Rapport voor

Ministerie van Binnenlandse Zaken

Verkenning Soevereine Cloud

Datum:	30 april 2026
Versie:	1.0
Opgesteld door:	Gartner
In samenwerking met:	Programma NDS Cloud

Samenvatting

Het geopolitieke klimaat en de groeiende zorgen over digitale soevereiniteit maken het gebruik van niet-Europese (met name Amerikaanse) clouddiensten steeds minder vanzelfsprekend. Het ontbreken van een gezamenlijke aanpak ten aanzien van het IT-landschap van de Nederlandse overheid leidt tot inefficiëntie en kwetsbaarheid.

Aan de hand van het EU Cloud Sovereignty framework heeft het NDS programma een soevereiniteitsambitie geformuleerd die gericht is op een zo hoog mogelijke mate van digitale soevereiniteit, waarbij continuïteit en vertrouwelijkheid van overheidsdienstverlening geborgd zijn. In het verlengde hiervan is Gartner verzocht de markt voor soevereine clouddiensten en strategische scenario's voor het realiseren van een soevereine clouddienst te verkennen.

De markt voor soevereine clouddiensten bevindt zich in een dynamische groeifase die door geopolitieke ontwikkelingen in een versnelling is gekomen. In deze markt ontplooien Europese en Nederlandse leveranciers en samenwerkingsverbanden verschillende initiatieven om tegenwicht te bieden aan de dominante positie van Amerikaanse hyperscalers en een antwoord te formuleren voor de gefragmenteerde markt. Hoewel de huidige Nederlandse overheidsdienstverlening nog sterk leunt op propriëtaire software, en daarmee met een technologische vendor lock-in kampt, bieden open-source oplossingen van Europese partijen een reële route naar het hoge soevereiniteitsniveau die de Nederlandse overheid ambieert.

Om de ambitie rondom digitale soevereiniteit van de Nederlandse overheid op gebied van cloud computing in de Nederlandse context te duiden en te concretiseren zijn vier scenario's uitgewerkt:

- Scenario A - *Nieuwe soevereine overheidsclouddienst*: een volledig nieuwe, centraal aangestuurde overheidscloud die los van de bestaande systemen wordt opgebouwd.
- Scenario B - M*odernisering bestaande overheidscloudinfrastructuur:* het moderniseren en centraal samenvoegen van de huidige, bestaande clouddiensten.
- Scenario C - *Nieuwe soevereine clouddiensten conform overheidsstandaarden*: een decentraal model waarbij de overheid enkel regisseur is en strikte technische standaarden en eisen oplegt waaraan meerdere (nieuwe) overheids- en marktpartijen moeten voldoen.
- Scenario D - Aansluitmodel voor clouddiensten onder overheidsregie: een decentraal 'marktplaats'-model waarbij bestaande infrastructuren van zowel overheid als marktpartijen worden gemoderniseerd en aangesloten onder overheidsregie

Ieder scenario kent zijn eigen voordelen, nadelen en risico's, en de optimale keuze wordt bepaald door vier kritieke factoren:

- *De vereiste snelheid van realisatie*: de keuze voor nieuwbouw of modernisering van bestaande infrastructuur bepaalt het tempo waarin aan alle eisen kan worden voldaan.
- *Het beschikbare budget*: het opbouwen van nieuwe platformen vergt aanzienlijk hogere initiële investeringen dan het moderniseren van bestaande diensten.
- *Het bepalen van een uniforme technologiestack*: de mate van uniformiteit fungeert als randvoorwaarde voor de haalbaarheid van scenario's die uitgaan van een centrale opzet.
- *De gewenste rol van de markt:* de keuze tussen overheidsregie of marktpartijen hangt samen met de gewenste balans tussen operationele ontzorging en de beheersing van soevereiniteit risico's.

Het ambitieniveau ten aanzien van de soevereine clouddienst ligt hoog en het betreft een complex vraagstuk. Dit betekent dat een significante voorinvestering nodig is. De realisatie van een soevereine clouddienst vereist een

gedegen implementatieplan dat op korte en lange termijn grote ambities vertaalt naar tastbare, gefaseerde en in scope afgebakende resultaten. Dit traject kan enkel slagen door serieuze bestuurlijke focus, de inzet van substantiële financiële middelen en de inrichting van centrale regievoering die inkoopkracht effectief bundelt.

Het realiseren van een soevereine overheidscloud vergt toewijding en daadkracht. Een zorgvuldige afweging van de scenario's is daarom nodig om tot een koers te komen die bijdraagt aan de strategische doelstellingen van de Nederlandse overheid. Het gekozen scenario dient geoperationaliseerd te worden door het operating model te ontwerpen, financieren en in te richten. Met het technisch detailontwerp wordt de architectuur ontworpen, uitgewerkt en vertaald naar een werkbaar fundament. Deze technische en organisatorische kaders vormen de basis voor een integrale implementatiestrategie. Afhankelijk van het gekozen scenario, kan vervolgens kan een gerichte aanbesteding worden gedaan om daadwerkelijke realisatie en ingebruikname tot stand te brengen.

Inhoudsopgave

1. Inleiding

Nederland is een van de meest gedigitaliseerde landen ter wereld[1][2]. De economie, zorg en publieke dienstverlening zijn verweven met digitale infrastructuren die ongekende kansen bieden voor innovatie en efficiëntie. Echter, deze verregaande digitalisering heeft als keerzijde een groeiende en kwetsbare afhankelijkheid van een beperkt aantal buitenlandse, vaak niet-Europese, technologieaanbieders. In een geopolitieke realiteit waarin data is uitgegroeid tot de kritieke infrastructuur van de digitale economie, kan de Nederlandse overheid het zich niet langer veroorloven om de controle over en continuïteit van haar meest kritieke overheidstaken uit handen te geven aan buitenlandse dienstverleners. Om deze autonomie te herstellen, zet de overheid met de strategie 'Samen Versnellen'[3] in op een overheidsbrede soevereine clouddienst.

De Nederlandse Digitaliseringsstrategie benadrukt het belang van samenwerken om weerbaarder te worden en versnippering tegen te gaan.[4] Deze centrale aanpak adresseert de huidige versnippering door een eenduidige werkwijze voor alle overheidsorganisaties, waardoor de afhankelijkheid van een klein aantal externe leveranciers wordt afgebouwd. Door te kiezen voor de meest passende soevereine oplossing borgt de overheid niet alleen de regie over vitale gegevens buiten de publieke cloud, maar stimuleert zij tegelijkertijd de Nederlandse dan wel Europese diensteneconomie.

Het Aanjaagteam Cloud binnen de Nederlandse Digitaliseringsstrategie (NDS) is gevraagd om te werken aan deze gezamenlijke koers. Het team werkt samen aan één opdracht: een verkenning van het realiseren van een overheidsbrede soevereine clouddienst in samenwerking met bestaande overheidsdienstverleners en de markt.[5]. Ter ondersteuning van dit proces is Gartner gevraagd om scenario's te schetsen en opties aan te dragen die helpen bij het bepalen van de strategische koers voor een soevereine overheidsclouddienst.

De overheidsbrede soevereine clouddienst moet niet gezien worden als een fysiek gebouw met servers waarop 'Overheidscloud' staat, maar als een gelaagd ecosysteem dat de volledige IT-infrastructuur van de overheid ondersteunt. Door te werken met verschillende niveaus, kan de beveiliging en opslag worden afgestemd op de gevoeligheid van specifieke data.[6]

Dit soevereiniteitsbesef past binnen een bredere, internationale trend waarbij overheden hun strategische afhankelijkheid verkleinen door vaker te kiezen voor IT-dienstverleners binnen de jurisdictie van Europa en/of Nederlands grondgebied. Gartner raamt de wereldwijde investeringen in soevereine cloudoplossingen voor 2026 op maar liefst 80 miljard dollar[7]. Tegen 2030 zal meer dan 75% van de organisaties in EMEA hun virtuele workloads migreren naar oplossingen die geopolitiek risico moeten verminderen, een stijging ten opzichte van minder dan 5% in 2025.

[1] IMD, IMD World Digital Competitiveness Ranking 2025

[2] CBS Digitalisering en kenniseconomie 2025

[3] Nederlandse Digitaliseringsstrategie, Samen versnellen; link

[4] Nederlandse Digitaliseringsstrategie, Samenversnellen, blz. 2; link

[5] Digitale Overheid, Samen bouwen aan een soevereine cloud voor de hele overheid; link

[6] Digitale Overheid, Samen bouwen aan een soevereine cloud voor de hele overheid; link

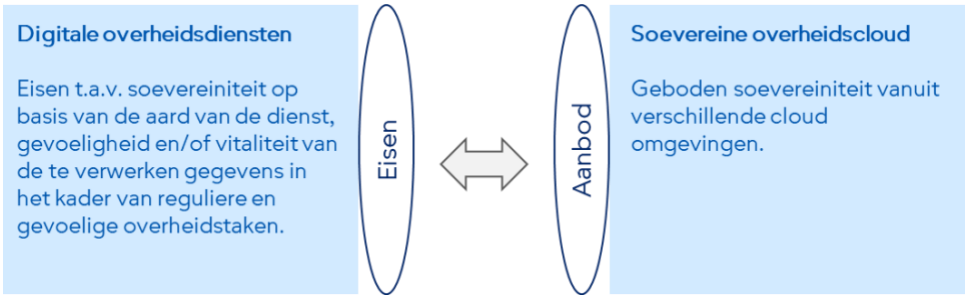
[7] Gartner says worldwide sovereign cloud IaaS spending will total 80$ billion in 2026; link

Om deze ontwikkeling te sturen heeft de Europese Commissie het EU Cloud Sovereignty Framework[8] ontwikkeld en beschikbaar gesteld. Dit raamwerk wordt reeds actief gebruikt, zoals bijvoorbeeld door het Directoraat-generaal Digitale Diensten van de EU in een recente aanbesteding[9].

Het EU Cloud Sovereignty Framework definieert de verschillende niveaus van digitale autonomie en soevereiniteit op basis van acht doelstellingen en bijbehorende attributen. Deze verkenning gebruikt het Europese soevereiniteitsraamwerk als basis om het ambitieniveau van de Nederlandse overheid te beschrijven.

Tijdens het schrijven van deze verkenning wordt er zowel op nationaal niveau als binnen het Europees parlement gewerkt aan nieuwe richtlijnen: de herziening van het Rijkscloudbeleid[10] en de Cloud and AI Development Act[11] van de EU. Deze beleidskaders bieden organisaties juridische en strategische handvatten om zowel het vereiste als het geboden soevereiniteitsniveau (zie figuur 1) van hun clouddiensten nauwkeurig te toetsen en verantwoordelijk in te kopen. Deze verkenning houdt rekening met deze ontwikkelingen en biedt een eerste basis voor een strategische inbedding ervan. Het kan gezien worden als een vertrekpunt voor de lange termijn-implementatie en uitrol van een soevereine overheidscloud.

Figuur 1 het vereiste en geboden soevereiniteitsniveau zijn beiden relevant



1.1. Totstandkoming van deze verkenning

Deze verkenning is uitgevoerd door Gartner Nederland B.V. (hierna genoemd als Gartner) in samenwerking met het programma NDS (i.c. het aanjaagteam en programmateam NDS Cloud) en CIO Rijk van het Ministerie van Binnenlandse Zaken. Gartner heeft een faciliterende, onderzoekende en adviserende rol. Het team van het Ministerie van Binnenlandse Zaken is bepalend t.a.v. de soevereiniteitsambitie en het beoordelen van scenario's.

1.2. Afbakening van de soevereine clouddienst

Om de diepgang en relevantie van deze marktbeschouwing te waarborgen, is de verkenning afgebakend langs technische, inhoudelijke en functionele lijnen. De focus ligt primair op de fundamenten van de cloud Infrastructure as a Service (IaaS) en Platform as a Service (PaaS)[12].

[8] European Commission, Directorate-General for digital services; Cloud Sovereignty Framework version 1.2.1 – Oct. 2025; link

[9] Aanbesteding om soevereine cloud diensten te werven voor EU-agentschappen; link

[10] Rijksbrede cloudbeleid 2022; link

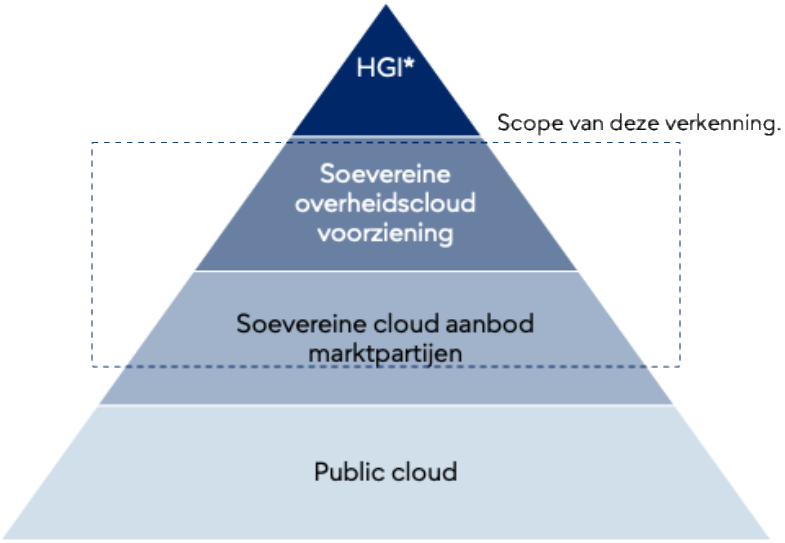
[11] EU Cloud and AI Development Act; link

[12] Container-as-a-Service (CAAS) wordt opgenomen als onderdeel van IaaS en PaaS.

Software as a Service (SaaS) valt nadrukkelijk buiten de scope van deze verkenning. Hoewel SaaS-oplossingen een groot deel van het applicatielandschap beslaan, richt deze verkenning zich op de onderliggende infrastructuur. Wel is van belang te vermelden dat de onderzochte IaaS- en PaaS-omgevingen (landing zones) in de toekomst als soeverein fundament moeten kunnen dienen voor het hosten van specifieke SaaS-applicaties, bijvoorbeeld voor digitale werkplekvoorzieningen.

De beoogde soevereine cloud is bedoeld voor de verwerking van informatie met het classificatieniveau tot en met Departementaal Vertrouwelijk (DV). Hoewel dit een begrip is dat oorspronkelijk bedoeld is voor de Rijksoverheid, wordt er in deze verkenning een pragmatische grens gesteld: de focus ligt op reguliere en gevoelige overheidstaken. Deze verkenning richt zich daarmee dus niet op informatie met een hoge rubricering (zoals staatsgeheim). In Figuur 2 worden de verschillende lagen in het cloud aanbod in functie van de informatieclassificatieniveaus weergegeven. De focus van dit onderzoek ligt specifiek op de tweede en derde laag. Hierbij is de analyse gericht op de technologische inrichting, met uitsluiting van de fysieke hardware.

Figuur 2 verschillende lagen in het cloud aanbod in functie van informatieclassificatieniveaus



*Hoog Gerubriceerde Informatie (HGI) betreft staatsgeheime of uiterst gevoelige data, waarvan openbaarmaking uitzonderlijk grote schade toebrengt aan de nationale veiligheid.

Het aanjaagteam cloud bevestigt[13] deze afbakening door het belang van business continuïteit en veilige opslag van data te benadrukken. Daarnaast geven de deelnemers aan dat de soevereine cloud 'alle primaire/operationele processen t.a.v. dataopslag, verwerking en programmatuur (t.b.v. de wettelijke taken)' moet kunnen faciliteren. Dit betreft een forse ambitie die getoetst moet worden op haal- en maakbaarheid, en middels een gefaseerd plan behapbaar dient te worden gemaakt.

1.3. Beperkingen van dit onderzoek

De gehanteerde uitgangspunten, ten aanzien van een soevereine clouddienst, in deze verkenning vormen een vertrekpunt dat is gebaseerd op inzichten uit interactieve werksessies met het NDS Cloud projectteam en het NDS

[13] Bron: werksessie met het Aanjaagteam NDS/Cloud d.d. 12 maart 2026.

Cloud Aanjaagteam. De uitgangspunten vormen daardoor geen uitputtende weergave van alle mogelijke overheidstaken en de daaruit voortvloeiende eisen aan clouddiensten.

De scenario's zijn op een hoog abstractieniveau gedefinieerd om de strategische koers te bepalen. Een gedetailleerde technische uitwerking of diepgaande architectuur valt buiten de scope van deze verkenning. Hierdoor is het mogelijk dat specifieke sub-scenario's of technische nuances niet expliciet zijn uitgelicht. Ook spreekt Gartner geen voorkeur uit voor een specifiek scenario en maakt ze geen keuzes namens het NDS Cloud team.

De classificatie van marktpartijen in de marktbeschouwing dient enkel ter illustratie van verschillende 'typen leveranciers'. De afwezigheid van een specifieke partij in de voorbeelden impliceert niet dat deze partij technisch of operationeel ongeschikt zou zijn voor het implementeren van de beschreven scenario's. Gartner heeft geen validatie of toets uitgevoerd of marktpartijen de geëvalueerde scenario's daadwerkelijk kunnen realiseren. De bevindingen zijn gebaseerd op de expertise van Gartner en openbaar beschikbare informatie.

De informatieverzameling die tijdens dit onderzoek is uitgevoerd (naast raadplegen van schriftelijke bronnen) is beperkt tot de werksessies met het NDS Cloud projectteam en het NDS Aanjaagteam. Er is geen aanvullend kwantitatief onderzoek (zoals enquêtes of externe consultaties buiten deze groepen) verricht om de resultaten te valideren. De conclusies zijn hiermee inherent verbonden aan de context en input van de betrokkenen tijdens de projectperiode.

1.4. Definities en afkortingen

Dit document bevat technische terminologie. Om de leesbaarheid te verhogen, worden de belangrijkste technische termen en definities in Tabel 1 toegelicht.

Tabel 1 technische definities en afkortingen

Term	Definitie
Cloud	Containerbegrip dat zowel kan verwijzen naar het leveren van Diensten via een cloudmodel als naar een specifieke instantie daarvan ("een cloud").
Cloud computing	Model dat het mogelijk maakt om • plaats- en tijdsonafhankelijk ("ubiquitous"), • op een gemakkelijke manier ("convenient), • op afroep ("on-demand"), • via een netwerk ("network access to") toegang te krijgen tot een voortdurend beschikbare gedeelde verzameling van configureerbare computing resources die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met cloudaanbieders dat voldoet aan vijf essentiële karakteristieken: • op afroep beschikbare selfservice; • breed beschikbare toegang via netwerken; • gedeelde computermiddelen; • gemeten dienstgebruik.

Clouddienst/cloud-voorziening	Afgebakend geheel van dienstverlening gebaseerd op cloud computing dat specifieke functionaliteit levert in antwoord op aanvragen van afnemers of van andere clouddiensten.
Soevereine clouddienst	Verzameling clouddiensten verankerd binnen de Europese jurisdictie die voldoet aan de eisen voor datalocalisatie en operationele autonomie. De soevereine cloud moet ervoor zorgen dat de data, activiteiten, infrastructuurcomponenten en technologie afgeschermd zijn van externe afhankelijkheden of juridische claims en beschermd zijn tegen directe invloed of toegang door overheden uit andere landen.
IaaS	Verzameling clouddiensten waarbij verwerking, opslag, netwerken en andere fundamentele computing resources worden aangeboden waarmee de klant willekeurige software kan implementeren en draaien, zoals operating systems en applicaties. De cloudafnemer voert geen beheer op de onderliggende infrastructuur noch op de interne werking van de geleverde clouddiensten. De cloudafnemer beheert de besturingssystemen, opslag en geïmplementeerde applicaties. De cloudafnemer beheert daarnaast mogelijk een beperkt deel van de netwerkcomponenten (bijvoorbeeld: firewalls).
PaaS	Verzameling van clouddiensten waarop de afnemer eigen gemaakte applicaties of aangekochte applicaties kan implementeren. De afnemer voert geen beheer op de interne werking van de clouddiensten zoals netwerk, servers, besturingssystemen of opslag. De afnemer heeft controle over de geïmplementeerde applicaties en mogelijke configuratie-instellingen voor de applicatie hosting omgeving.
SaaS	Verzameling clouddiensten in de vorm van een of meer voor eindgebruikers van de Afnemer. De Applicaties zijn toegankelijk vanaf verschillende clientapparaten via een thin-clientinterface, zoals een webbrowser (bijvoorbeeld webgebaseerde e-mail) of een programmainterface. De Cloudafnemer beheert of controleert de onderliggende infrastructuur niet, noch netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikerspecifieke applicatieconfiguratie-instellingen.

