van een pentest is dat deze op verzoek, incidenteel wordt uitgevoerd. Een pentest is een combinatie van geautomatiseerde en handmatige testen. Zie ook: vulnerability management. Bronnen: Wikipedia en Algemene Rekenkamer

Platform as a Service (PaaS) – Type cloud servicemodel. De afnemer kan door hem gemaakte of aangeschafte applicaties implementeren op de cloudinfrastructuur met behulp van programmeertalen, bibliotheken, diensten en tools die door de aanbieder worden ondersteund. De afnemer beheert of controleert de onderliggende cloud-infrastructuur niet, inclusief netwerk, servers, besturingssystemen of opslag.

Wel heeft de afnemer controle over de ingezette applicaties en mogelijk configuratie-instellingen voor de applicatie-hosting omgeving. Zie ook: Cloud servicemodellen. Bron: NIST

Private cloud – De cloudinfrastructuur wordt geleverd voor exclusief gebruik door één organisatie met meerdere afnemers. De infrastructuur kan eigendom zijn van, beheerd worden door en geëxploiteerd worden door de organisatie, een derde partij of een combinatie daarvan, en kan zich op of buiten de locatie bevinden. Bron: NIST

Public cloud – De cloudinfrastructuur is beschikbaar voor open gebruik door het algemene publiek. De infrastructuur kan eigendom zijn van, beheerd en geëxploiteerd worden door een zakelijke, academische of overheidsorganisatie, of een combinatie daarvan. De infrastructuur bestaat op het terrein van de cloudaanbieder. Bron: NIST

Reseller – Een reseller is een organisatie die door een cloud service provider is gemachtigd tot de wederverkoop van licenties. Een reseller kan door een cloud service consumer worden ingeschakeld om te helpen de clouddienst aan te kopen/te implementeren. Bron: Algemene Rekenkamer

Right-to-audit – Een bepaling in een contract die een partij het recht geeft om een andere contractpartij te controleren. Deze controle of audit gebeurt veelal door een onafhankelijke derde partij. Bron: Internet

Risicoafweging – Een risicoafweging is een methode waarbij strategische risico's van cloudgebruik worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg. Een risico-afweging moet plaatsvinden voordat de organisatie voor cloudgebruik kiest.
Bron: Algemene Rekenkamer

Risicoanalyse – Een risicoanalyse is een methode waarbij operationele risico's van cloudgebruik worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg.
Een risicoanalyse moet plaatsvinden voordat de organisatie voor een specifiek cloudgebruik kiest. Bron: Algemene Rekenkamer

Security incident – Een (informatie)beveiligingsincident is een of meerdere (ongewenste of onverwachte) gebeurtenissen die een grote kans hebben op het bedreigen van de bedrijfsprocessen en/of een bedreiging vormen voor de beschik-baarheid, integriteit en/of vertrouwelijkheid van gegevens. Bron: Internet

SLM – Strategisch leveranciersmanagement is initiatiefnemer van rijksbrede contractafspraken en inkoopvoorwaarden voor software en clouddienstverlening. Deze afspraken landen in mantelovereenkomsten met IT-leveranciers. SLM is versnipperd. Zo is bijvoorbeeld voor de clouddiensten van Microsoft, Google Cloud en Amazon Web Services het ministerie van JenV verantwoordelijk. Voor Oracle is dit het ministerie van EZ (DICTU) en voor IBM is dit het ministerie van Financiën (Belastingdienst). Bron: SLM

Soevereiniteit (digitaal) – Het vermogen om autonoom te kunnen beslissen en handelen aangaande de essentiële digitale aspecten in economie, maatschappij en democratie. Dit betreft dus het gebruik en inrichting van digitale systemen en de daarmee gegenereerde en opgeslagen data en gerelateerde werkprocessen.
Bron: Algemene Rekenkamer

Software as a Service (SaaS) – Type cloud servicemodel. De afnemer kan gebruikmaken van de applicaties van de provider die draaien op een cloud-infrastructuur. De applicaties zijn toegankelijk vanaf verschillende client-apparaten via een thin client-interface, zoals een webbrowser (bijv. web-gebaseerde e-mail), of een programma-interface. De afnemer beheert of controleert de onderliggende cloudinfrastructuur niet, inclusief netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikersspecifieke applicatieconfiguratie-instellingen.
Zie ook: Cloud servicemodellen. Bron: NIST

Statelijke actoren – Statelijke actoren zijn landen die zich met digitale spionage-activiteiten richten op doelwitten binnen publieke en private sectoren in binnen- en buitenland. Hiervoor worden onder andere aanvallen op de digitale delen van de toeleveringsketens ingezet. In tegenstelling tot cybercriminelen, beschikken statelijke actoren veelal onbeperkt over tijd en geld om kwetsbaarheden uit te buiten.
Bron: Internet

Tenant – Een cloudtenant is een individu of organisatie die zich abonneert op en gebruikmaakt van services die worden geleverd door een cloudcomputing-platform. Deze services omvatten virtuele machines, opslag en software. Tenants delen dezelfde infrastructuur op een veilige, geïsoleerde manier. Bron: Internet