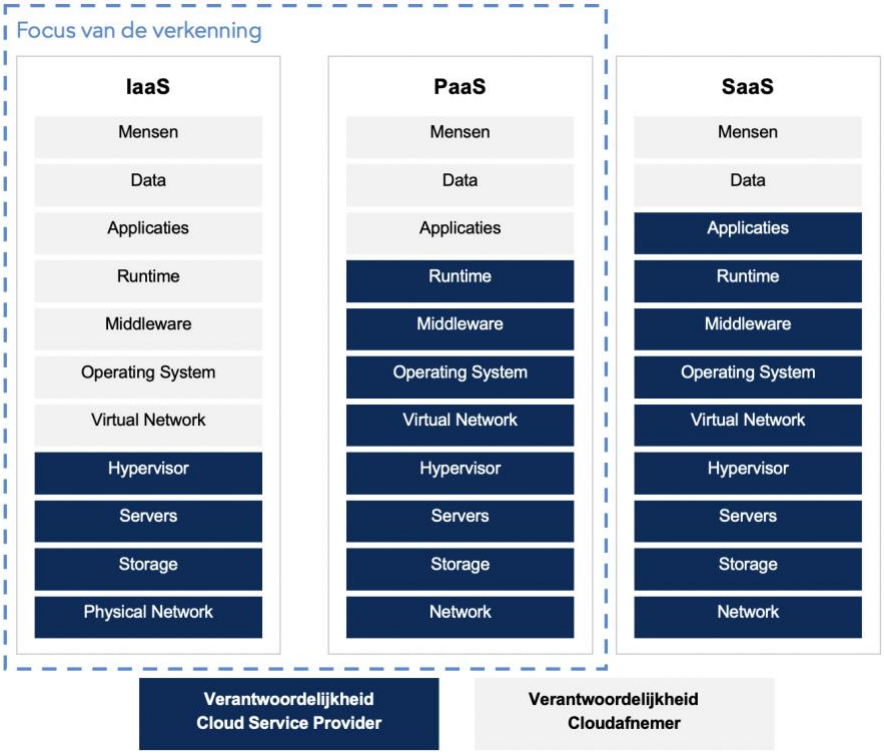
Voor de mogelijke samenwerking van de Nederlandse overheid met de markt om tot een soevereine clouddienst te komen zijn er meerdere rollen mogelijk waarin de marktpartijen kunnen opereren. Voor deze rollen worden de definities zoals opgenomen in Tabel 2 gebruikt.

Figuur 2 brengt een aantal van deze termen en rollen in relatie tot elkaar in de context van clouddienstverlening.

Tabel 2 aanvullende definities met betrekking tot mogelijk rollen marktpartijen

Term	Definitie
Cloud service provider	Een Cloud Service Provider (CSP) is een leverancier die uitgebreide cloud computing-diensten ontwikkelt, exploiteert en levert, waaronder Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS). In de context van soevereine clouddiensten voor overheidsinstanties zijn CSP's primair verantwoordelijk voor het ontwerpen van de technische architectuur en het waarborgen dat het cloud platform voldoet aan strenge lokale en regionale regelgeving. Om volledige soevereiniteit te bereiken, moeten CSP's verbeterde gegevensbeschermingsmaatregelen integreren, gegevensresidentiecontroles handhaven en op elk operationeel niveau op maat gemaakte beveiligingsprotocollen implementeren.
Cloud afnemer	Ook wel cloud consumer of cloudgebruiker genoemd; is een persoon of organisatie die een zakelijke relatie onderhoudt met een cloudaanbieder (cloud service provider) en gebruikmaakt van hun diensten.
Managed service provider	Managed service providers (MSP's) zijn leveranciers die uitbesteed beheer van cloudoperaties en aanvullende diensten aanbieden die ervoor zorgen dat de cloudomgeving veilig, compliant en met maximale efficiëntie draait. In de context van soevereine clouddiensten fungeren MSP's als de partij die het beheer van de cloudomgeving verzorgen namens de overheid.
System integrator	Systeemintegratoren (SI's) zijn gespecialiseerde leveranciers die zich richten op het integreren van uiteenlopende IT-componenten, legacy-systemen en clouddiensten in uniforme, interoperabele oplossingen die voldoen aan de specifieke operationele en regelgevende behoeften van klanten. Bij soevereine cloud-implementaties voor overheidsinstanties zijn SI's verantwoordelijk voor het realiseren van de clouddienst, waarna deze voor het beheer kan worden overgedragen aan de overheid dan wel een externe managed service provider.
Detachering	Aanbieders van detacheringsdiensten zijn gespecialiseerd in het aanbieden van gespecialiseerd en vaak tijdelijk personeel om tekorten aan capaciteit en kennis en vaardigheden binnen een organisatie op te vullen. Op het gebied van soevereine cloudimplementatie voor overheidsklanten leveren deze aanbieders cruciaal technisch talent dat mogelijk ontbreekt binnen het huidige personeelsbestand van de overheid. Hun focus ligt op het leveren van deskundige cloud-engineers, beveiligingsspecialisten en compliance-professionals die het ontwerp, de implementatie en de voortdurende verbetering van sovereign cloudoplossingen kunnen ondersteunen.

Figuur 3 verdeling verantwoordelijkheden clouddiensten



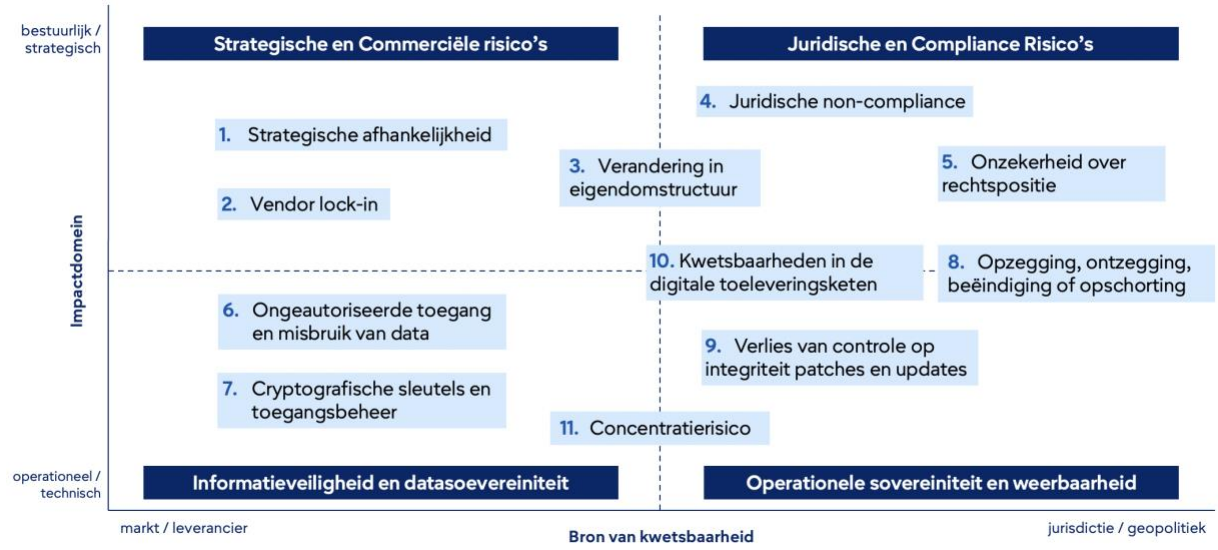
2. Risico's

In dit hoofdstuk worden de belangrijkste risico's, die de Nederlandse overheid met de overstap naar een soevereine cloud beoogt te mitigeren[14], toegelicht (zie Figuur 4). De kernvraag is hoe overheidstaken beschermd worden tegen een toenemende afhankelijkheid van niet-Europese mogendheden, terwijl de bedrijfscontinuïteit van overheidstaken naar de maatschappij geborgd blijft. Deze risico's variëren van het verlies van juridische controle over data tot de dreiging van een plotselinge onderbreking van de dienstverlening door geopolitieke verschuivingen of commerciële geschillen. De risico's geven invulling aan de redenen waarom een soevereine clouddienst voor de Nederlandse overheid nodig is. Dit hoofdstuk biedt daarmee ook input voor de ambitie ten aanzien van het soevereiniteitsniveau en de eisen waaraan een dergelijke voorziening moet voldoen.[15]

De afhankelijkheid van niet-Europese leveranciers/cloud providers brengt risico's met zich mee, maar ook het gebruik van meer soevereine alternatieven is niet vrij van risico's zoals bevestigd door Marktpartijen tijdens een door BZK uitgevoerde Open Dialoog[16]. Bijvoorbeeld, het niet kunnen benutten van innovaties, cybersecurity, schaalvoordelen en tekort aan kennis die nodig is voor beheer en exploitatie.

Deze risico's moeten tegen elkaar worden afgewogen en waar nodig en mogelijk worden voorzien van mitigerende maatregelen. Deze mitigerende maatregelen vormen input voor de eisen aan een toekomstige soevereine clouddienst voor de Nederlandse overheid. De risico's van meer soevereine oplossingen worden als onderdeel van de scenario's verder besproken in hoofdstuk 6.

Figuur 4 overzicht van risico's die de Nederlandse overheid met een soevereine cloud beoogt af te dekken



[14] Bron: werksessies met de NDS werkgroep en het aanjaagteam cloud

[15] Hoewel dit hoofdstuk risico's inzichtelijk maakt, is het bewust geen gedetailleerde, uitputtende risicoanalyse.

[16] Bron: NDS Cloud: verslag Open Dialoog; link

1. Strategische afhankelijkheid

Kwetsbaarheid	Gebruik van leverancier specifieke technologieën met beperkte interoperabiliteit en portabiliteit al dan niet in combinatie met grote volumes en langdurige contracten met mondiale cloudleveranciers.
Dreiging	Geopolitieke druk, zoals sancties, kan het gedrag van cloudleveranciers beïnvloeden.
Impact	De Nederlandse overheid heeft niet langer ondersteuning ten aanzien van functionele, technische en beveiligingsupdates als gevolg van geopolitiek ingegeven besluiten.

2. Vendor lock-in

Kwetsbaarheid	Gebruik van leverancier specifieke technologieën met beperkte interoperabiliteit en portabiliteit al dan niet in combinatie met grote volumes en langdurige contracten met mondiale cloudleveranciers.
Dreiging	Leveranciers kunnen hun dominante positie benutten door prijzen te verhogen, restrictieve voorwaarden op te leggen of hun diensten plotseling te wijzigen.
Impact	• Verminderde operationele flexibiliteit en kostbare migratie naar alternatieven. • Substantiële verhoging van de kosten door EU-importtarieven op technologiediensten vanuit de landen buiten de EU. • Substantiële verhoging van de kosten van clouddienstverlening door eenzijdige verhoging van prijzen door cloudleveranciers, gebruikmakend van vendor lock-in.

3. Verandering in eigendomsstructuur

Kwetsbaarheid	Marktpartijen die kritieke infrastructuur leveren kunnen worden overgenomen door buitenlandse partijen, waardoor de eigendomsstructuur verandert.
Dreiging	Verlies van controle over infrastructuur, risico op beïnvloeding door buitenlandse belangen, verminderde compliance met nationale eisen.
Impact	• Directe gevolgen voor soevereiniteit en continuïteit van dienstverlening. • Mogelijke noodzaak tot beëindiging samenwerking.

4. Juridische non-compliance

Kwetsbaarheid	De juridische opzet en technische implementatie van de dienstverlening maken het onmogelijk om aan de vereisten van Nederlandse en Europese wetgeving te voldoen.
Dreiging	Toezichthouders of gerechtelijke organisaties stellen een overtreding van Nederlandse of Europese wetgeving vast dan wel constateren het niet voldoen aan wettelijke eisen.

Impact	• Sancties door toezichthouders. • Mogelijke juridische geschillen wanneer data bij buitenlandse providers onder externe jurisdictie valt. • Gedwongen aanpassingen in contracten (mogelijk tegen hoge kosten en/of impact op de dienstverlening). • Juridische onzekerheid.

5. Onzekerheid over rechtspositie

Kwetsbaarheid	Verwachtingen ten aanzien van de juridische positie als afnemer zijn niet duidelijk door mogelijke toepasbaarheid van wetgeving uit meerdere landen en/of complexe structuren en constructen van contracten.
Dreiging	Leveranciers beroepen zich op andere wetgeving dan de Nederlandse/Europese wetgeving wat nadelig uitpakt voor de afnemer.
Impact	• Juridische geschillen en/of procedures. • Verminderde soevereiniteit door van toepassing blijken niet-Europese wetgeving. • Verminderde continuïteit van overheidstaken. • Verminderde vertrouwelijkheid van data.

6. Ongeautoriseerde toegang tot en misbruik van data

Kwetsbaarheid	Afhankelijkheid van digitale diensten die onder buitenlandse jurisdictie vallen.
Dreiging	Buitenlandse autoriteiten kunnen wettelijke bevoegdheden en sancties gebruiken om toegang tot data te verkrijgen, ongeacht de fysieke locatie van de data. Nederlandse dan wel Europese wetten bieden onvoldoende bescherming om dit tegen te gaan.
Impact	• Verplichte verstrekking incl. mogelijke openbaarmaking van gevoelige data, zelfs wanneer deze fysiek in eigen land is opgeslagen en zonder dat bekend wordt gemaakt dat toegang tot deze data is verschaft. • Geheime informatie (veiligheid, politiek, commercieel) komt in handen van buitenlandse mogendheden op basis van wettelijke mogelijkheden van overheden en verzwakt de positie van Nederland in het geopolitieke spectrum. • Persoonsgegevens komen in handen van buitenlandse mogendheden op basis van buitenwettelijke mogelijkheden (bijv. cybercriminaliteit of spionage) van overheden en maakt burgers kwetsbaar voor beïnvloeding. • Verminderd vertrouwen van burgers, bedrijven en andere overheden/partners. • Misbruik incl. schending auteursrechten bij gebruik van data van de Nederlandse overheid of andere Nederlandse partijen in AI-modellen in buitenlandse jurisdictie.

7. Beheer van cryptografische sleutels en toegangspaden

Kwetsbaarheid	Encryptiesleutels en identiteiten (beheerdersaccounts, directoryservices) worden gegenereerd of beheerd door niet-EU-aanbieders of personeel, waardoor zij technische mogelijkheden hebben om toegang te krijgen tot gegevens of de configuratie van systemen aan te passen.
Dreiging	Buitenlandse autoriteiten die de aanbieder dwingen sleutels af te staan, of insiders die beheerderstoegang misbruiken, mogelijk onder een zwijgbevel (zgn. “gag order”).
Impact	• Verlies van vertrouwelijkheid voor gevoelige datasets. • Onvermogen om geloofwaardig te beweren dat data beschermd is tegen buitenlandse toegang. • Mogelijke niet-naleving van de AVG en sectorspecifieke beveiligingsregels.

8. Ontzegging, beëindiging of opschorting van dienst

Kwetsbaarheid	De leverancier valt onder sancties van derde landen en exportcontroles, waarbij deze gedwongen kan worden (of ervoor kiest) om diensten op te schorten (voor een individu en, of organisatie).
Dreiging	Buitenlandse regeringen die sancties opleggen, of leveranciers die (te snel) aan verzoeken voldoen om hun eigen risico te verkleinen.
Impact	• Plotseling verlies van toegang tot kritieke systemen, records en communicatie. • Mogelijke operationele uitval, onvermogen om burgers te bedienen. • Politieke chantage en zelfcensuur als gevolg van deze mogelijkheid.

9. Verlies van controle op integriteit van patches en updates

Kwetsbaarheid	Updates voor besturingssystemen, SaaS en firmware worden ontworpen, ondertekend en verspreid door buitenlandse aanbieders met voor de Nederlandse overheid beperkte mogelijkheden om code te inspecteren of de release-timing te beïnvloeden. Dit geldt voor alle propriëtaire software en niet alleen voor de updates daarop.
Dreiging	Kwaadaardige of foutieve updates (of dat nu door compromittering, insiderbedreigingen of gehaaste releases komt) verspreiden zich snel naar kritieke overheidssystemen.
Impact	• Storingen, beveiligingsincidenten of verlies van data integriteit bij meerdere instanties tegelijk. • Nakoming van wettelijke verplichtingen in het geding.

10. Kwetsbaarheden in de digitale toeleveringsketen

Kwetsbaarheid	Digitale ecosystemen steunen op complexe mondiale toeleveringsketens met hardware- en softwarecomponenten.

Dreiging	Cyberaanvallen en statelijke actoren richten zich op componenten in de keten, van chipfabrikanten tot cloud integrators.
Impact	• Systemische verstoringen met bredere gevolgen voor organisaties in dezelfde keten. • Ongeautoriseerde toegang tot vertrouwelijke data. • Financiële schade en reputatieverlies. • Nationale veiligheidsrisico's wanneer kritieke infrastructuur met internationale ketens wordt gecompromitteerd.

11. Concentratierisico

Kwetsbaarheid	Gebruik van een beperkte set aan technologieën. Door de afwezigheid van technologische spreiding en diversificatie ontstaat een technologische 'Single Point of Failure'.
Dreiging	Wijdverspreide zero-day kwetsbaarheid, een fundamentele architectuurfout of een gerichte, grootschalige cyberaanval treft specifiek deze ene dominante technologie waarop de overheid leunt.
Impact	• Grootschalige uitval/onbeschikbaarheid van overheidsdiensten en -taken • (Gevoelige) persoonsgegevens gestolen en/of openbaar gemaakt • Informatie relevant voor Nederlandse veiligheid gestolen en/of openbaar gemaakt • Informatie relevant voor Nederlandse concurrentiepositie gestolen en/of openbaar gemaakt

3. Soevereine clouddiensten

Deze verkenning formuleert geen visie op zichzelf, maar is gebaseerd op de verschillende visies en strategieën vanuit Europa en de Nederlandse overheid.

De Nederlandse Digitalisseringsstrategie (NDS) omschrijft de urgente maatschappelijke opgaven waar Nederland mee wordt geconfronteerd met betrekking tot soevereiniteit als volgt: "Nederland staat voor grote maatschappelijke opgaven in een sterk veranderende omgeving. En digitalisering is één van de belangrijkste sleutels tot oplossingen. Daarom is investeren in onze digitale basis urgent en belangrijk voor Nederland en de grote opgaven waar de samenleving voor staat. De overheid is één van de grootste afnemers van digitale diensten. En hierdoor ook aanjager van digitale ontwikkelingen die essentieel zijn voor een weerbare samenleving en een welvarende, toekomstgerichte en productieve economie."[17]

Daarmee benadrukt de NDS[18] de noodzaak voor verandering en de behoefte aan gerichte centrale regie o.a. op het aspect strategische autonomie. Dit wordt benadrukt door het kabinet[19]. De uitgangspunten uit de NDS zijn van toepassing op deze rapportage.

Vanuit de Agenda Digitale Open Strategische Autonomie[20] uit 2023 wordt onder andere gesproken over het mitigeren van risicovolle strategische afhankelijkheidsrelaties[21]. Deze risico's hebben betrekking op de beschikbaarheid, betrouwbaarheid van dienstverleners en eigenaarschap van gegevens. Op het gebied van kwetsbaarheden ten aanzien van cloud dienstverlening wordt benoemd dat de Nederlandse en Europese markt vooral kleine lokale aanbieders kent die moeilijk kunnen concurreren met de mondiale spelers uit de VS en China. De diensten van de mondiale spelers worden bovendien gekenmerkt door gebrekkige onderlinge interoperabiliteit en portabiliteit, waardoor de afhankelijkheid wordt vergroot. Vanuit Europa wordt ingezet op een waarde-gedreven, gefedereerd data-ecosysteem met een gedecentraliseerde data-infrastructuur, waarbij cloudinteroperabiliteit, zelfbeschikking over (co)gegenereerde data uit IoT producten en het promoten van B2B-datadelen belangrijke pijlers zijn. Als mitigerende acties wordt gekeken naar een combinatie van (Europese) wetgeving, nationaal beleid, deelname aan (Europese) samenwerkingsverbanden en het definiëren van standaarden.

De digitale overheid van morgen vraagt om een stevig fundament van leidende principes die verder gaan dan louter technische inrichting. Deze principes geven richting aan de juridische, organisatorische, technische en semantische aspecten van de digitale infrastructuur en zorgen dat technologische vooruitgang in balans blijft met publieke waarden zoals vertrouwen, transparantie en legitimiteit:[22]

1. Veerkracht en aanpassingsvermogen
2. Democratische legitimiteit
3. Europese samenwerking en gedeelde waarden
4. Risicobewust leiderschap

---

[17] De Nederlandse Digitaliseringsstrategie, Samen versnellen; link

[18] Digitale Overheid: Nederlandse Digitaliseringsstrategie; link

[19] Agenda Digitale Open Strategische Autonomie; link

[20] Open Overheid; Agenda Digitale Open Strategische Autonomie; link

[21] Daarnaast wordt gesproken over het versterken van het Europese politiek-economisch fundament en het vergroten van het Europese geopolitiek handelingsvermogen, deze liggen verder van de kernvraag van deze verkenning vandaan en zullen minder expliciet worden meegenomen.

[22] De principes worden verder toegelicht in de Visie Digitale autonomie en soevereiniteit van de overheid

5. Privacy en datasoevereiniteit als kern

Het verhogen van digitale autonomie en soevereiniteit kan plaatsvinden door enerzijds maatregelen ter verkleining van de kans op gebeurtenissen die de vertrouwelijkheid van gegevens en/of de continuïteit van dienstverlening in gevaar brengen (het vergroten van de weerbaarheid) en anderzijds het verkleinen van de impact op het moment dat dergelijke gebeurtenissen zich voordoen (het vergroten van de veerkracht/aanpassingsvermogen). Het vergroten van de weerbaarheid kan plaatsvinden door actief de afhankelijkheid van niet-EU dienstverleners te verkleinen. De vorming van een soevereine clouddienst kan hier een belangrijke bijdrage aan leveren. Een dergelijke migratie kost tijd en brengt ook kosten en risico's met zich mee. Daarom moet er ook gekeken worden naar maatregelen die de impact kunnen verkleinen voor applicaties en data die (nog) niet naar een soevereine clouddienst worden gemigreerd. Bijvoorbeeld het creëren van een data back-up en (waar noodzakelijk) de applicatiesoftware, buiten de omgeving van de huidige cloudprovider[23], zodat herstel van de dienstverlening mogelijk is. Daarnaast kan de vertrouwelijkheid worden versterkt middels versleuteling van data (encryption), waardoor gegevens niet direct zichtbaar en bruikbaar zijn wanneer deze bijvoorbeeld door de Amerikaanse overheid worden opgevraagd.

De focus van deze verkenning richt zich op de opgave om de weerbaarheid te verhogen, waarbij de Nederlandse overheid de mogelijkheden tot het verhogen van de veerkracht niet uit het oog moet verliezen.

3.1. Doel

Het doel dat de Nederlandse overheid met de soevereine clouddienst wil bereiken is tweeledig:

- Enerzijds moeten overheidsbrede soevereine clouddiensten de verdere digitalisering versnellen en de, in de NDS expliciet benoemde, versnippering tegengaan om overheidstaken efficiënter en effectiever uit te voeren. Waar individuele overheidsinstanties nu vaak suboptimale condities accepteren tegen relatief hoge kosten, stelt een collectieve soevereine clouddienst de overheid in staat om schaalvoordelen in eigen beheer te realiseren en de regie op de kostenstructuur terug te pakken.
- Anderzijds vraagt het verhogen van de Nederlandse digitale weerbaarheid en veerkracht om hogere soevereiniteit en autonomie.

3.2. Stand van zaken

Momenteel is er geen overheidsbrede soevereine clouddienst beschikbaar. De Nederlandse overheid is op dit moment te afhankelijk geworden van een klein aantal externe leveranciers[24]. Dit wordt mede veroorzaakt doordat individuele overheidsorganisaties hun behoeftes op gebied van cloud computing vaak zelfstandig hebben uitgewerkt en aanbesteed. Op basis van diverse redenen is gekozen voor grote (internationale) leveranciers, waardoor risicovolle afhankelijkheden zijn ontstaan. Daarnaast nemen onderdelen van de Rijksoverheid diensten af van Overheidsdatacenters en interne dienstverleners. Deze Overheidsdatacenters zijn bezig met het doorontwikkelen van de eigen infrastructuur zodat de Rijksoverheid sneller, flexibeler, schaalbaarder en veiliger haar wettelijke taken kan uitvoeren.[25] Hoofdstuk 5 analyseert het huidige aanbod in nader detail.

[23] Mitigerende/preventieve maatregelen zoals bijv. het creëren van back-up (evt. buiten Europa) blijven relevant voor de Soevereine cloudvoorziening.

[24] Digitale Overheid, De Nederlandse Digitaliseringsstrategie Prioriteit 1 - Cloud

[25] Bron: https://www.adviescollegeicttoetsing.nl/documenten/2026/02/16/advies-enterprise-cloud

3.3. EU Cloud Sovereignty Framework

Het EU-raamwerk[26] is door de Europese Commissie ontwikkeld als instrument voor marktvergelijking. Voor deze verkenning is het raamwerk gebruikt om de ambities voor een Nederlandse soevereine cloud aan te scherpen.

Het EU Cloud Sovereignty Framework heeft een gelaagde structuur. In tegenstelling tot traditionele modellen die direct inzoomen op technische data-beveiliging, begint dit raamwerk op een hoger abstractieniveau, waarbij soevereiniteit in soevereiniteitsdoelstellingen wordt verdeeld. De diepgang van de geboden garanties wordt uitgedrukt in SEAL-niveaus (Sovereignty Evaluation Assurance Levels). Deze niveaus (SEAL 0 t/m 4) bepalen de mate van zekerheid en de strengheid van de toetsing, een hoger SEAL-niveau biedt meer soevereiniteit.

Tabel 3 geeft de verschillende doelstellingen van het raamwerk weer, gevolgd door een beschrijving van de verschillende soevereiniteitsniveaus, en Tabel 4 geeft de verschillende SEAL-niveaus weer met bijhorende beschrijvingen.

Tabel 3 Soevereiniteitsdoelstellingen uit het EU Sovereign Cloud Framework

#	Doelstelling	Beschrijving
SOV-1	Strategische soevereiniteit	Strategische soevereiniteit omvat de mate waarin de diensten van een cloudaanbieder (of technologische actor) verankerd zijn binnen het juridische, financiële en industriële ecosysteem van de Europese Unie. Het beoordeelt de stabiliteit van eigendom, invloed op het bestuur en de afstemming op strategische prioriteiten van de EU.
SOV-2	Juridische en rechtsgebonden soevereiniteit	Juridische en rechtsgebonden soevereiniteit evalueert de juridische omgeving, de blootstelling aan buitenlandse autoriteiten en de afdwingbaarheid van rechten die de diensten van een technologieleverancier beheersen. Het bepaalt de mate waarin diensten verankerd zijn in de Europese jurisdictie en geïsoleerd zijn van externe juridische claims.
SOV-3	Data & AI soevereiniteit	Data & AI soevereiniteit richt zich op de bescherming, controle en onafhankelijkheid van data-assets en AI-diensten binnen de EU. Het behandelt hoe gegevens worden beveiligd, waar ze worden verwerkt en de mate van autonomie die afnemers behouden over AI-functionaliteiten.
SOV-4	Operationele soevereiniteit	Operationele soevereiniteit meet het praktische vermogen van EU-spelers om een technologie onafhankelijk van buitenlandse controle te exploiteren, te ondersteunen en verder te ontwikkelen. Het richt zich op continuïteit van de operatie, beschikbaarheid van vaardigheden en veerkracht tegen externe afhankelijkheden.
SOV-5	Supply chain soevereiniteit	Toeleveringsketen soevereiniteit evalueert de geografische oorsprong, transparantie en veerkracht van de technologische toeleveringsketen. Hierbij ligt de focus op de mate waarin kritieke componenten en processen onder EU-controle blijven of blootgesteld zijn aan niet-EU afhankelijkheden.

[26] Formeel heeft dit raamwerk geen status voor verschillende landen.

SOV-6	Technologische soevereiniteit	Technologische soevereiniteit evalueert de mate van openheid, transparantie en onafhankelijkheid in de onderliggende technologische stack. Dit borgt dat EU-spelers oplossingen kunnen laten samenwerken, auditen en doorontwikkelen zonder afhankelijk te zijn van buitenlandse bedrijfseigen (propriëtaire) systemen.
SOV-7	Beveiliging & compliance soevereiniteit	Beveiliging & Compliance soevereiniteit meet de mate waarin beveiligingsoperaties, compliance-verplichtingen en veerkrachtmaatregelen binnen de EU controle blijven, om onafhankelijkheid van buitenlandse jurisdicties en operationele zekerheid (assurance) op de lange termijn te garanderen.
SOV-8	Ecologische duurzaamheid	Ecologische duurzaamheid beoordeelt de autonomie en veerkracht van clouddiensten op de lange termijn in relatie tot energieverbruik, afhankelijkheid en de schaarste van grondstoffen.

Tabel 4 SEAL-niveaus EU Sovereign Cloud Framework

Niveau	Soevereiniteitsniveau	Beschrijving
SEAL-0	Geen soevereiniteit	Dienst, technologie en/of exploitatie staan onder exclusieve controle van niet-EU derde partijen die volledig bestuurd worden vanuit niet-EU rechtsgebieden.
SEAL-1	Jurisdictionele soevereiniteit	EU-wetgeving is formeel van toepassing met beperkte praktische afdwingbaarheid; dienst, technologie en/of exploitatie staan onder exclusieve controle van niet-EU derde partijen.
SEAL-2	Data-soevereiniteit	EU-wetgeving is van toepassing en afdwingbaar, waarbij wezenlijke niet-EU afhankelijkheden blijven bestaan; dienst, technologie en/of exploitatie staan onder indirecte controle van niet-EU derde partijen.
SEAL-3	Digitale veerkracht	EU-wetgeving is van toepassing en afdwingbaar, waarbij EU-spelers betekenisvolle maar geen volledige invloed uitoefenen; dienst, technologie en/of exploitatie staan onder marginale controle van niet-EU derde partijen.
SEAL-4	Volledige digitale soevereiniteit	Technologie en exploitatie staan onder volledige EU controle, zijn uitsluitend onderworpen aan EU-wetgeving en hebben geen kritieke niet-EU afhankelijkheden.

3.4. Dilemma's vragen om een realistische benadering

De weg naar een soevereine clouddienst is een strategische keuze die rust op het principe: 'open waar het kan, beschermen waar het moet'[27]. In de praktijk brengt deze koers een aantal concessies met zich mee, waaronder economische dilemma's waarbij de (tijdelijke) stijging van kosten een reëel risico vormt. Wanneer de overheid

[27] Open Overheid, Visie Digitale autonomie en soevereiniteit van de Overheid

minder leunt op de dominante wereldspelers, gaan bestaande schaalvoordelen deels verloren en moet er geïnvesteerd worden in oplossingen die specifiek aan de soevereiniteitseisen voldoen.

Naast de financiële consequenties speelt het spanningsveld rondom innovatie een cruciale rol. Waar Amerikaanse hyperscalers kant-en-klare, geavanceerde functionaliteiten bieden, kan de keuze voor een meer soevereine koers betekenen dat de overheid genoegen moet nemen met een lager innovatietempo. Om dit te voorkomen, is een proactieve houding vereist waarbij de overheid zelf investeert om technologisch bij te blijven.

Deze transitie kan alleen slagen als de overheid de markt verleidt tot verandering door haar strategische vraag te bundelen. Het inzetten van gezamenlijke inkoopkracht is essentieel om een open en soeverein ecosysteem te stimuleren[28], maar hier stuit de praktijk op een belangrijke barrière: een centraal sturend orgaan dat deze vraag kan centraliseren, ontbreekt momenteel nog. Het vormgeven van deze regierol is een van de grootste uitdagingen in het proces. Zonder een dergelijk centraal punt blijft de vraag versnipperd en de invloed op de markt beperkt.

Zonder substantiële investeringen en ingrijpende organisatorische maatregelen zal het onmogelijk blijven om het niveau van ‘soeverein genoeg’ te bereiken en de soevereiniteit te verankeren in de operationele koers.

[28] NDS, ‘Samen Versnellen’, de vrijblijvendheid voorbij blz 4

4. Soevereiniteitsambitie van de Nederlandse overheid

4.1. Ambitie op basis van EU Cloud Sovereignty Framework

In navolging van de werksessies met het programma NDS Cloud, is geconcludeerd dat het programma voor de implementatie van een soevereine cloud, een minimaal soevereiniteitsniveau van *SEAL-4* volgens het EU Cloud Sovereignty Framework (zie paragraaf 3.3) ambieert. Deze ambitie, die de bereidheid van de overheid om strikte regie te voeren over digitale soevereiniteit en autonomie reflecteert, is bekrachtigd door de stuurgroep van het programma NDS Cloud. Het NDS team heeft hierbij een nuancering aangebracht ten aanzien van de praktische uitvoerbaarheid op het gebied van de doelstellingen SOV-5 (supply chain soevereiniteit)en , SOV-6 (technologie soevereiniteit) en SOV-8 (milieu duurzaamheid). De reden voor deze nuancering ligt bij de actuele marktcondities en de diepe technologische afhankelijkheid van non-EU hardware-leveranciers. Volledige onafhankelijkheid op deze specifieke domeinen wordt op korte tot middellange termijn als onrealistisch beschouwd.

Tabel 5 Ambitieniveau op basis van EU Cloud Sovereignty Framework

Doel	Omschrijving	Ambitieniveau
SOV-1	Strategische soevereiniteit omvat de mate waarin de diensten van een cloudaanbieder (of technologische actor) verankerd zijn binnen het juridische, financiële en industriële ecosysteem van de Europese Unie. Het beoordeelt de stabiliteit van eigendom, invloed op het bestuur en de afstemming op strategische prioriteiten van de EU.	SEAL-4
SOV-2	Juridische en rechtsgebonden soevereiniteit evalueert de juridische omgeving, de blootstelling aan buitenlandse autoriteiten en de afdwingbaarheid van rechten die de diensten van een technologieleverancier beheersen. Het bepaalt de mate waarin diensten verankerd zijn in de Europese jurisdictie en geïsoleerd zijn van externe juridische claims.	SEAL-4
SOV-3	Data & AI soevereiniteit richt zich op de bescherming, controle en onafhankelijkheid van data-assets en AI-diensten binnen de EU. Het behandelt hoe gegevens worden beveiligd, waar ze worden verwerkt en de mate van autonomie die afnemers behouden over AI-functionaliteiten.	SEAL-4
SOV-4	Operationele soevereiniteit meet het praktische vermogen van EU-spelers om een technologie onafhankelijk van buitenlandse controle te exploiteren, te ondersteunen en verder te ontwikkelen. Het richt zich op continuïteit van de operatie, beschikbaarheid van vaardigheden en veerkracht tegen externe afhankelijkheden.	SEAL-4
SOV-5	Toeleveringsketen soevereiniteit evalueert de geografische oorsprong, transparantie en veerkracht van de technologische toeleveringsketen. Hierbij ligt de focus op de mate waarin kritieke componenten en processen onder EU-controle blijven of blootgesteld zijn aan niet-EU afhankelijkheden.	SEAL-4*
SOV-6	Technologische soevereiniteit evalueert de mate van openheid, transparantie en onafhankelijkheid in de onderliggende technologische	SEAL-4*

	stack. Dit borgt dat EU-spelers oplossingen kunnen laten samenwerken, auditen en doorontwikkelen zonder afhankelijk te zijn van buitenlandse bedrijfseigen (propriëtaire) systemen.	
SOV-7	Beveiliging & Compliance soevereiniteit meet de mate waarin beveiligingsoperaties, compliance-verplichtingen en veerkrachtmaatregelen binnen de EU controle blijven, om onafhankelijkheid van buitenlandse jurisdicties en operationele zekerheid (assurance) op de lange termijn te garanderen.	SEAL-4
SOV-8	Ecologische duurzaamheid beoordeelt de autonomie en veerkracht van clouddiensten op de lange termijn in relatie tot energieverbruik, afhankelijkheid en de schaarste van grondstoffen.	De bestaande MVI-criteria worden gehanteerd[29].

* Zie de nuancering die boven de tabel ten aanzien van deze doelstellingen is opgenomen.

Deze ambitie dient als fundament voor de scenariovorming in deze marktbeschouwing. Daarom worden in hoofdstuk 7 uitsluitend scenario's omschreven die minimaal voldoen aan het ambitieniveau zoals in Tabel 5 is omschreven.

4.2. Beoordelingscriteria die extra prioriteit krijgen

Aanvullend heeft het programma NDS Cloud de criteria uit het Europese raamwerk beoordeeld om vast te stellen welke criteria extra prioriteit moeten krijgen met oog op het geambieerde soevereiniteitsniveau en het reduceren van strategische afhankelijkheden. De uitkomsten hiervan zijn weergegeven in Tabel 6. Dit betekent dat het voor de criteria die in het *blauw* zijn aangeduid belangrijk is dat deze vanuit Nederland geleverd/gerealiseerd kunnen worden.

Tabel 6 Belangrijkste beoordelingscriteria per soevereiniteitsaspect

Doel	Beoordelingscriteria
SOV-1 – Strategisch	1. *Ervoor zorgen dat instanties die beslissende bevoegdheid hebben over uw diensten, onder de jurisdictie van de EU vallen.* 2. *De garanties tegen verandering van zeggenschap evalueren.* 3. De mate waarin de aanbieder afhankelijk is van financiering uit EU-bronnen. 4. De omvang van investeringen, banen en waarde creatie binnen de EU. 5. Betrokkenheid bij EU-initiatieven, Consistentie met de op EU-niveau gedefinieerde doelstellingen op het gebied van digitale, groene en industriële soevereiniteit. 6. Het vermogen om veilige activiteiten te handhaven tegen verzoeken om de dienst te staken of op te schorten, of als de ondersteuning door de leverancier wordt ingetrokken of verstoord.