Virtuele machine – Een virtuele machine is een computerprogramma dat een computer nabootst, waar andere programma's op kunnen worden uitgevoerd.
Bron: Wikipedia

Vulnerability management – Kwetsbaarheidsbeheer is het proces van het identificeren, evalueren, behandelen en rapporteren van beveiligingskwetsbaarheden in systemen en de software die erop draait.
Kenmerk van een kwetsbaarheidstest (vulnerability scan) is dat deze veelal geautomatiseerd plaatsvindt en met een grote regelmaat. Dit in tegenstelling tot pentesten waar ook deels handmatig wordt getest en die meer incidenteel plaats-vinden. Zie ook: pentest. Bronnen: Internet en Algemene Rekenkamer

Bijlage 5 Literatuur

Autoriteit Persoonsgegevens (2022). *Inzet van Cloud Service Providers*. Kenmerk z2022-00846. Den Haag: eigen beheer.

Autoriteit Persoonsgegevens (2023). *Beleidsreactie Advies Autoriteit Persoonsgegevens inzake het Rijksbreed Cloudbeleid 2022*. Kenmerk 2023-000002846. Den Haag: eigen beheer.

ADR (2024). *Onderzoeksrapport Evaluatie public cloudbeleid Rijksoverheid*. Den Haag: eigen beheer.

Algemene Rekenkamer (2020). *Factsheets: Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek.* Den Haag: eigen beheer.

Algemene Rekenkamer (2024). *Focus op AI bij de rijksoverheid.* Den Haag: eigen beheer.

BZK (2021). *I-strategie Rijk 2021-2025.* Den Haag: eigen beheer.

BZK (2022). *Rijksbreed cloudbeleid 2022.* Tweede Kamer, vergaderjaar 2021-2022, 26 643, nr. 904.

BZK (2023a). *Beantwoording Schriftelijk overleg over het Rijksbreed cloudbeleid 2022.* Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 963.

BZK (2023b). *Implementatiekader risicoafweging cloudgebruik.* Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 964.

BZK (2023c). *Beleidsreactie op een brief van de AP.* Tweede Kamer, vergaderjaar 2022-2023, 26 64, nr. 965.

BZK (2023d). *Verzamelbrief Digitalisering december 2023.* Tweede Kamer, vergaderjaar 2023-2024, 26 643, nr. 1112.

BZK (2024a). *Informatie- en communicatietechnologie (ICT).* Tweede Kamer, vergaderjaar 2023-2024, 26 643, nr. 1149.

BZK (2024b). *Verzamelbrief Digitalisering juni 2024.* Tweede Kamer, vergaderjaar 2023-2024, 26 643, nr. 1197.

BZK (2024c). *Evaluatie Rijksbreed Cloudbeleid.* Tweede Kamer, vergaderjaar 2023-2024, 26 643, nr. 1225.

Clingendael (2024a). *Too late to act? Europe's quest for cloud sovereignty.* Den Haag: eigen beheer.

Clingendael (2024b). *Nederland en de EU: Zet in op cloudsoevereiniteit.* Den Haag: eigen beheer.

CSR (2021). *Nederlandse Digitale Autonomie en Cybersecurity.* CSR Advies 2021, nr. 3.

EZK (2023). *Agenda Digitale Open Strategische Autonomie.* Tweede Kamer, vergaderjaar 2023-2024, kenmerk 2023D42774.

EZK (2024). *Antwoord op vragen van de leden Kathmann, Six Dijkstra en Sneller over de verhuizing van het.nl domein.* Tweede Kamer, vergaderjaar 2023-2024, aanhangsel 1305.

Forum Standaardisatie (2024a). *Monitor Open Standaarden 2023.* Den Haag: eigen beheer.

Forum Standaardisatie (2024b). *Standaarden en standaardisatieactiviteiten voor clouddiensten.* Den Haag: eigen beheer.

ICTU (2024). *Monitor Open Standaarden.* Den Haag: eigen beheer.

Moerel en Timmers (2020). *Reflecties over digitale soevereiniteit, Preadvies Staatsrechtconferentie 2020.* Universiteit Utrecht: eigen beheer.

NCSC (2021). *(Publieke) clouddienstverlening: Enkele ervaringen uit onze cloud journey.* Den Haag: eigen beheer.

NCSC (2022). *Cloud Act requests (Memorandum of GreenbergTraurig to NCSC).* Den Haag: eigen beheer.