[29] Maatschappelijk Verantwoord Inkopen criteria; link

SOV-2 – Juridisch	1. Het nationale rechtssysteem dat van toepassing is op de activiteiten en contracten van de aanbieder. 2. Mate van blootstelling aan niet-EU-wetgeving met grensoverschrijdende reikwijdte (bijv. de Amerikaanse CLOUD Act, de Chinese cyberbeveiligingswet). 3. Het bestaan van juridische, contractuele of technische kanalen waarmee niet-EU-autoriteiten toegang tot gegevens of systemen kunnen afdwingen. 4. Toepasselijkheid van internationale regelingen, die het gebruik of de overdracht kunnen beperken. 5. Locatie van creatie, registratie en ontwikkeling van intellectueel eigendom (EU versus derde landen), rechtsgebied waar intellectueel eigendom wordt gecreëerd en ontwikkeld.
SOV-3 – Data & AI	*1. Ervoor zorgen dat alleen de klant, en niet de aanbieder, effectieve controle heeft over de cryptografische toegang tot zijn gegevens.* 2. Inzicht in wanneer, waar en door wie gegevens worden geraadpleegd, met inbegrip van controleerbaarheid van het gebruik van AI-modellen, mechanismen die onomkeerbare verwijdering van gegevens garanderen, met verifieerbaar bewijs. *3. Strikt beperken van opslag en verwerking tot Europese rechtsgebieden, zonder terugval op derde landen.* 4. Mate waarin AI-modellen en datapijplijnen worden ontwikkeld, getraind, gehost en beheerd onder EU-controle, waardoor de afhankelijkheid van niet-EU-technologiestacks tot een minimum wordt beperkt.
SOV-4 – Operationeel	*1. Gemakkelijke migratie van workloads of integratie met alternatieve EU-gecontroleerde oplossingen zonder vendor lock-in.* *2. Mogelijkheid voor EU-exploitanten om de technologie te beheren, te onderhouden en te ondersteunen zonder tussenkomst van niet-EU-leveranciers.* *3. Aanwezigheid van een EU-gebaseerde talentenpool met de expertise om de dienst te exploiteren en in stand te houden.* *4. De garantie dat operationele ondersteuning wordt geleverd vanuit de EU en uitsluitend onderworpen is aan EU-wetgeving.* *5. De beschikbaarheid van volledige technische documentatie, broncode en operationele knowhow die langdurige autonomie mogelijk maken.* *6. De locatie en juridische controle van kritieke leveranciers of onderaannemers die betrokken zijn bij de dienstverlening.*
SOV-5 - Toeleveringsketen	1. Geografische herkomst van belangrijke fysieke onderdelen, productielocatie - landen waar hardware wordt geproduceerd of geassembleerd. 2. Rechtsgebied en herkomst van ingebouwde code die hardware en firmware aanstuurt. 3. Herkomst van software: waar en door wie software wordt ontworpen en geprogrammeerd, locatie en rechtsgebied waar softwareverpakking, distributie en updates onder vallen. 4. Mate van afhankelijkheid van niet-EU-leveranciers, faciliteiten of eigen technologieën. 5. Inzicht in de volledige keten van leveranciers en onder-leveranciers, inclusief auditrechten.

SOV-6 – Technologie	1. Mogelijkheid tot integratie met andere technologieën via goed gedocumenteerde en niet-propriëtaire API's of protocollen, mate waarin de oplossing voldoet aan openbaar beheerde en algemeen aanvaarde normen, waardoor de afhankelijkheid van één leverancier wordt verminderd. 2. Of software toegankelijk is onder open licenties, met rechten om te controleren, te wijzigen en te herdistribueren, waardoor transparantie en aanpasbaarheid worden gewaarborgd. 3. Inzicht in het ontwerp en de werking van de dienst, met inbegrip van architectuurdocumentatie, gegevensstromen en afhankelijkheden 4. Mate van onafhankelijkheid van de EU op het gebied van hoogwaardige rekencapaciteit, met inbegrip van processors, versnellers en software-ecosystemen.
SOV-7 – Veiligheid en naleving	1. Het behalen van EU- en internationaal erkende certificeringen (bijv. ISO, ENISA-regelingen). 2. Naleving van GDPR, NIS2, DORA en andere EU-kaders. *3. Beveiligingscentra en responsteams die uitsluitend onder EU-jurisdictie opereren, controle over beveiligingsmonitoring/logging - mogelijkheid voor klanten of EU-autoriteiten om rechtstreeks toezicht te houden op logs, waarschuwingen en monitoringfuncties.* 4. Transparante, tijdige en EU-conforme rapportage van inbreuken of kwetsbaarheden, onderhoud Autonomie - mogelijkheid om onafhankelijk van niet-EU-leveranciers beveiligingspatches te ontwikkelen, te testen en toe te passen. 5. Mogelijkheid voor EU-entiteiten om onafhankelijke beveiligings- en nalevingsaudits uit te voeren met volledige toegang.
SOV-8 - Milieuduurzaamheid	1. Toepassing van energie-efficiënte infrastructuur (bijv. lage PUE) en meetbare verbeteringsdoelstellingen. 2. Circulaire economiepraktijken die hergebruik, renovatie en verantwoorde verwerking van hardware aan het einde van de levensduur garanderen. 3. Transparante meting en openbaarmaking van CO2-uitstoot, waterverbruik en andere duurzaamheidsindicatoren.

5. EU Marktbeschouwing

Dit hoofdstuk richt zich op het aanbod binnen de (soevereine) cloud markt in de EU. Het doel is om de volwassenheid, geschiktheid en de richting van de Europese markt te duiden en wat dit specifiek betekent voor de mogelijkheden van samenwerking met de markt voor de Nederlandse overheid. Deze marktscan geeft geen compleet overzicht van alle beschikbare leveranciers. Bij het analyseren van de leveranciers is gekeken naar zowel marktpartijen als overheidsdienstverleners die een rol kunnen spelen in de totstandkoming van een soevereine clouddienst voor de Nederlandse overheid.

Het is van belang om de huidige marktdynamiek te onderkennen. De markt voor soevereine clouddiensten bevindt zich in een vroege, uiterst dynamische fase waarin organisaties en consortia hun proposities in hoog tempo door ontwikkelen. Voorbeelden van deze dynamiek zijn productlanceringen (waardoor functionele mogelijkheden worden verruimd), investeringen in nieuwe capaciteit (met meer schaalgrootte als gevolg), overnames en samenwerkingsverbanden (met mogelijke gevolgen voor schaalgrootte, prijsniveaus maar ook SEAL-niveaus). Door te focussen op bruikbare typologieën in plaats van een detailanalyse van specifieke dienstverleners en hun portfolio wordt zoveel mogelijk voorkomen dat deze analyse kort na het verschijnen van het rapport ingehaald is door de situatie in de markt. Om grip te krijgen op deze beweeglijke markt, focust deze marktbeschouwing op clouddiensten die door cloud dienstverleners end-to-end worden aangeboden en die de overheid als zodanig kan contracteren. De analyse is uitgevoerd aan de hand van de volgende vier vragen:

1. Welke verschillende ontwikkelmodellen zijn er binnen Europa zichtbaar om de soevereiniteit en autonomie te borgen?
2. Welke typen (soevereine) clouddiensten en technologische oplossingen zijn momenteel beschikbaar in Europa?
3. Welke (voorbeelden van) marktpartijen positioneren zich als leverancier van deze (soevereine) diensten?[30]
4. Wat doen andere overheden om een soevereine clouddienst te realiseren?

De beantwoording van deze vragen is gebaseerd op een synthese van Gartner-research en de resultaten van de marktverkenning die het NDS-aanjaagteam heeft uitgevoerd in het kader van de 'Open Dialoog[31]'. Daarnaast worden de rollen die door marktpartijen kunnen worden vervuld in de totstandkoming van een soevereine clouddienst (zie paragraaf 1.5 Definities), meegenomen worden in de uitwerking van de scenario's in hoofdstuk 7.

5.1. Ontwikkelmodellen voor soevereiniteit en autonomie

De ontwikkeling van soevereine clouddiensten wordt gedreven door een tweetal drijvende krachten:

1. Leveranciers die invulling willen geven aan een toenemende vraag naar soevereiniteit en autonomie
2. Overheden die stappen ondernemen om de risico's die gepaard gaan met het gebruik en de afhankelijkheid van niet-Europese leveranciers te verminderen.

[30] In de beschouwing van de markt zijn we voor de genoemde voorbeelden uitgegaan van leveranciers die dergelijke diensten op het moment van schrijven daadwerkelijk leveren

[31] Tenderned, Verslag Open Dialoog Compleet v1.0.pdf

Leveranciers zijn al enkele jaren bezig om een meer soeverein aanbod aan clouddiensten te definiëren en in de markt te zetten. Hier is een veelheid van initiatieven waarneembaar, van het opzetten van compleet nieuwe diensten tot het doorontwikkelen van bestaande diensten en het aangaan van samenwerkingsverbanden. Dat laatste gebeurt zowel in de vorm van Europese leveranciers met Amerikaanse hyperscalers om de technologie van de hyperscalers in een meer soevereine vorm te kunnen aanbieden via een Europese dienstverlener[32], als in samenwerkingsverbanden tussen partijen om schaalvoordelen en interoperabiliteit te bewerkstelligen die het aantrekkelijker maken om met deze leveranciers te werken. Door gezamenlijke technische standaarden te hanteren, geven zij aan een schaalbaar en veilig alternatief te bieden. De focus ligt daarbij op vitale infrastructuur en interoperabiliteit tussen leveranciers in de alliantie.

Ondanks toenemende samenwerking en convergentie van het aanbod is er op het moment van schrijven van deze verkenning nog steeds sprake van een grote mate van fragmentatie in de markt. Paragrafen 5.2 en 5.3 gaan dieper in op de typologieën van cloud diensten die als gevolg van deze ontwikkelingen ontstaan en hoe zich dat specifiek in de markt van Nederlandse leveranciers manifesteert.

Ook overheden zijn de afgelopen jaren initiatieven gestart om meer soevereine clouddiensten voor de overheid te creëren, veelal in samenwerking met of ondersteund door marktpartijen. In sommige gevallen wordt er een nieuwe voorziening gebouwd, waarbij de overheid een aanbesteding gebruikt om marktpartijen te betrekken bij de bouw, het beheer van, en de migratie naar de nieuwe clouddienst. In andere gevallen wordt er een gezamenlijke, nieuwe onderneming opgericht om invulling te geven aan de publiek-private samenwerking, of worden leveranciers en oplossingen geselecteerd op basis van de specifieke eisen om invulling te geven aan de clouddienst voor de overheid. De initiatieven vanuit de overheid hebben zowel betrekking op IaaS en PaaS dienstverlening als op alternatieve werkplekoplossingen voor productiviteit en samenwerking.

Paragraaf 5.4 gaat nader in op voorbeelden van initiatieven die overheden in andere landen ontplooien om te komen tot meer soevereine alternatieven voor cloud dienstverlening.

5.2. Typologieën en voorbeelden van het marktaanbod

Zoals eerder aangegeven is de markt voor soevereine clouddiensten sterk in beweging en bestaat er een spectrum aan diensten die onder de noemer ‘soeverein’ wordt aangeboden. Binnen dit spectrum zijn verschillende niveaus van soevereiniteit te ontwaren. In plaats van een statische lijst met aanbieders (deze is snel verouderd), hanteert deze marktbeschouwing een typologie die onderscheid maakt op basis van twee aspecten:

1. Bevindt de controle over en het beheer van de dienstverlening zich organisatorisch gezien binnen of buiten de EU?
2. Waar de ultieme controle en support over de broncode van de software ligt. Hier wordt gekeken naar de software die als fundament wordt gebruikt voor het leveren van clouddiensten. Dit aspect heeft vooral betrekking op de IaaS laag van de dienstverlening. Het tweede aspect kent drie categorieën:
    - *Propriëtaire (commerciële) software*: Gelicentieerde software waarbij broncode niet openlijk wordt gepubliceerd en het gebruik wordt bepaald door licentievoorwaarden van de leveranciers, vaak gecombineerd met betaalde modellen, door leveranciers aangeboden Service Level Agreements

[32] AWS, Opening the AWS European Sovereign Cloud.

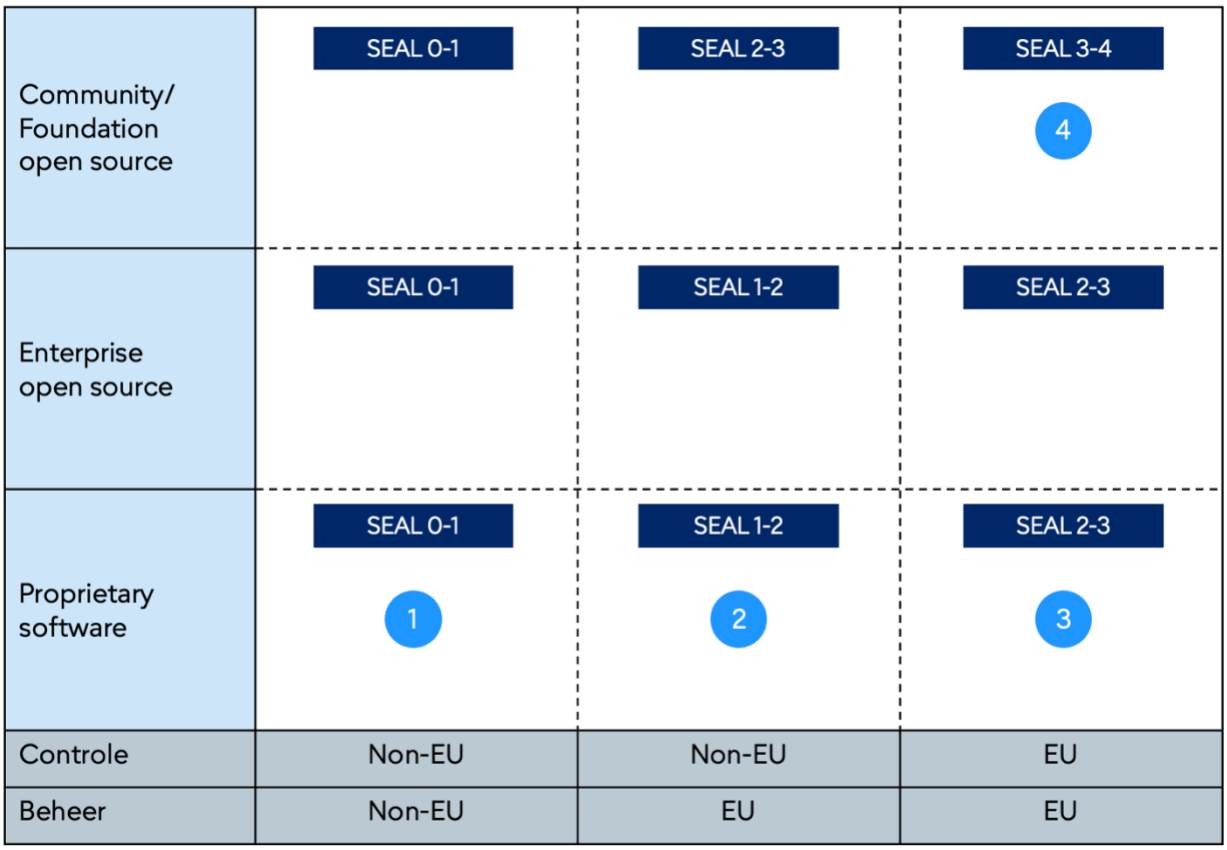
(SLA)'s en ondersteuning. Kopers vertrouwen op product roadmaps van leveranciers en commerciële ondersteuningscontracten in plaats van op community governance of open herdistributierechten.

- *Enterprise open source:* Open-source projecten of distributies die worden ondersteund door een of meer commerciële leveranciers die gecertificeerde distributies, betaalde ondersteuningsabonnementen, trainingen, enterprise-addons (opencore of freemium patronen) en commerciële SLA's aanbieden, terwijl de broncode beschikbaar blijft onder een opensource licentie. Dit model ruilt vrij beschikbare broncode in voor door leveranciers beheerde operationele garanties en lagere voorafgaande licentiekosten in plaats van traditionele propriëtaire licenties.
- *Community/foundation open source*: Projecten die worden gehost of beheerd door neutrale stichtingen of standaardisatieorganen (bijvoorbeeld CNCF, Linux Foundation, Eclipse Foundation) die fungeren als industriële standaarden, maar de nadruk leggen op community governance, diversiteit van bijdragers (zowel commerciële partijen als overheden), transparante roadmaps en open licenties die aansluiten bij OSI-definities. Deze projecten vertrouwen voornamelijk op gemeenschapsprocessen in plaats van op één enkele commerciële leverancier voor langdurig onderhoud en beleid.

Op basis van deze aspecten ontstaan er negen typologieën. Figuur 5 beeld de typologieën af incl. het indicatieve SEAL-niveau[33].

[33] Daadwerkelijke SEAL-niveaus moeten per leverancier op basis van het specifieke aanbod worden vastgesteld, derhalve kan hier enkel een indicatie worden gegeven.

Figuur 5 soevereine cloud typologieën met bijhorende SEAL score



Hoewel er verschillende cloud-typologieën bestaan, zien we in de Europese praktijk slechts enkele vormen in substantiële mate terug. Hieronder worden deze toegelicht aan de hand van een aantal praktijkvoorbeelden. [34].

Langs de as van de propriëtaire software worden alle weergegeven typologieën waargenomen:

1. *Ultieme controle en beheer beiden buiten de EU:* dit betreft de public cloud diensten die geen specifieke aanpassingen hebben ten behoeve van verhoogde soevereiniteit en autonomie aangeboden door hyperscalers. Aangezien hier sprake is van diensten waarvoor de ultieme controle geheel buiten de EU ligt of waar EU-wetgeving weliswaar formeel van kracht is maar slechts zeer beperkt afdwingbaar, zal het SEAL niveau zich op 0 of maximaal 1 bevinden. De bekendste (en binnen de Nederlandse overheid vaak toegepaste) voorbeelden binnen deze typologie zijn Microsoft Azure, Amazon Web Services (AWS) en Google Cloud Platform.
2. *Ultieme controle buiten de EU, beheer binnen de EU*: dit betreft met name Europese dochterondernemingen van internationale cloud dienstverleners die een meer soeverein alternatief

[34] Voorbeelden die worden genoemd dienen uitsluitend ter illustratie. Of leveranciers wel of niet zijn opgenomen in deze verkenning is op geen enkele wijze een classificatie van de leverancier, en of haar aanbod geschikt is voor het leveren van clouddiensten in de specifieke context van de soevereine clouddienst voor de Nederlandse overheid. Ook is er sprake van een momentopname en kan de ultieme controle als gevolg van een overname buiten de EU komen te liggen.

bieden voor hun public cloud diensten door middel van een Europese juridische entiteit, datacenters in Europa die niet gekoppeld zijn aan de public cloud diensten van de moedermaatschappij en beheer door inwoners van Europa. EU-wetgeving is hier weliswaar formeel van kracht en door lokale juridische entiteiten afdwingbaar, maar er blijven materiële afhankelijkheden buiten de EU bestaan vanwege de indirecte controle vanuit een niet-Europese moedermaatschappij. Het SEAL-niveau voor deze typologie zal zich daarom op 1 of maximaal 2 bevinden. Voorbeelden binnen deze typologie zijn de AWS European Sovereign Cloud en Oracle EU Sovereign Cloud.

3. *Ultieme controle en beheer beiden binnen de EU*. De leverancier zelf valt in dit geval volledig onder Europese wetgeving en deze wetgeving is afdwingbaar. Niettemin is er vanwege het gebruik van propriëtaire software voor het cloud platform sprake van een marginale mate van invloed van buiten de EU, waardoor het SEAL niveau zich op 2 of maximaal 3 bevindt.

    - Enerzijds betreft dit samenwerkingsverbanden waarin Europese leveranciers zorgdragen voor de datacenterlocaties en het beheer terwijl Amerikaanse cloud serviceproviders de technologie onder de dienstverlening leveren. Voorbeelden hiervan zijn S3NS en Delos Cloud.
    - Anderzijds betreft het Europese leveranciers die cloud platform software van een Amerikaanse softwareleverancier (zoals bijvoorbeeld VMWare) gebruiken. Nederlandse voorbeelden hiervan zijn KPN en Eurofiber.

4. *Ultieme controle en beheer beiden binnen de EU* met Open Source technologie. Langs de as van open source software zien we een dominantie van OpenStack als cloud platform waarop de cloud dienstverlening wordt gebaseerd. Slechts in een enkel geval is duidelijk dat het een variant betreft die door een commerciële partij worden ondersteund (enteprise open source, bijvoorbeeld de T Cloud Public op basis van een Huawei OpenStack distributie), in de meeste gevallen gaat het om community/foundation open source software.

    - Voor de Europese markt worden cloud diensten op basis van het open source cloud platform OpenStack voornamelijk aangeboden door partijen waarvan de ultieme controle en het beheer binnen de EU liggen. De leverancier valt in dit geval volledig onder EU-wetgeving en ook vanuit de software is er geen of nauwelijks sprake van invloed van buiten de EU. Daarom zullen leveranciers binnen deze typologie typisch op SEAL niveau 3 of zelfs 4 zitten. Voorbeelden binnen deze typologie zijn OVHCloud, STACKIT en Cleura.

5.3. De Nederlandse markt voor soevereine clouddiensten

5.3.1. Commercieel aanbod voor soevereine clouddiensten

In Tabel 7 wordt een overzicht gegeven van partijen die in de Nederlandse markt, vanuit datacenters in Nederland, soevereine clouddiensten aanbieden. Dit overzicht bevat partijen die actief hebben deelgenomen aan de Open Dialoog (danwel vertegenwoordigd zijn door de brancheverenigingen Dutch Cloud Community en NLdigital die als toehoorder bij de Open Dialoog aanwezig waren) en strategische Europese spelers zoals OVHcloud en Leaseweb vanwege hun 'enterprise-grade' oplossingen.

Tabel 7 Voorbeelden van marktpartijen die vanuit datacenters in Nederland clouddiensten leveren

Leverancier	Focus/Specialisatie	Gebruikte Datacenter leveranciers	Gebruikte technologie	Bijzonderheden
Info Support	Mission critical / Ecofed	ITB2, BIT Ede	OpenNebula (OSS)	ITB2 stopt en neemt geen nieuwe klanten meer aan.
Centric	Overheid / AI workloads	Equinix, NorthC	VMWare (via Uniserver partnership)	Partnership met Nebul aangekondigd om EU AI workloads aan te bieden.
Intermax	Zorg / Managed Kubernetes	NorthC	VMWare	ISO-gecertificeerd
KPN CloudNL	Overheid / Enterprise	Haarlem, Eindhoven, Almere	VMWare (Sovereign status)	Eigen datacenters, Gecertificeerd AWS VMWare MSP.
Uniserver	Hybride Cloud	NorthC, Equinix, Equans	HPE, Cisco, VMWare	VMWare Cloud Foundation Pinnacle Partner.
Eurofiber	Vitale infra / Connectiviteit	8 locaties (o.a. AMS, UTR)	VMWare	Eigen datacenters, met eigen vezelnetwerk. Draait vitale GVB-infrastructuur.
Previder	MSP / Hybride Cloud	Hengelo, Vianen	VMWare, Veeam	Eigen datacenters, eerste Haven-compliant IaaS platform.
OVHcloud	Europese Enterprise leverancier	Global (EU focus), Amsterdam (co-locatie)	OpenStack (OSS), VMWare	SecNumCloud gecertificeerd, bouwen eigen servers handmatig (backdoor preventie).
Leaseweb	Enterprise leverancier	Global (o.a. NL)	CloudStack (OSS), KVM	European Cloud Campus member (IPCEI-CIS), ISO gecertificeerd, ook datacenters in VS.

De huidige Nederlandse markt voor soevereine clouddiensten kenmerkt zich door een opvallende inzet van VMWare als virtualisatie laag. Hoewel deze software zichzelf kenmerkt als 'Sovereign Cloud Solution'[35] blijft het feit bestaan dat de technologie in handen is van het Amerikaanse Broadcom. Dit brengt vragen met zich mee over de juridische invloed van de Amerikaanse overheid en de commerciële afhankelijkheid van licentievoorwaarden, dit zijn risico's die zorgvuldig moeten worden afgewogen tegen de stabiliteit en bekendheid van het platform.

[35] VMWare, VMWare Sovereign Cloud Solution Overview

De ‘enterprise-grade’ oplossingen die voldoen aan de strengste eisen voor security, schaalbaarheid en autonomie zijn bijvoorbeeld die van OVHcloud en Leaseweb. Deze partijen onderscheiden zich door het gebruik van open source-gebaseerde technologie zoals OpenStack en CloudStack. OVHcloud gaat hierin het verst, naast dat het over de SecNumCloud-certificering beschikt, bouwt het de servers zelf om “backdoors” vanuit Amerikaanse hardware leveranciers te voorkomen. Leaseweb biedt een vergelijkbare robuustheid en is nauw betrokken bij Europese initiatieven zoals IPCEI-CIS, al opereren zij ook in de VS, wat voor sommige strikt soevereine scenario's een aandachtspunt kan zijn.

Nederlandse commerciële dienstverleners presteren goed op het gebied van lokale compliance en specifieke sector-eisen. Het zijn vaak betrouwbare partners met diepe wortels in de Nederlandse markt, maar hun fysieke infrastructuur, vaak beperkt tot twee datacenters, vormt een natuurlijke grens voor de mate van veerkracht (“resiliency”) en schaalbaarheid.

5.3.2. Leveranciers vanuit de Rijksoverheid

Tabel 8 geeft een overzicht van organisaties die binnen de Rijksoverheid clouddiensten leveren. Het overzicht is opgesteld op basis van de door deze partijen opgeleverde informatie.

Tabel 8 cloudleveranciers vanuit de Rijksoverheid

Organisatie	Focus/ Specialisatie	Gebruikte Datacentra	Gebruikte technologie	Opmerkingen m.b.t. Open Source en Selfservice
DUO	Housing, IaaS, PaaS	ODCN & 1x eigen DC	VMware vSphere/VCF, OpenShift, Calico, Cisco ACI, Ansible, Salt, PostgreSQL, MS-SQL.	Migratie gaande van DB2 naar open-source databases (PostgreSQL). Selfservice is geïmplementeerd als vereiste voor agile teams.
DICTU	PaaS, IaaS en Network-as-a-Service	ODCN	VMware, SUSE Harvester/Rancher/ RKE, Cisco ACI, Terraform, Ansible, Oracle, MS-SQL.	60% propriëtaire databases in huidige situatie. Transitie gepland naar volledige selfservice.
Justitiële ICT Organisatie (JIO)	Housing, hosting, IaaS, PaaS.	ODC Amsterdam (Equinix), ODC Noord, MS Azure (Cloud).	VMware, OpenShift, Kubernetes, Cisco, Ivanti, Ansible, MS-SQL.	Selfservice is in ontwikkeling. Open-source adoptie beperkt wegens sterke afhankelijkheid van leveranciersondersteuning
Rijkswaterstaat	Housing, hosting, IaaS, PaaS	ODC-Amsterdam (Equinix), POP-locaties in Rhoon en Utrecht.	VMware Tanzu, OpenShift, Cisco ACI, EVPN-VXLAN, Ansible, Terraform, PostgreSQL.	50/50 verdeling m.b.t. databases tussen open source en propriëtair. In transitie naar een open-source cloudarchitectuur (inclusief netwerk en beheer) met verregaande selfservice autonomie

Organisatie	Focus/ Specialisatie	Gebruikte Datacentra	Gebruikte technologie	Opmerkingen m.b.t. Open Source en Selfservice
RIVM	Housing, Hosting, IaaS en PaaS, Werkplekdienstverlening	Amsterdam (Equinix RODC), deels fuserend met ODC-Noord; Public Cloud (Azure)	Nutanix, HPE Greenlake, VMware, MS Azure, Red Hat OpenShift, Cisco ACI/DNA, Ansible.	Selfservice nu enkel mogelijk op het Azure platform, niet on-premises. propriëtaire software krijgt vaak de voorkeur wegens gegarandeerde support en continuïteit.
SSC-ICT	Housing, Hosting, PaaS (gebaseerd op Kubernetes).	ODC Rijswijk (primair), Den Haag, Apeldoorn, Groningen.	VMware vSphere, SUSE Rancher, OpenShift, Cisco ACI, Terraform, Ansible.	Grote afhankelijkheid (95%) van propriëtaire databases (Oracle, MS-SQL). Gefaseerde verschuiving naar open-source, gedreven door digitale soevereiniteitskaders. Volledige selfservice ontbreekt.
Belastingdienst	Housing, Hosting, IaaS en PaaS	Apeldoorn	VMWare, F5, OpenShift, Ansible, Terraform, Helm, Db2, Oracle, MS-SQL.	95% propriëtaire databases. Na initiële onboarding opereren teams autonoom (selfservice). Eigen, specifiek intern OSS-beleid geïmplementeerd
ODC-Noord	Housing, Hosting, IaaS en PaaS	Groningen (twee locaties) en Rijswijk.	VMware, KVM, OpenShift, OpenStack, vCloud, Ansible, Terraform, Saltstack, PostgreSQL.	Biedt gedeelde en dedicated clusters. Autonome selfservice na verplichte onboarding. 'Open source, tenzij' wordt pragmatisch toegepast; Oracle valt buiten scope
Logius	PaaS en SaaS	ODC-Noord, RWS	SUSE Rancher, Haven, S3	Facturatie o.b.v. toewijzing van resources (niet op gebruik). Self - service voor 50% mogelijk na handmatige onboarding.

5.4. Voorbeelden van initiatieven van andere overheden

Meerdere Europese overheden zijn initiatieven gestart om de afhankelijkheid van Amerikaanse cloud leveranciers te verminderen door in te zetten op meer soevereine clouddiensten. Tabel 9 geeft een overzicht met initiatieven die kunnen dienen als input voor het definiëren van scenario's voor de Nederlandse overheid om tot een soevereine clouddienst te komen.

Tabel 9 Voorbeelden van initiatieven van Europese overheden

Initiatief/ Categorie	Land/Regio	Belangrijkste Kenmerken	Aanpak	Voordelen	Nadelen/Risico's
G-Cloud	België	Hybride 'community cloud' voor de overheid, waarbij diensten uit publieke clouds van private firma's gecombineerd worden met overheidsdatacenters.	Gezamenlijke aanpak door meerdere publieke instellingen, aangestuurd vanuit een Cloud Governance Board, met een gemeenschappelijke roadmap. De samenwerking is vrijwillig.	Biedt schaalvoordelen, flexibele en schaalbare infrastructuur op maat, betere dienstverlening en stimuleert technische specialisatie en innovatie.	Doordat het een vrijwillige samenwerking is en geen "keurslijf", bepalen instellingen zelf hun eigen tempo, wat de adoptiesnelheid kan beïnvloeden.
Deutschland-Stack)	Duitsland	Hybride multi-cloudmodel met sterke soevereine controle en open standaarden.	Segmentatie op basis van classificatie en missie: Bundescloud als gecentraliseerde private cloud voor de overheid, Delos als nationale partnercloud voor AI, en pCloudBw voor defensie. Er wordt gebruikgemaakt van migratiegolven en open bouwstenen (SCS, BSI C5) en standaarden (ODF).	Voorkomt afhankelijkheid van één enkele leverancier en zorgt voor sterke interoperabiliteit, zekerheid en gecentraliseerd beheer (FinOps/SecOps).	De knelpunten zijn niet de technologie, maar capaciteits- en verandermanagement, waardoor migraties langdurig zijn (gepland in golven van 2021 tot 2028).

Initiatief/ Categorie	Land/Regio	Belangrijkste Kenmerken	Aanpak	Voordelen	Nadelen/Risico's
Bundescloud 2.0		Beheerd door de IT-dienstverlener van de staat (ITZBund).	Open source technologie met VS-NfD certificatie.	Hoge digitale soevereiniteit zonder afhankelijkheid van commerciële partijen.	Minder innovatiesnelheid. Schaalbaarheid is beperkter vergeleken met publieke hyperscalers. De interoperabiliteit tussen verschillende Bundescloud initiatieven is een uitdaging.
Delos Cloud		Gebaseerd op Microsoft-technologie, maar beheerd door een Duitse partij (Delos).	Maakt Microsoft-diensten (Office 365, Azure) beschikbaar binnen een beveiligde, Duitse omgeving.	Toegang tot de modernste tools en innovatiekracht van Microsoft, met behoud van strikte Europese privacyregels.	Blijvende vendor lock-in met politieke en technische afhankelijkheid van een Amerikaanse leverancier.
pCloudBw		'Google Cloud Air Gapped' onderdeel van de private Cloud van de Bundeswehr.	Soevereine oplossing van Google die de BWI GmbH in staat stelt, geïsoleerd van andere Google-systemen of netwerken, Google Cloud te installeren en te exploiteren binnen haar eigen datacenters.	Schaalbaarheidsvoordelen van een hyperscaler. Flexibel voor lokale overheden. Sterke integratie met bestaande regionale IT-systemen.	Blijvende vendor lock-in met politieke en technische afhankelijkheid van een Amerikaanse leverancier.
Nationale Soevereine Cloud	Noorwegen	Nationale soevereine cloud specifiek gericht op het opslaan van niet geclassificeerde data.	Opgezet samen met private Noorse bedrijven die direct of indirect door de Noorse overheid worden gecontroleerd.	Biedt een lokaal Europees alternatief en garandeert een onafhankelijke exit strategie.	Het initiatief loopt vertraging op, bevindt zich nog in de planningsfase en er zijn nog geen officiële aanbestedingen (RFP's) op de markt gebracht.

Initiatief/ Categorie	Land/Regio	Belangrijkste Kenmerken	Aanpak	Voordelen	Nadelen/Risico's
Valtori & Cloud Guidelines	Finland	Een gecentraliseerd Center of Excellence (Valtori) voor on-premises diensten in combinatie met multiscaler-richtlijnen voor de overheid.	Aanbieden van gecentraliseerde on-premises diensten en centraal onderhandelde voorwaarden voor het gebruik van vier multiscalers, afgestemd op de behoeften van de overheid. Centraal in soevereiniteitsaanpak staat de naleveing van het PiTuKri [36]security Raamwerk	Zorgt voor centraal beheer en houdt rekening met de speciale eisen van de overheidssector tijdens leveranciersonderhandelingen.	Kampt met een problematische afhankelijkheid van Microsoft Azure, wat een ernstig vendor lock-in risico creëert.
Government Private Cloud	Roemenië	De opzet van een tweetal nieuwe cloud omgevingen, één voor puur intern gebruik binnen de overheid, de ander met een connectie naar public cloud diensten van hyperscalers	Diensten worden onder regie van de Roemeense overheid gebouwd door marktpartijen in vier datacenters van de Roemeense overheid.	Controle door de Roemeense overheid waarbij de kennis en kunde van marktpartijen wordt benut voor de realisatie van de clouddienst en voor de migratie van applicaties naar de nieuwe clouddienst.	Complexe organisatorische opzet door betrokkenheid van meerdere overheidsdiensten (aan leverende en afnemende kant) en marktpartijen.
Clarence	Luxemburg	Partnership tussen Luxconnect (100% eigendom Luxemburgse overheid) en Proximus Luxembourg voor het realiseren van een soevereine, 'air gapped' cloud voorziening.	De clouddienst maakt gebruik van de technologiestack van Google in een van het internet geïsoleerde omgeving.	Luxemburg heeft toegang tot moderne functionaliteit met meer soevereiniteit dan via public cloud diensten. De clouddienst is volledig geïsoleerd van het internet, en daarom, theoretisch, in staat te blijven functioneren bij grote verstoringen. [37]	Desondanks "disconnected" aanpak, nog steeds grote technologische afhankelijkheid van een Amerikaanse dienstverlener.

[36] National Cyber Security Centre Finland, PiTuKri framework, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_1_english.pdf

[37] Clarence – LuxConnect, https://www.luxconnect.lu/clarence/

Initiatief/ Categorie	Land/Regio	Belangrijkste Kenmerken	Aanpak	Voordelen	Nadelen/Risico's
Polo Strategico Nazionale	Italië	Nieuwe onderneming opgericht voor de levering van clouddiensten aan de Italiaanse overheid. De onderneming is eigendom van private ondernemingen (TIM, Leonardo, CDP en Sogei).	Er wordt gebruik gemaakt van technologie stacks van Oracle en Google. Er worden zowel volledig 'air gapped' en public cloud diensten aangeboden.	Overheidsdiensten hebben keuze uit verschillende niveaus van soevereiniteit met in alle gevallen toegang tot moderne functionaliteit.	In alle gevallen blijft er een sterke technologische e afhankelijkheid van Amerikaanse leveranciers.
Suite Numérique	Frankrijk	Het initiatief vervangt traditionele propriëtaire kantoorsuites door een verzameling gespecialiseerde, web gebaseerde tools die zijn afgestemd op digitale samenwerking	Gebruikmakend van een combinatie van open source applicaties (in plaats van een volledige suite ontworpen als een monoliet) met geïntegreerde toegang en single sign-on	Slechts zeer beperkte afhankelijkheid van non-EU leveranciers, lage mate van vendor lock-in door divers portfolio aan oplossingen	De functionaliteit vertoont gaps ten opzichte van de Microsoft Office, initieel zijn er veel bugs en issues met betrouwbaarheid gemeld door gebruikers.
Open-Source-Strategie Schleswig-Holstein	Duitsland	Vervangen van de Microsoft werkplek software door open source alternatieven.	Er wordt gebruik gemaakt van diverse open source alternatieven voor productiviteit (LibreOffice), email en agenda (Open-Xchange), videoconferentie (OpenTalk), bestandsdeling (Nextcloud) en besturingssysteem om stap voor stap de afhankelijkheid van Microsoft af te bouwen.	Afname van vendor lock-in, verminderde afhankelijkheid van niet-Europese leveranciers van software en diensten.	Verhoogde complexiteit bij het oplossen van verstoringen door gefragmenteerd supportmodel.
EuroStack	EU	Multinationaal consortium van Europese leveranciers en instellingen gericht op federatieve oplossingen.	De inzet van open-source technologieën (OpenStack, Kubernetes, Ceph) en 'air-gapped' of fysiek gescheiden operaties met nationale controle.	Biedt een lage jurisdictierisico, behoudt Europese controle en stimuleert sterke interoperabiliteit.	Bevindt zich momenteel nog in de ontwikkelingsfase met proefprojecten (pilotprojecten).

Initiatief/ Categorie	Land/Regio	Belangrijkste Kenmerken	Aanpak	Voordelen	Nadelen/Risico's
GAIA-X	EU	Non-profit organisatie en initiatief met een brede basis van Europese bedrijven en autoriteiten.	Focust op het creëren van gemeenschappelijke standaarden, certificeringen en open-source interoperabiliteit voor gefedereerde diensten.	Verlaagt jurisdictierisico's aanzienlijk door gedeelde open standaarden en geen vendor lock-in.	Ook dit initiatief is nog in ontwikkeling en vereist brede adoptie in standaardiseringsprojecten.

5.5. Lessen vanuit de markt

Uit de praktijk blijkt dat het volledig zelfstandig bouwen van een soevereine clouddienst een technologische en organisatorische complexiteit met zich meebrengt. Daarom is een publiek-private samenwerking (PPS) de internationale norm. Landen als Italië en Luxemburg laten zien dat de innovatiekracht van de markt een belangrijke factor kan zijn, mits deze binnen strikte overheidskaders wordt aangestuurd. Er is sprake van een paradox: ondanks de roep om soevereiniteit blijft de samenwerking met Amerikaanse hyperscalers de actuele praktijk. Zelfs in landen met een sterke focus op soevereiniteit wordt gekozen voor technologie van hyperscalers als Microsoft, Google of Oracle.

De reden hiervoor is tweeledig. Enerzijds is de functionele kloof tussen Europese alternatieven en de Amerikaanse hyperscalers op dit moment simpelweg te groot om te negeren. De innovatiesnelheid op het gebied van AI, security en schaalbaarheid is bij deze partijen ongeëvenaard. Anderzijds dwingt dit overheden tot het creëren van 'soevereine schillen' rondom deze Amerikaanse technologie. In de praktijk betekent dit dat overheden proberen de voordelen van deze platforms te benutten, terwijl de juridische en operationele risico's afgedekt worden middels contractuele voorwaarden, lokale exploitatie en technische isolatie (air-gapping).

Daarnaast dwingt de beperkte fysieke schaal van lokale Europese marktpartijen, een uitdaging waar ook Nederlandse partijen mee kampen, tot een federatieve aanpak. Dit sluit aan op (in het volgende hoofdstuk beschreven) scenario waarbij verschillende infrastructuren aan elkaar worden geknoopt om voldoende volume te genereren. Wat betreft het moderniseren van bestaande infrastructuur, leert de praktijk dat dit proces vaak moeizaam verloopt. Bestaande legacy-systemen en gefragmenteerde datacenters fungeren als een rem op de transitie, waardoor moderniseringstrajecten in de praktijk veel tijd en middelen vragen.