Bijlage 6 Eindnoten

1. De volledig uitgeschreven naam wordt niet meer gebruikt. Het CIBG is een agentschap van het ministerie van VWS. De naam CIBG stamt uit 2000 en staat voor Centraal Informatiepunt Beroepen Gezondheidszorg. Sindsdien heeft de organisatie veel meer taken gekregen en dekt de naam niet meer de lading. Daarom wordt alleen de lettercombinatie CIBG gebruikt.
2. Deze principes hebben we als Algemene Rekenkamer bepaald op basis van voor-onderzoek en eerdere IT-audits.
3. Zie bijvoorbeeld: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/
4. Zie bijvoorbeeld: https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers
5. Zie bijvoorbeeld: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ en https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/
6 Bronnen: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft, https://www.dictu.nl/strategisch-leveranciersmanagement-oracle en https://www.rijksoverheid.nl/documenten/publicaties/2023/08/31/strategisch-leveranciersmanagement-rijk-voor-ibm-en-red-hat
7. https://www.dutchitchannel.nl/research/421377/google-en-microsoft-groeien-het-sterkst-in-public-cloud-markt
8. Het aanbieden van clouddiensten door bijvoorbeeld een overheidsdienstencentrum is private cloud voor het Rijk als totaalorganisatie. In onze uitvraag aan ministeries en overzichten spreken we dan ook alleen over public, private en hybrid cloud.
9. Zie ook: Algemene Rekenkamer (2024). Focus op AI bij de rijksoverheid. Den Haag: eigen beheer.
10. Voor uitgebreidere verhandelingen over dit begrip verwijzen we naar recente rapporten van Clingendael (Clingendael, 2024a en 2024b).
11. Dit is een door ons licht aangepaste definitie uit Moerel en Timmers (2020).
12. Bron: https://e-estonia.com/solutions/e-governance/data-embassy/
13. Bronnen: https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/#backingupgovernment

14. Bronnen: https://www.interxion.com, https://eur-lex.europa.eu, https://www.legalz.nl/blog/cloud-act, https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa, https://sosafe-awareness.com/blog/privacy-shield-decision, https://www.agconnect.nl/artikel/ec-neemt-nieuwe-privacyregels-aan-voor-datadoorgifte-aan-vs, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
15. Bron: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
16. Zie bijvoorbeeld: https://www.dutchncca.nl/eu-cybersecurity-certification/cloud-services en https://ec.europa.eu/newsroom/cipr/items/713799/en
17. Het ministerie van Defensie valt buiten de scope van het Rijksbreed cloudbeleid, waardoor een aantal aspecten van dit onderzoek niet van toepassing is op dit ministerie.
18. Voor dit cloudoverzicht leverden we een template aan, waarin we een aantal kenmerken hebben uitgevraagd. Te weten: 1. Applicatie/clouddienst 2. Dienstaanbieder 3. Cloudprovider 4. Reseller 5. Contract(en) aanwezig? 6. Servicemodel (IaaS, PaaS, Saas) 7. Globale omschrijving clouddienstverlening 8. Globale omschrijving cloudgegevens 9. Public, hybrid of private cloud 10. Materieel cloudgebruik? 11. Geografische regio verwerking & opslag 12. Financiële omvang contract 13. Ingangsdatum contract 14. Verval-/einddatum contract 15. Risicoafweging gemaakt? 16. Is de afweging inclusief financiële aspecten (kosten/baten)?
    De exacte uitvraag was: “een cloudoverzicht van alle afgesloten cloud-contracten. Zowel publieke, hybride, als private clouddiensten. Zowel materieel als niet-materieel cloudgebruik. Voor het ministerie zowel als voor de onder directe verantwoordelijkheid van de minister vallende organisatieonderdelen, zoals agentschappen (maar dus geen zbo’s)”.
19. Uit I-strategie Rijk 2021-2025.
20. Inhoudelijk toetsten we of een strategische afweging ‘wel/niet naar de cloud gaan’ wordt gefaciliteerd en of de methodiek expliciet ingaat op cloud. Zie ook bijlage 2 voor ons uitgewerkte normenkader.
21. Te weten: 20 oktober 2022 inzake ‘Rijksbreed cloudbeleid’ en op 26 juni 2024 inzake ‘Inkoop- en aanbestedingsbeleid toeziend op hardware en software van de rijksoverheid’.
22. De volledig uitgeschreven naam wordt niet meer gebruikt, zie ook eindnoot 1.
23. Zie bijvoorbeeld: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/

24. Zie bijvoorbeeld: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ en https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/
25. Zie bijvoorbeelden: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/ en https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers
26. Zie bijlage 1 voor welke contracten en afspraken we concreet hebben getoetst voor deze 3 public cloud-diensten.
27. Bron: https://www.ssc-ict.nl/over-ssc-ict
28. De volledig uitgeschreven naam wordt niet meer gebruikt, zie ook voetnoot 1.
29 Bron: https://www.cibg.nl/onze-organisatie
30 Zie ook het onderzoek dat Forum Standaardisatie heeft laten uitvoeren: Standaarden en standaardisatieactiviteiten voor clouddiensten.
31. Zie bijvoorbeeld: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ en https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/
32. De volledig uitgeschreven naam wordt niet meer gebruikt, zie ook voetnoot 1.
33. We gebruiken de woorden clouddiensten, -applicaties, -implementaties, -toepassingen, -systemen, en -services afwisselend. Hiermee bedoelen we hetzelfde. Ook het woord cloudcontract gebruiken we: hiermee bedoelen we de voorgaande woorden, specifiek gecontracteerd.

Algemene Rekenkamer
Postbus 20015
2500 EA Den Haag
(070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

De tekst in dit document is vastgesteld op 19 december 2024. Dit document is op 15 januari 2025 aangeboden aan de Tweede Kamer.

Den Haag, januari 2025