Een succesfactor die uit alle casussen naar voren komt, is de governance. Vrijblijvendheid in de samenwerking werkt vertragend voor de adoptiesnelheid. Juist bij de meer decentrale modellen, is een strakke, centrale regie vanuit de overheid noodzakelijk. Zonder dwingende technische standaarden en een heldere roadmap dreigt de soevereine cloud te versnipperen, waardoor het beoogde ambitieniveau niet gerealiseerd wordt.

Ondanks de dilemma’s en uitdagingen wordt uit de voorbeelden uit de markt en overheidsinitiatieven duidelijk dat voor alle in hoofstuk 6 opgenomen scenario’s voorbeelden bestaan op basis waarvan deze scenario’s realistisch blijken.

6. Scenario's

Dit hoofdstuk beschrijft de uitgangspunten en de scenario's voor de totstandkoming van een soevereine clouddienst. Hoewel deze scenario's de strategische richting bepalen, fungeren zij nadrukkelijk als fundament voor verdere uitwerking en niet als een uitvoeringsplan.

6.1. Uitgangspunten

De realisatie van een soevereine clouddienst kan via diverse scenario's vormgegeven worden. Om het aantal mogelijkheden overzichtelijk te houden wordt als eerste een viertal uitgangspunten gedefinieerd. Deze zijn van toepassing op alle scenario's.

Voortbouwend op de keuze voor een SEAL-4 soevereiniteitsniveau (inclusief de nuancering ten aanzien van de praktische uitvoerbaarheid op het gebied van de doelstellingen SOV-5 (supply chain soevereiniteit), SOV-6 (technologie soevereiniteit) en SOV-8 (milieu duurzaamheid), zie hoofdstuk 4), verschuift de focus nu naar de uitwerking van de realisatie van dit ambitieniveau. Omdat SEAL-4 strikte eisen stelt, dwingt dit de overheid tot een mate van centrale sturing waarvoor op dit moment nog geen overheidsbrede besluitvormingsorgaan bestaat. De Gartner-verkenning wordt daarom benut om de weg naar integrale besluitvorming voor te bereiden, zodat de benodigde regie op de scenario's ingevuld kan worden. Daarnaast, en in lijn daarmee, worden voor het definiëren van de scenario's de volgende uitgangspunten gehanteerd:

1. De soevereine clouddienst bedient het gehele Huis van Thorbecke, waarvoor interbestuurlijke samenwerking en schaalbaarheid randvoorwaardelijk zijn[38]. Interoperabiliteit is daarmee een integraal onderdeel van de opzet van de clouddienst.
    a. Tijdens de realisatie kan sprake zijn van een fasering waarin niet alle onderdelen van de overheid in een keer in staat gesteld worden de diensten van de clouddienst te gebruiken.
    b. Er is sprake van een minimum gegarandeerde afname waar (een aantal) organisaties zich aan committeren. Hierbij wordt ook gezorgd dat gelijksoortige overlappende initiatieven worden ontmoedigd om zo de benodigde schaalgrootte en economische levensvatbaarheid te stimuleren.
2. De soevereine clouddienst komt tot stand in een samenwerking tussen de Nederlandse overheid en de markt.
    a. De regie en beslissende stem liggen te allen tijde bij de overheid. De overheid investeert in de ontwikkeling en instandhouding van de competenties die hiervoor benodigd zijn.
    b. De bestaande overheidsdatacenters (ODC's) spelen een rol als fysiek fundament van de soevereine clouddienst en fungeren als de centrale plek voor de verankering van specialistische kennis.
    c. Er zijn duidelijke afspraken nodig met betrekking tot exit scenario's van commerciële partijen in de samenwerking als gevolg van bijvoorbeeld overnames of faillissementen. Voor interne overheidsclouddiensten gelden vergelijkbare continuïteitseisen, waarbij de focus ligt op het voorkomen van een kwalitatieve achterstand ten opzichte van de markt.

[38] Uitgangspunten 1a en 1b staan mogelijk op gespannen voet met elkaar, dit zal een punt van aandacht zijn bij de verdere uitwerking en operationalisering van het voorkeursscenario.

d. De opzet is gericht op samenwerking tussen marktpartijen en draagt niet bij aan (verdere) fragmentatie. De overheid en de markt zijn dan ook bereid om zelf en samen de kennis binnen de overheid en binnen Nederland te verhogen.
e. De opzet van de samenwerking is op de lange termijn economisch levensvatbaar.

3. Er moet sprake zijn van een echte clouddienst met de relevante kenmerken (zoals selfservice, betalen naar gebruik, etc.) om het een bruikbaar alternatief voor de public cloud te maken.

   a. Er is een krachtige positie nodig voor de dienstverlenende partij(en) om het model van klant specifiek maatwerk te doorbreken. In plaats van optimalisatie op individuele applicaties of maatwerk-infrastructuur, wordt een generiek platform (IaaS/PaaS) aangeboden voor de gehele overheid. Dit vereist dat applicatieontwikkelaars (zowel in de markt als binnen de overheid) hun software moeten aanpassen om op de standaard cloud infrastructuur te kunnen draaien, in plaats van dat de infrastructuur per applicatie wordt aangepast. Dit vereist ook de juiste prioriteitstelling bij de opdrachtgevers van die applicatieontwikkelaars om deze aanpassingen mogelijk te maken.
   b. Het ontwerp voor de soevereine clouddienst moet centraal door een kleine kern worden ontwikkeld, niet door een breed gremium[39]. Dit ontwerp wordt openbaar gemaakt zodat het voor alle partijen verifieerbaar is dat aan de eisen voldaan wordt.
   c. Het aanbod aan clouddiensten biedt een concurrerende balans tussen prijs, functionaliteit en gebruiksgemak, waardoor het voor overheidsorganisaties een volwaardig alternatief vormt voor de publieke cloud om in hun behoeften te voorzien.
   d. Zoals vastgelegd in de afbakening (Hoofdstuk 1.2) wordt het programma voor de soevereine clouddienst niet belast met lopende dossiers als digitale werkplekken, specifieke AI-voorzieningen of applicatie migraties, om de focus op de realisatie te bewaren. De soevereine clouddienst voorziet wel in een platform waar deze workloads mogelijk kunnen landen waarmee deze tegemoetkomt aan de belangrijkste of meest voorkomende behoeften van de overheid. De soevereine clouddienst is niet bedoeld als voorziening voor alle behoeften.
   e. Toegang voor overheidspartijen naar diensten vanuit de clouddienst is georganiseerd via een enkele (of een zeer klein aantal) portal(s). Achter deze portal is Service Integration & Management (SIAM) ingericht om orkestratie van bijvoorbeeld incidentoplossing en doorvoeren van wijzigingen te bewerkstelligen.
   f. De clouddienst biedt voldoende veerkracht voor totale onbeschikbaarheid van een datacenter. Daarom wordt uitgegaan van een opzet met minimaal 3 datacenters, met voldoende risicospreiding, om een voldoende mate van veerkracht te behouden als één datacenter voor langere tijd onbeschikbaar is.

4. De technologie is (zoveel mogelijk) modulair opgebouwd op basis van open standaarden binnen het moderne cloud-ecosysteem. De gebruikte technologie voorkomt overmatige vendor lock-in, borgt interoperabiliteit en maakt een exit-strategie mogelijk. Hierbij wordt aangesloten bij bestaande standaarden zoals Haven.

6.2. Assen voor scenariodefinitie

Scenario's dienen als strategische navigatiepunten voor de Nederlandse overheid en reflecteren fundamentele keuzes die de overheid kan maken in de realisatie van de soevereine clouddienst. Deze keuzes zijn langs een tweetal

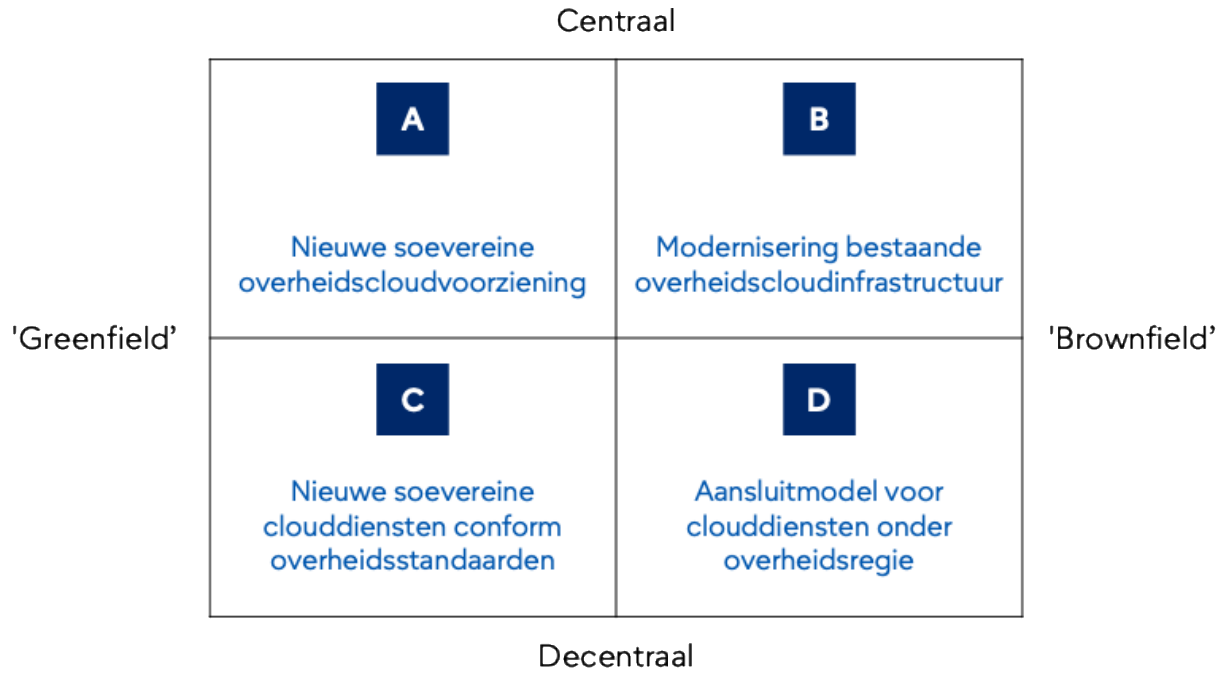
[39] Marktpartijen hebben in de Open Dialoog aangeboden om via de inzet van architecten hun expertise beschikbaar te stellen voor de verdere uitwerking van het ontwerp.

assen gedefinieerd die ieder een beslispunt weergeven. Uit een langere lijst van variabelen zijn onderstaande assen geselecteerd als de wezenlijke afwegingen die bepalend zijn voor de routes de Nederlandse overheid kan volgen:

- Aanbod: centraal vs. decentraal. Dit betreft de structuur van de dienstverlening. Worden clouddiensten vanuit één centrale voorziening aangeboden, of wordt er gekozen voor een aanbod selectie van diverse leveranciers (bijv. via een marktplaats)?
- Implementatie (greenfield vs. brownfield): Dit weegt een integrale nieuwbouwontwikkeling ('greenfield') af tegen de stapsgewijze aanpassing en optimalisatie van de al bestaande infrastructuur ('brownfield').

In samenwerking met het NDS-team zijn vier scenario's uitgewerkt die de meest realistische ontwikkelpaden voor de Nederlandse overheid vormen (zie Figuur 6). Hierbij is een strikte ondergrens gehanteerd: scenario's die niet voldoen aan de eerder gestelde soevereiniteitsambitie zijn buiten beschouwing gelaten. Hiermee garandeert de overheid dat elk scenario een robuuste basis biedt voor juridische en operationele soevereiniteit en autonomie.

Figuur 6 scenario indeling voor soevereine overheidsclouddiensten



A. Nieuwe soevereine overheidsclouddienst: Een 'nieuw naast bestaand'-model waarbij een volledig nieuwe centrale infrastructuur wordt opgetuigd.
B. Modernisering bestaande overheidscloudinfrastructuur: De focus ligt op het moderniseren, ombouwen en convergeren van de huidige infrastructuren (zoals bestaande overheidsdatacenter (ODC)-omgevingen).
C. Nieuwe soevereine clouddiensten conform overheidsstandaarden: Hierbij stelt de overheid een nieuwe set aan standaarden en specificaties op, waarna de levering door een combinatie van overheids- en marktpartijen kan worden verzorgd

D. Aansluitmodel voor clouddiensten onder overheidsregie: Het decentraal door ontwikkelen en gereed maken van bestaande infrastructuren (zowel vanuit dienstverleners van de overheid als marktpartijen), toewerkend naar de nieuwe set aan standaarden.

Om de scenario's te presenteren wordt gebruik gemaakt van de volgende structuur:

- Algemene beschrijving
- Organisatorische kenmerken
- Technische kenmerken (implementatie)
- Mogelijke rol van de markt
- Tijdslijnen
- Randvoorwaarden
- Risico's
- Voor- en nadelen

6.3. Scenario A: Nieuwe soevereine overheidsclouddienst

In dit scenario wordt de soevereine clouddienst nieuw gebouwd als een greenfield-omgeving (nieuw naast bestaand) waarbij een centrale organisatie de volledige regie voert. Hoewel deze omgeving op logisch niveau als één centrale entiteit wordt aangestuurd, bestaat de fysieke uitvoering uit een netwerk van meerdere Overheidsdatacenters die gebruik maken van een gestandaardiseerde technologiestack. Dit concept doorbreekt het bestaande model van contractuele en organisatorische kaders. Doordat de overheid zelf de volledige controle heeft over de onderste lagen van de infrastructuur en niet afhankelijk is van publieke cloudleveranciers of propriëtaire softwarepakketten, wordt een hoge mate van digitale soevereiniteit bereikt. Dit scenario stelt de overheid in staat om de technologische koers volledig zelf te bepalen, wat essentieel is voor het voldoen aan de soevereiniteitsambitie van SEAL-4*.

6.3.1. Organisatorische kenmerken

Middels een vorm van samenwerking met marktpartijen (in een volgende paragraaf wordt gedefinieerd welke rollen de overheid en de marktpartijen in deze samenwerking vervullen) wordt één enkele soevereine clouddienst gerealiseerd voor de Nederlandse overheid. Het dienstenaanbod wordt vanuit één enkele overheidsorganisatie, al dan niet als samenwerkingsverband met de markt, geleverd aan alle vragende partijen binnen de Nederlandse overheid. Hierbij ligt het management van de IT-portfolio centraal bij de overheid, terwijl de dagelijkse operationele taken kunnen verdeeld worden over verschillende leveranciers.

6.3.2. Technische kenmerken

De basis wordt gevormd door een container-platform dat direct op de hardware is geïnstalleerd. Hierop wordt een virtualisatie laag toegevoegd om zowel moderne applicaties als traditionele virtuele machines in één omgeving te beheren. Het beheer van het gehele platform gebeurt via een centrale, geautomatiseerde aanpak en gebruiksvriendelijke interfaces die de onderliggende technologie toegankelijk maken. [40]

[40] Technische details zijn uitvoerig beschreven in de NDS architectuuroverleg 'ontwerpsessies'.

6.3.3. Mogelijke rol van de markt

In dit scenario kan de rol van de markt bestaan uit:

- Het leveren van kennis en capaciteit als aanvulling op een organisatie die de Nederlandse overheid opzet voor de realisatie van de clouddienst,
- Het bouwen van de soevereine clouddienst conform de specificaties van de overheid om deze vervolgens in beheer over te dragen, en/of
- Het beheren en onderhouden van (delen van) de clouddienst voor de overheid met een resultaatverplichting.

In dit scenario ligt het niet voor de hand dat marktpartijen als end-to-end leverancier van clouddiensten optreden.

6.3.4. Tijdslijnen

Vanwege het opbouwen van een nieuw platform zijn er een aantal stappen die moeten worden doorlopen voordat er voor het eerst gebruik gemaakt kan worden van de soevereine clouddienst. Het start met het opstellen van een programma van eisen en het maken van een gedetailleerd technisch ontwerp. Afhankelijk van de rol die van de markt wordt verwacht, zullen er aanbestedingen moeten worden gestart. Dit kan te maken hebben met de verwerving van de benodigde hardware en software (voor zover noodzakelijk naast open source) het bouwen van de clouddienst en/of beheer en support.

Na deze mogelijke aanbestedingen volgt de daadwerkelijke realisatie van het platform en de opzet van de eerste diensten. Deze stappen vergen bij elkaar minimaal een aantal maanden tot meer dan een jaar voordat de nieuwe voorziening klaar is voor de eerste workloads in productie. Daarna is tijd nodig voor het verder schalen van functionaliteit en capaciteit om meer workloads in productie te kunnen nemen. Als er een nieuw datacenter moet worden gerealiseerd voor het creëren van voldoende capaciteit kan dit een doorlooptijd van enkele jaren vergen voordat deze capaciteit beschikbaar is. Bij het gebruik van co-locatie faciliteiten kan deze capaciteit sneller worden gerealiseerd. Vooruitlopend op, en in parallel met, de technische realisatie is er ook tijd nodig voor het opzetten van de organisatie die centraal de regie gaat voeren over de nieuwe clouddienst en afhankelijk van de rol van de markt ook een rol gaat spelen bij de totstandkoming en het beheer. Het opzetten van deze organisatie en het aanwerven en selecteren van het benodigde personeel gaat minimaal enkele maanden vergen.

6.3.5. Risico’s

De technologische realisatie van dit scenario stelt hoge eisen aan zowel het uitwerken van een detailontwerp voor de technologiestack, het opzetten van de dienstverlening en het voeren van de regie over de realisatie en het beheer vanuit de Nederlandse overheid, wat een diepgaand niveau van expertise en specialistische vaardigheden vereist. Indien deze kennis niet intern geborgd kan worden, ontstaat er een directe afhankelijkheid van externe inhuur of diensten, met hogere operationele kosten en grotere afhankelijkheid tot gevolg.

Een risico van dit scenario is de zichtbaarheid van verdere versnippering indien het parallelle beleid (het daadwerkelijk overbrengen van workloads naar de nieuwe clouddienst) niet succesvol wordt uitgevoerd. In tegenstelling tot andere scenario’s, waar versnippering verspreid plaatsvindt binnen individuele aanbestedingen, zorgt de introductie van een centrale soevereine cloud voor een herkenbaar 'extra' aanbod. Dit maakt het succes van de consolidatie politiek kwetsbaar.

Vanuit de Wet Markt en Overheid en de Kaderwet zelfstandige bestuursorganen kunnen beperkingen bestaan in het leveren van diensten vanuit de Rijksoverheid aan andere onderdelen van het huis van Thorbecke.

6.3.6. Voor- en nadelen

Voordelen	Nadelen
Hoge soevereiniteit	Operationele complexiteit. Bij opschalen van de dienstverlening is een structureel, nieuwe manier van werken vereist
Onafhankelijkheid, beperkte vendor lock-in	Politiek gevoeliger bij onsuccesvolle implementatie
Profiteren van open source innovatie	

6.3.7. Scenario specifieke randvoorwaarden

Het detailontwerp van de soevereine cloud wordt gedaan door een klein, gespecialiseerd team. Door de regie strikt bij deze specialisten te beleggen, wordt voorkomen dat het ontwerp verwatert door een compromisgerichte werkwijze met te veel verschillende belanghebbenden.

Daarnaast is een onvoorwaardelijk, meerjarig commitment van de overheid aan de soevereine cloud cruciaal. Zonder de expliciete garantie dat de overheid jarenlang aan dit model vasthoudt, ontbreekt het overheids- en marktpartijen (zowel aanbieders als afnemers) aan het nodige vertrouwen om te investeren, waardoor het concept uiteenvalt.

6.4. Scenario B: Modernisering bestaande overheidscloudinfrastructuur

In dit scenario staat de transformatie en convergentie naar een nieuwe standaard van de huidige infrastructuur centraal, waarbij bestaande middelen, bijvoorbeeld de Overheidsdatacenter (ODC) -omgevingen als fundament dienen. Het kernconcept is dat het eigenaarschap en de fysieke locatie van de infrastructuur ongewijzigd blijven binnen de overheid of een gedeelde overheidsdienst, en dat de onderliggende techniek wordt gemoderniseerd. De mate van soevereiniteit in dit model is in potentie hoog, omdat men voortbouwt op vertrouwde, fysiek afgeschermde locaties. De voornaamste uitdaging ligt in het doorbreken van bestaande (legacy-gerelateerde) beperkingen op zowel infrastructuur als organisatie vlak. Deze belemmeringen zorgen ervoor dat het realiseren van het beoogde SEAL-4*-niveau een langere doorlooptijd vereist.

6.4.1. Organisatorische kenmerken

Door voort te bouwen op de bestaande ODC’s en vergelijkbare voorzieningen, wordt toegewerkt naar een dienstenportfolio dat voldoet aan het centraal opgestelde high-level ontwerp en eisen. Deze transitie vereist een aanpassing in huidige contracten, budgettering en governance binnen de ODC’s.

6.4.2. Technische kenmerken

De technische kenmerken van dit model worden bepaald door een architectuur die de brug slaat tussen traditionele virtualisatie en cloud-native standaarden. In plaats van de huidige infrastructuur volledig te vervangen, wordt een nieuw (container)platform direct geïntegreerd met de bestaande virtualisatie laag. Hierdoor blijven de bestaande

opslagsystemen behouden, terwijl het netwerkbeheer wordt geactualiseerd om de aansluiting op de nieuwe technologie te realiseren.

6.4.3. Mogelijke rol van de markt

In dit scenario kan de rol van de markt bestaan uit:

- Het leveren van kennis en capaciteit als aanvulling op een organisatie die de Nederlandse overheid opzet voor moderniseren en convergeren van bestaande voorzieningen,
- Het moderniseren en convergeren van bestaande infrastructuren tot de beoogde clouddienst conform de specificaties van de overheid om deze vervolgens in beheer over te dragen, en/of
- Het beheren en onderhouden van (delen van) de clouddienst voor de overheid met een resultaatverplichting.

In dit scenario ligt het niet voor de hand dat marktpartijen als end-to-end leverancier van clouddiensten optreden.

6.4.4. Tijdslijnen

Het moderniseren en convergeren van de bestaande infrastructuur betekent dat huidige diensten gecontinueerd kunnen worden, of tot op zekere hoogte ingezet kunnen worden om workloads te repatriëren. Op dat moment zal het nog niet voldoen aan het uitgangspunt dat er een echte clouddienst met alle relevante kenmerken wordt gebouwd.

Ook dit scenario start met het opstellen van een programma van eisen en het maken van een gedetailleerd technisch ontwerp. Afhankelijk van de rol die van de markt wordt verwacht zullen er aanbestedingen moeten worden gestart of bestaande contracten moeten worden opengebroken. Dit kan te maken hebben met de benodigde ondersteuning bij het moderniseren en convergeren van bestaande infrastructuur, waar nodig ook met de verwerving van hardware en software (voor zover noodzakelijk naast open source) en/of beheer en support.

Na een aanbesteding volgt de daadwerkelijke modernisering en convergentie van de huidige platformen en diensten. Omdat deze stappen moeten worden genomen bij infrastructuren die reeds in productie zijn en waar applicaties ook regelmatig moeten worden voorzien van updates en upgrades, is een zorgvuldige planning belangrijk voor de timing van infrastructuurwijzigingen en de synchronisatie daarvan met de noodzakelijke aanpassingen de applicatielaag.

Dit proces zal waarschijnlijk meerdere jaren vergen, afhankelijk van de delta tussen de huidige infrastructuren en het detailontwerp voor de soevereine clouddienst. Ook hier geldt dat als er een nieuw datacenter moet worden gerealiseerd voor het creëren van voldoende capaciteit, dit een doorlooptijd van enkele jaren kan vergen voordat deze capaciteit beschikbaar is. Bij het gebruik van co-locatie faciliteiten kan deze capaciteit sneller worden gerealiseerd.

Vooruitlopend op, en in parallel met, de technische realisatie is er ook tijd nodig voor het opzetten van de organisatie die centraal de regie gaat voeren over de nieuwe clouddienst en afhankelijk van de rol van de markt ook een rol gaat spelen bij de totstandkoming en het beheer. Het opzetten van deze organisatie en het aanwerven en selecteren van het benodigde personeel gaat minimaal enkele maanden vergen.

6.4.5. Risico's

Het succes van dit scenario staat of valt bij de modernisering van het huidige aanbod. Zolang het huidige gebrek aan een on-demand, selfservicemodel voortduurt en aanvraagprocedures voor (cloud)resources weken/maanden in beslag nemen, is het voorgestelde model in de praktijk niet levensvatbaar.

Technisch en organisatorisch bestaat het risico dat de huidige aanbieders over onvoldoende capaciteit en competenties beschikken om zowel in volumes als functionaliteit snel genoeg op te schalen in lijn met de vraag.[41]

Door een convergentie van bestaande dienstverlening naar een centraal gestuurd model gaan bestaande verantwoordelijkheden ten aanzien van run, support en beveiliging niet meer passen.

Vanuit de Wet Markt en Overheid en de Kaderwet zelfstandige bestuursorganen kunnen beperkingen bestaan in het leveren van diensten vanuit de Rijksoverheid aan andere onderdelen van het huis van Thorbecke.

6.4.6. Voor- en nadelen

Voordelen	Nadelen
Snel kunnen starten door hergebruik bestaande voorzieningen	Mogelijk langer durende/blijvende vendor lock-in op virtualisatie laag
Minder versnippering van landschap (t.o.v andere scenario's)	Matig trackrecord in de markt en bij de overheid ten aanzien van snel moderniseren van bestaande (legacy) infrastructuren
Lagere initiële investering	

6.4.7. Scenario specifieke randvoorwaarden

Om bestaande infrastructuren tijdig te transformeren naar de nieuwe standaarden, is een krachtig centraal mandaat vereist dat zowel de uitvoering als de verdere opschaling prioriteert.

Om interoperabiliteit te borgen moeten nieuwe security policies volledig aansluiten op de geldende standaarden en beleidskaders. Hiermee wordt voorkomen dat er binnen de clouddienst afwijkende veiligheidsniveaus ontstaan. Tegelijkertijd wordt van de ODC's vereist dat zij hun operatie in lijn brengen met marktconforme compliance-eisen en certificeringen.

Dit scenario vereist expertise en vaardigheden op het beheer van zowel legacy-omgevingen als nieuwe infrastructuren.

6.5. Scenario C: Nieuwe soevereine clouddiensten conform overheidsstandaarden

In dit scenario heeft de overheid vooral de rol van regisseur. Het kernconcept draait om het loslaten van het centrale eigenaarschap van de fysieke infrastructuur. De overheid stelt als normsteller een strikte set aan standaarden en

[41] Dit risico is nu nog niet goed in te schatten aangezien de huidige omvang van workloads niet bekend is

technische specificaties op waaraan platforms moeten voldoen. De feitelijke infrastructuur staat bij meerdere overheids- en marktpartijen die deze diensten op basis van de gestelde kaders aanbieden. De mate van soevereiniteit wordt in dit model niet gewaarborgd door fysieke muren, maar door juridische en technische handhaving van de gestelde standaarden. Dit biedt een grotere mate van autonomie (voor afnemers) mede omdat men niet afhankelijk is van één centrale voorziening. De implementatie van dit scenario is een groeiproces waarin in eerste instantie slechts een beperkt aantal infrastructuren het gewenste SEAL-4 niveau zal bereiken.

6.5.1. Organisatorische kenmerken

Er komt een orgaan dat verantwoordelijk is/wordt gemaakt voor het ontwerp en naleving van de gedefinieerde standaarden. Daarnaast behouden al leverende dan wel nieuwe overheids- en marktpartijen grotendeels hun rol als end-to-end leverancier, maar met een nieuw portfolio aan ‘soevereine clouddiensten’ (naast de reeds bestaande).

6.5.2. Technische kenmerken

De technische kenmerken van dit model steunen volledig op interoperabiliteit en certificering. De infrastructuur is gebaseerd op een ‘policy-as-code' benadering, waarbij aanbieders hun technologie moeten laten auditen op basis van de overheidsspecificaties. Hierbij wordt in ieder geval ingezet op open standaarden voor API's, data-portabiliteit en configuratiemanagement (zoals Haven), om te stimuleren dat afnemers relatief eenvoudig kunnen wisselen tussen verschillende gecertificeerde aanbieders.

6.5.3. Mogelijke rol van de markt

In dit scenario zal er vanwege het decentrale karakter mogelijk sprake zijn van zowel een rol bij de totstandkoming en het beheer van clouddiensten die onder directe verantwoordelijkheid van de overheid vallen als het zelfstandig realiseren en leveren van clouddiensten die conform de specificaties van de overheid aan overheidsorganisaties end-to-end kunnen worden geleverd. In de ondersteuning van de overheid zal de rol van de markt kunnen bestaan uit:

- Het leveren van kennis en capaciteit als aanvulling op een organisatie die de Nederlandse overheid opzet voor de realisatie van clouddiensten,
- Het bouwen van soevereine clouddiensten conform de specificaties van de overheid om deze vervolgens in beheer over te dragen, en/of
- Het beheren en onderhouden van (delen van) clouddiensten voor de overheid met een resultaatverplichting.

6.5.4. Tijdslijnen

Vanwege het opbouwen van nieuwe platformen zijn er een aantal stappen die moeten worden doorlopen voordat er voor het eerst gebruik gemaakt kan worden van soevereine clouddiensten. Ook hier start het proces met het opstellen van een programma van eisen en het opstellen van (gedetailleerde) standaarden. Het ontwerpen van deze standaarden is tijdrovend, aangezien het niet slechts een technische exercitie is, maar een complex afstemmingsproces tussen uiteenlopende overheidslagen en marktpartijen. Om interoperabiliteit en veiligheid te verzekeren, moeten deze standaarden bovendien aansluiten op zowel nationale kaders als de strikte, in beweging zijnde EU-regelgeving.

Waar de overheid ondersteuning nodig heeft bij het realiseren van nieuwe clouddiensten zullen dezelfde stappen moeten worden doorlopen als voor de centrale opzet, al kunnen dit door het decentrale karakter meerdere trajecten

parallel aan elkaar zijn. Deze stappen, de aanbestedingen en de realisatie, vergen bij elkaar minimaal een aantal maanden tot meer dan een jaar voordat de nieuwe voorziening klaar is voor de eerste workloads in productie.

Daarna is tijd nodig voor het verder schalen van functionaliteit en capaciteit om meer workloads in productie te kunnen nemen. Als er nieuwe datacenters moeten worden gerealiseerd voor het creëren van voldoende capaciteit kan dit een doorlooptijd van enkele jaren vergen voordat deze capaciteit beschikbaar is. Bij het gebruik van co-locatie faciliteiten kan deze capaciteit sneller worden gerealiseerd.

Vanuit de overheid is vooruitlopend op, en in parallel met, de technische realisatie ook tijd nodig voor het opzetten van de organisatie die de regie gaat voeren over standaarden en bewaking van de interoperabiliteit en portabiliteit. Het opzetten van deze organisatie en het aanwerven en selecteren van het benodigde personeel gaat minimaal enkele maanden vergen.

6.5.5. Risico's

Er ontstaat een afname van soevereiniteit wanneer een lokale partij wordt overgenomen (door een non-EU organisatie) of wanneer de juridische controle over de data-opslagplaatsen verwatert.

Het is de vraag of er voldoende bereidheid is bij marktpartijen om naast hun bestaande portfolio te investeren in een specifieke set aan diensten exclusief voor de overheid, waarbij zij met elkaar en overheidsdiensten concurreren.

Het is de vraag of een dergelijk scenario de schaalgrootte gaat opleveren die nodig is voor het meebewegen met de fluctuerende vraag van de overheid als de capaciteit verspreid zit over meerdere leverende organisaties en niet gedeeld kan worden met andere klanten. Daarnaast speelt mee dat de investeringen over meerdere partijen verspreid zijn om tot gelijksoortige oplossingen te komen.

6.5.6. Voor- en nadelen

Voordelen	Nadelen
Flexibiliteit voor afnemers	Onvoorspelbare soevereiniteit door mogelijke overnames van marktpartijen
Snelle adoptie van nieuwe technologie door marktwerking	Gefragmenteerde inkoop kan voor hogere kosten zorgen en maakt beheersen van de soevereiniteit moeilijker
Concurrentie tussen leverende partijen kan innovatie en focus op kwaliteit bevorderen	Operationele uitdaging om standaarden te handhaven

6.5.7. Scenario specifieke randvoorwaarden

Er moet een robuust stelsel van certificering en continu toezicht worden ingericht om te controleren of marktpartijen aan de soevereiniteitseisen blijven voldoen. De benodigde expertise en skills binnen de overheid verschuiven van diepe technische beheer-kennis naar regie-expertise op het gebied van vendor management en technische auditing.

Er dienen dwingende afspraken te liggen over exit-scenario's in het geval van faillissement of overname door non-EU organisaties.

Om de benodigde schaalgrootte te realiseren, moet de overheid manieren vinden om de vraag te bundelen richting de leverende partijen. Door de vraag te aggregeren, wordt het voor marktpartijen rendabel om te investeren in een specifiek overheidsportfolio.

6.6. Scenario D: Aansluitmodel voor clouddiensten onder overheidsregie

In dit scenario moderniseren de overheid en marktpartijen de bestaande infrastructuren om deze aan te sluiten op een breder ecosysteem waar de markt ook onderdeel van is. Het kernconcept draait om het loslaten van de exclusieve afhankelijkheid van centrale overheidsdatacenters. In plaats daarvan wordt ingezet op een model waarin overheidstaken flexibel kunnen worden belegd. Afhankelijk van de behoefte draaien deze binnen de eigen ODC's of bij een diversiteit aan externe, vaak lokale marktpartijen. Hierbij staat niet alleen de fysieke locatie centraal, maar vooral de interoperabiliteit en data-soevereiniteit via federatieve diensten, waardoor de overheid de regie behoudt over data, ongeacht welke (private) partij de onderliggende infrastructuur levert. Ook binnen dit scenario zal het beoogde SEAL-4*-niveau aanvankelijk op een beperkt aantal infrastructuren worden gerealiseerd, met de mogelijkheid tot verdere opschaling in een latere fase.

6.6.1. Organisatorische kenmerken

Een centraal orgaan beheert de ‘marktplaats’ aan diensten die door de overheid worden aangeboden en draagt zorg voor initiële en periodieke certificering waardoor marktpartijen en overheidsdienstverleners pas toegang verkrijgen tot het ecosysteem nadat zij hebben aangetoond aan alle gestelde kaders te voldoen. Door deze toetredingseisen centraal te beleggen, ontstaat een robuuster mechanisme voor de handhaving van standaarden dan bij decentrale sourcing. Dit stelt het orgaan in staat om met een diversiteit aan kleine en grote lokale marktpartijen samen te werken om een nieuwe vendor lock-in te voorkomen. Daarnaast, hebben afnemers de autonomie om clouddiensten te selecteren die optimaal aansluiten bij hun specifieke behoeften.

6.6.2. Technische kenmerken

De technische kenmerken van dit model worden gevormd door de opzet van een 'marktplaats-concept'. Bestaande omgevingen worden technisch gereed gemaakt om te koppelen met soevereine cloud leveranciers die voldoen aan de eisen voor soevereiniteit en interoperabiliteit. Dit vereist een sterke nadruk op standaardisatie van API’s en identiteitsmanagement, zodat diensten tussen verschillende leveranciers en de eigen systemen kunnen communiceren.

6.6.3. Mogelijke rol van de markt

In dit scenario zal er vanwege het decentrale karakter mogelijk sprake zijn van zowel een rol bij de modernisering van bestaande infrastructuren en het beheer van de clouddiensten die onder directe verantwoordelijkheid van de overheid vallen als het zelfstandig aanpassen en leveren van clouddiensten die conform de specificaties van de overheid aan overheidsorganisaties end-to-end kunnen worden geleverd. In de ondersteuning van de overheid kan de rol van de markt bestaan uit:

- Het leveren van kennis en capaciteit als aanvulling op een organisatie die de Nederlandse overheid opzet voor de modernisering van infrastructuren,
- Het moderniseren van bestaande tot soevereine clouddiensten conform de specificaties van de overheid om deze vervolgens in beheer over te dragen, en/of

- Het beheren en onderhouden van (delen van) clouddiensten voor de overheid met een resultaatverplichting.

6.6.4. Tijdslijnen

Het moderniseren van bestaande infrastructuren betekent dat huidige diensten gecontinueerd kunnen worden, of tot op zekere hoogte ingezet kunnen worden om workloads te repatriëren. Op dat moment zal het nog niet voldoen aan het uitgangspunt dat er clouddiensten met alle relevante cloud-kenmerken worden gerealiseerd.

Ook hier start het proces met het opstellen van een programma van eisen en het opstellen van (gedetailleerde) standaarden. Het juridisch verankeren van toetredingscriteria, wat essentieel is om partijen op rechtmatige gronden te kunnen weigeren of certificeringen in te trekken, is een omvangrijk proces. Waar de overheid ondersteuning nodig heeft bij het moderniseren van bestaande infrastructuren zullen dezelfde stappen moeten worden doorlopen als voor de centrale opzet, al kunnen dit door het decentrale karakter meerdere trajecten parallel aan elkaar zijn.

Afhankelijk van de rol die van de markt wordt verwacht zullen er aanbestedingen moeten worden gestart. Dit kan te maken hebben met de benodigde ondersteuning bij het moderniseren van bestaande infrastructuren, waar nodig ook met de verwerving van hardware en software (voor zover noodzakelijk naast open source) en/of beheer en support. Na de aanbesteding volgt de daadwerkelijke modernisering van de huidige platformen en diensten. Omdat deze stappen moeten worden genomen bij infrastructuren die reeds in productie zijn en waar applicaties ook regelmatig moeten worden voorzien van updates en upgrades, is een zorgvuldige planning belangrijk voor de timing van infrastructuurwijzigingen en de synchronisatie daarvan met de noodzakelijke aanpassingen de applicatielaag.

Dit proces zal waarschijnlijk meerdere jaren vergen, afhankelijk van de delta tussen de huidige infrastructuren en het detailontwerp voor de soevereine clouddienst. Ook hier geldt dat als er nieuw datacenters moeten worden gerealiseerd voor het creëren van voldoende capaciteit dit een doorlooptijd van enkele jaren kan vergen voordat deze capaciteit beschikbaar is. Bij het gebruik van co-locatie faciliteiten kan deze capaciteit sneller worden gerealiseerd. Voor de voorzieningen die end-to-end door marktpartijen worden geleverd aan overheidsorganisaties gelden soortgelijke tijdslijnen om bestaande diensten waar dit mogelijk is zodanig aan te passen dat ze aan de standaarden van de overheid voldoen.

Vanuit de overheid is vooruitlopend op, en in parallel met, de technische realisatie ook tijd nodig voor het opzetten van de organisatie die de regie gaat voeren over standaarden en bewaking van de interoperabiliteit en portabiliteit. Het opzetten van deze organisatie en het aanwerven en selecteren van het benodigde personeel gaat minimaal enkele maanden vergen.

6.6.5. Risico’s

Dit scenario brengt een significante toename van de regie- en beheerlast met zich mee. De technische realisatie is complex en vereist een design-comité om dwingende standaarden vast te stellen en de afstemming met een diversiteit aan marktpartijen te borgen.

In dit gefedereerde model, waarbij overheidstaken flexibel over verschillende partijen zijn verspreid, neemt de bestuurlijke en operationele grip af. Het tijdig identificeren van en ingrijpen bij incidenten is complexer doordat de directe controle over de volledige keten ontbreekt.

6.6.6. Voor- en nadelen

Voordelen	Nadelen
Minimale afhankelijkheid van één partij	Complex, moeilijk te integreren door specifieke IPCEI CIS en ECOFED[42] eisen
Stimulans van lokale economie	Schaalt niet zo goed als een alternatief scenario
	Vereist juridisch inrichten van screening proces

6.6.1. Scenario specifieke randvoorwaarden

Er moet een centraal orgaan zijn dat de 'marktplaats' beheert en de kwaliteit van aangesloten leveranciers bewaakt, wat een fundamentele wijziging in het inkoop- en aanbestedingsbeleid betekent. Dit orgaan moet ook het mandaat hebben om een leverancier direct af te sluiten of een migratie te dwingen als de soevereiniteit in gevaar komt.

Op het gebied van expertise en vaardigheden vraagt dit om een transitie van puur technisch beheer naar integratie-architectuur en ketenregie. De overheid moet in staat zijn om complexe ketens van diensten over verschillende leveranciers heen te monitoren en te beveiligen.

6.7. Ontwikkelmodellen

De typering van de ontwikkelmodellen komt tot stand door een analyse langs de volgende dimensies:

- Regie in de samenwerking met de markt (overheid vs. markt): bij welke partij(en) ligt de regie en/of het zwaartepunt van de uitvoering binnen het samenwerkingsverband? Is de overheid de drijvende kracht of ligt het zwaartepunt bij de markt?
- Vraagsturing (centraal vs. pluriform/decentraal): dit raakt aan de autonomie van individuele overheidsorganisaties. Behoudt een gemeente of uitvoeringsorganisatie de vrijheid om zelf soevereine leveranciers te selecteren binnen de Rijksbrede IT-sourcingstrategie[43]?
- De rol die leveranciers hebben in de totstandkoming, het beheer en onderhoud van de clouddienst voor de Nederlandse overheid:
    - Detachering: biedt toegang tot kennis en capaciteit en creëert beperkte afhankelijkheid van leveranciers, stelt zware eisen aan de overheid ten aanzien van regievoering en aansturing.
    - Systeemintegratie: biedt resultaatverantwoordelijkheid bij de leverancier voor de totstandkoming, maar houdt de controle over het beheer van de productiesituatie bij de overheid.
    - Managed services: biedt ontzorgen ten aanzien van het beheer van de omgevingen, maar vereist meer toegang tot gegevens en creëert meer afhankelijkheid van de leverancier en beperkt daarmee de autonomie van de overheid.
    - Cloudleverancier: biedt direct toegang tot oplossing waarbij de integrale verantwoordelijkheid en controle bij de leverancier liggen, deze optie biedt vanzelfsprekend de minste autonomie voor de Nederlandse overheid.

[42] ECOFED, European Cloud Services in an Open Federated Ecosystem, link

[43] Digitale overheid, IT-sourcing

6.7.1. Combinatie van scenario’s

De uiteenlopende behoefte binnen de overheid vereisen een divers aanbod aan clouddiensten. Dit spectrum varieert niet alleen in servicemodellen (zoals IaaS en PaaS), maar ook in functionele specificaties, waaronder elastische schaalbaarheid en hoge prestaties enerzijds, en langdurige dataopslag met hoge volumes anderzijds. Ook kunnen deze diensten een uiteenlopend afnamevolume kennen. Door deze diversiteit is het aannemelijk dat één scenario niet toereikend genoeg is, maar dat er een combinatie van scenario’s mogelijk, of zelfs nodig, is om voor de overheid tot de beste oplossing te komen.

Ter illustratie is een combinatie van verschillende scenario’s mogelijk waarbij verschillende servicemodellen onder afzonderlijke scenario's worden ondergebracht; zo kan de levering van IaaS-voorzieningen via het ene scenario worden gerealiseerd, terwijl de complexiteit van PaaS-dienstverlening een ander scenario vereist. Een ander voorbeeld langs de lijnen van afnamevolumes; het ene scenario faciliteert de ontwikkeling en levering van hoog-volume dienstverlening, terwijl een ander scenario kleinschalige diensten met een specifieke behoefte voorziet.

6.7.2. Impact op aanbestedingen

Voor zowel de aanbesteding van de levering van soevereine clouddiensten door de markt als van de levering van dergelijke diensten door overheidsdienstverleners aan andere overheden, worden momenteel belemmeringen ervaren vanuit bestaande wet- en regelgeving. Voor levering van soevereine clouddiensten door leveranciers hebben overheidspartijen te maken met het aanbestedingsrecht waarbinnen het moeilijk is om bijvoorbeeld partijen uit te sluiten waarvan de ultieme controle buiten de EU ligt. Voor levering van diensten tussen overheidsorganisaties onderling bestaan er beperkingen vanuit de Wet Markt en Overheid en de Kaderwet zelfstandige bestuursorganen.

Deze belemmeringen zijn reeds onderkend vanuit het programma NDS en deze passen binnen de scope van een tweetal interventies die als onderdeel van dit programma actief zijn, namelijk:

- Interventie IT-sourcing & bundelen inkoopkracht;
- Interventie wetgeving.

Onder verwijzing naar deze interventies wordt in deze verkenning niet verder ingegaan op de oplossingsrichting voor deze mogelijke belemmeringen.

6.8. Generieke randvoorwaarden en afhankelijkheden

Ongeacht welk scenario (of combinatie van scenario’s wordt gekozen als strategische richting voor de realisatie van een soevereine clouddienst voor de Nederlandse overheid zijn er een aantal randvoorwaarden die ingevuld moeten worden om betekenisvolle stappen te kunnen zetten die tot daadwerkelijk gebruik van soevereine clouddiensten gaan leiden.

- Het is noodzakelijk dat er met voldoende snelheid en mandaat besluiten genomen kunnen worden namens de gehele overheid om vanuit de overheid als geheel de regie te kunnen voeren op de totstandkoming van de soevereine clouddienst. Het opzetten van een centrale regie maakt deel uit van de NDS opgave. Er zijn gremia die een start maken om deze overheidsbrede regie te voeren, waaronder het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO). Daarnaast is een instellingsbesluit voor het opzetten van de leverende organisatie noodzakelijk.

- Er zal vanuit de overheid budget (zowel in geld als beschikbare tijd van medewerkers) beschikbaar moeten worden gesteld om invulling te geven aan activiteiten die te maken hebben met het verder uitwerken van het optimale scenario, het opzetten/uitbouwen van een regiefunctie (inclusief de bemensing daarvan), het creëren van de standaarden en het detailontwerp voor de soevereine clouddienst, het uitvoeren van de benodigde aanbestedingen, waar nodig de aanschaf van middelen (datacenter capaciteit, hardware, software, tooling), het bouwen en uitrollen van de dienstverlening en uiteindelijk het beheer en onderhoud.
- Er zal grondig onderzoek plaats moeten vinden naar de wijze om in een adequaat beveiligingsniveau te voorzien. In het ontwerp van de soevereine clouddienst moeten keuzes gemaakt worden ten aanzien van de technologiestack en welke beveiligingsfunctionaliteiten wel en niet (standaard) deel uitmaken van het platform. Vervolgens moet worden vastgesteld welke aanvullende beveiligingsmechanismen en tooling nodig zijn in aanvulling op wat het platform biedt en of deze in een open source variant beschikbaar zijn. Wanneer dit niet het geval is moet worden geëvalueerd in hoeverre propriëtaire beveiligingsoplossingen compatibel zijn met de voorgenomen technologiestack.
- Er zal voldoende capaciteit beschikbaar gemaakt moeten kunnen worden om de clouddienst te kunnen realiseren. Er is op het moment van schrijven op meerdere vlakken sprake van schaarste (o.a. stroom, mensen, hardware). Er zal dus vroegtijdig geanticipeerd moeten worden op toekomstige capaciteitsbehoeften en rekening gehouden te worden met (lange) levertijden.
- Iedere afnemer zal een raamwerk moeten hanteren voor het bepalen van de juiste landingsplaats voor applicaties en data dat past binnen de eigen risicobereidheid en context van de organisatie. De soevereine clouddienst is niet bedoeld als de ultieme landingsplaats voor alle applicaties en data voor alle overheidstaken. In Figuur 7 is een voorbeeld opgenomen van een beslismatrix die als vertrekpunt kan worden gekozen.

Figuur 7 voorbeeld beslismatrix plaatsing applicaties en data

Type hosting	Hoge mate van soevereiniteit vereist	Zekere mate van soevereiniteit vereist	Hoge mate van security en resilience vereist	Gemiddelde security en resilience vereist	Beperkte security en resilience vereist
Public cloud					
Marktaanbod soevereine cloudopplossingen					
Soevereine overheidscloud					
On-premises					
HGI omgeving					

Voorbeeld

7. Conclusies en vervolgstappen

7.1. Conclusies

Programma NDS Cloud heeft een duidelijke ambitie uitgesproken om een zo hoog mogelijk soevereiniteitsniveau (SEAL-4) na te streven dat realistisch geïmplementeerd kan worden. Dit niveau moet een effectieve ondersteuning van overheidstaken mogelijk maken, waarbij de continuïteit en vertrouwelijkheid van de dienstverlening optimaal zijn geborgd. De geformuleerde uitgangspunten (zie paragraaf 6.1) geven een eerste richting en invulling aan de vraag hoe een soevereine clouddienst voor de overheid eruit moet zien.

Een viertal scenario's is ontwikkeld op basis van keuzes om een nieuwe clouddienst te bouwen versus bestaande omgevingen door te ontwikkelen en om een centraal versus een decentraal aanbod op te zetten. Deze scenario's kennen ieder hun eigen voordelen, nadelen en risico's.

De vraag wat voor de Nederlandse overheid het optimale scenario of combinatie van scenario's is, wordt sterk beïnvloed door een aantal factoren (die deels in het verlengde liggen van de in paragraaf 6.8 vermelde randvoorwaarden en afhankelijkheden):

- Snelheid waarmee de soevereine clouddienst moet worden gerealiseerd en op welke schaalgrootte
- Beschikbaarheid van budget om te een voorinvestering te doen in de realisatie van de soevereine clouddienst
- Mogelijkheid om tot een uniforme technologiestack te komen die daadwerkelijk wordt toegepast
- De gewenste rol van de markt

Vereiste snelheid van realisatie

Er zijn substantiële veranderingen nodig om de ambitie om een soevereine clouddienst te realiseren die voldoet aan SEAL-4 (met uitzondering waar dat niet realiseerbaar is op dit moment) in combinatie met de randvoorwaarden die in paragraaf 6.8 zijn geformuleerd, daadwerkelijk operationeel te krijgen. Indien de insteek is dat de soevereine clouddienst zo snel mogelijk aan alle eisen moet kunnen voldoen geeft dit een voorkeur voor scenario's waarbij een nieuwe omgeving naast de bestaande infrastructuren (organisatie en technologie) wordt opgebouwd. Specifiek zou dit in de richting van scenario's A (Nieuwe soevereine overheidsclouddienst) of C (Nieuwe soevereine clouddiensten conform overheidsstandaarden) wijzen.

Hiertegenover staat dat wanneer er een voorkeur is om snel applicaties en data ten behoeve van belangrijke overheidstaken te repatriëren uit publieke cloud omgevingen, ook als deze nog niet aan alle soevereiniteitsdoelstellingen voldoen, dan zijn de scenario's waarbij bestaande infrastructuren worden gemoderniseerd (en geconvergeerd) beter toegerust om invulling te geven aan deze opgave. Specifiek zou dit in de richting van scenario B (Modernisering bestaande overheidscloudinfrastructuur) of scenario D (aansluitmodel voor clouddiensten onder overheidsregie) wijzen. Ten aanzien van het snel kunnen migreren van applicaties dient niet alleen naar de opzet van de clouddienst te worden gekeken, maar zeker ook rekening gehouden te worden met de complexiteit van het aanpassen van de applicaties aan het doelplatform.

Beschikbaar budget

Het opzetten van soevereine clouddiensten vergt in alle gevallen een voorinvestering, maar bij scenario's waarbij nieuwe diensten en bijbehorende platformen worden opgebouwd naast bestaande, is de vereiste investering vooraf substantieel groter dan wanneer bestaande diensten worden gemoderniseerd (en geconvergeerd). Indien er slechts

beperkt budget beschikbaar is om op relatief korte termijn te investeren in de totstandkoming van de soevereine clouddienst, is er waarschijnlijk geen andere reële keuze dan uit te gaan van scenario's die bestaande infrastructuren moderniseren (en convergeren). Specifiek zou dit in de richting van scenario B (Modernisering bestaande overheidscloudinfrastructuur) of scenario D (Aansluitmodel voor clouddiensten onder overheidsregie) wijzen. Hiermee is overigens niet gezegd dat deze scenario's op het gebied van totale kosten lager uitvallen, dat is van een veelheid aan factoren afhankelijk. Bovendien betekent beperkt budget het langzamer bereiken van grotere soevereiniteit en het voorlopig niet bereiken van een hoge mate van soevereiniteit (SEAL-4).

Een optie is om marktpartijen te bewegen (een deel van) de voorinvestering voor hun rekening te nemen. Daar dient dan een commitment ten aanzien van afname van diensten bij die marktpartijen tegenover te staan om deze voorinvestering te rechtvaardigen. Indien dit realiseerbaar is staan ook de scenario's open waarin de soevereine clouddienst naast bestaande infrastructuren wordt opgebouwd.

Uniforme technologiestack

De Nederlandse overheid bestaat uit veel partijen die ieder in hun eigen context werken en daarmee hun eigen eisen stellen aan een soevereine clouddienst. De mate waarin het lukt om op basis van deze verschillende vertrekpunten tot een uniforme technologiestack te komen zal bepalend zijn voor de vraag of de scenario's, waarin van een centrale opzet wordt uitgegaan, voldoende realiseerbaar blijken. Indien de verwachting is dat door de verschillende achtergronden er uiteindelijk toch altijd een pluriforme set technologiestacks noodzakelijk is, dan heeft dit tot gevolg om voor de meer decentrale scenario's te kiezen. Specifiek zou dit in de richting van scenario C (Nieuwe soevereine clouddiensten conform overheidsstandaarden) of scenario D (Aansluitmodel voor clouddiensten onder overheidsregie) wijzen.

Rol van de markt

De rollen voor de markt zoals die eerder zijn besproken verschillen per scenario. Wanneer er een voorkeur is om niet afhankelijk te zijn van marktpartijen voor end-to-end dienstverlening (bijvoorbeeld met het oog op het risico op overname door een niet-Europese partij) dan ligt het meer voor de hand om te kiezen voor scenario's waarin vanuit de overheid centraal een soevereine clouddienst wordt gerealiseerd. Dit is mogelijk met hulp van marktpartijen in de rol van detacheerder, system integrator of leverancier van managed services. Specifiek zou dit in de richting van scenario A (Nieuwe soevereine overheidsclouddienst) of scenario B (Modernisering bestaande overheidscloudinfrastructuur).

Maken van de keuze

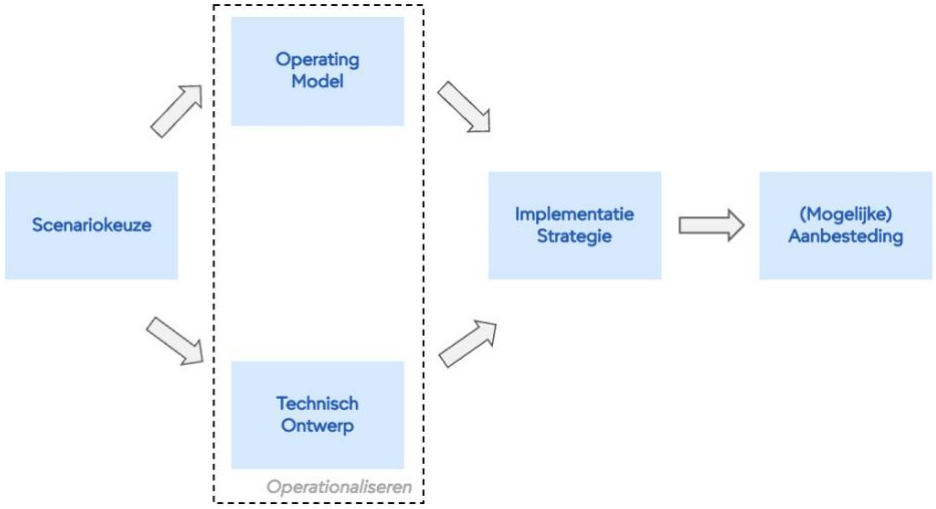
Het is aan de Nederlandse overheid om op basis van deze overwegingen en de weging daarvan in haar eigen context om de keuze te maken voor het optimale scenario.

7.2. Vervolgstappen

De realisatie van een overheidsbrede soevereine clouddienst is een omvangrijke transitie die vraagt om een stapsgewijze aanpak. Het lonkend perspectief is een weerbaar IT-ecosysteem waarin de Nederlandse overheid op elk moment de regie voert over haar eigen data en diensten, onafhankelijk van geopolitieke druk of technologische lock-ins.

Om verlamming door complexiteit te voorkomen, worden ontwerp, ontwikkeling en realisatie stap voor stap georganiseerd. Dit stelt betrokkenen in staat om optimaal in te spelen op onzekerheden en leereffecten direct te benutten, wat de uitvoerbaarheid ten goede komt. De verschillende vervolgstappen worden beschreven in Figuur 8.

Figuur 8 relevante aspecten t.b.v. ontwerp en realisatie



Scenariokeuze

De eerste stap is de bestuurlijke besluitvorming over de strategische koers. Deze keuze bepaalt de balans tussen snelheid, kosten en de mate van soevereiniteit. Het scenario kan gekozen worden mede op basis van de in deze verkenning gedefinieerde scenario's of een combinatie daarvan.

Scenario operationaliseren

Na de keuze wordt het scenario geoperationaliseerd langs twee parallelle lijnen. Dit vormt het fundament voor de dagelijkse praktijk van de clouddienst:

Operating model

Het operating model is de blauwdruk die beschrijft hoe de overheid haar strategie in de praktijk brengt. Een operating model bestaat uit componenten die in samenhang worden ontworpen en ingericht. Het inrichten van de componenten in een operating model betekent dat keuzes gemaakt moeten worden op o.a. de volgende aspecten:

- Governance inrichten en uitwerken in duidelijke taken, verantwoordelijkheden en bevoegdheden om de soevereine clouddienst te ontwikkelen, realiseren en beheren inclusief het vastleggen van opdrachtgever- en eigenaarschap met oog op gedegen regievoering.
- Concretiseren van de business case (te realiseren baten, te maken kosten) incl. nadere uitwerking van de benodigde financiersmix t.b.v. het financieren van activiteiten en investeringen.
- Benodigde prestaties (o.b.v. beoogd gebruik) specificeren en vastleggen in dienstverlenings- en leveranciersafspraken.
- Talentbehoefte inventariseren en uitwerken in een strategisch HR-plan met oog voor werving, selectie en beloning van benodigd talent.
- Werkwijzen vastleggen en inrichten in processen t.b.v. 'run and change' van de soevereine clouddienst. Benodigde tooling ontwerpen, werven, inrichten en realiseren. Inclusief het selecteren en inrichten van fysieke locaties.

Technisch ontwerp

Een functionerende soevereine cloud heeft een gedegen architectuur nodig waarin belangrijke onderdelen in samenhang worden ontworpen en gaan functioneren. Het technisch ontwerp is het technisch fundament waarin wordt vastgelegd hoe soevereiniteitseisen (zoals SEAL-4) technisch worden afgedwongen.

Implementatie strategie

Zodra het ontwerp staat, volgt de strategie voor de feitelijke realisatie. Hierin worden kritieke workloads geprioriteerd en wordt een migratie-aanpak ontworpen. Onderdeel hiervan is de sourcing: het organiseren van de inkoop en de samenwerking met Nederlandse en/of Europese marktpartijen. Daarnaast wordt de governance ingericht om de integrale verandering te begeleiden, inclusief processen voor kwaliteits- en risicomanagement.

(Mogelijke) aanbesteding

Afhankelijk van de gekozen sourcingstrategie kan een gerichte aanbesteding plaatsvinden om de technische bouwstenen en diensten te verwerven.