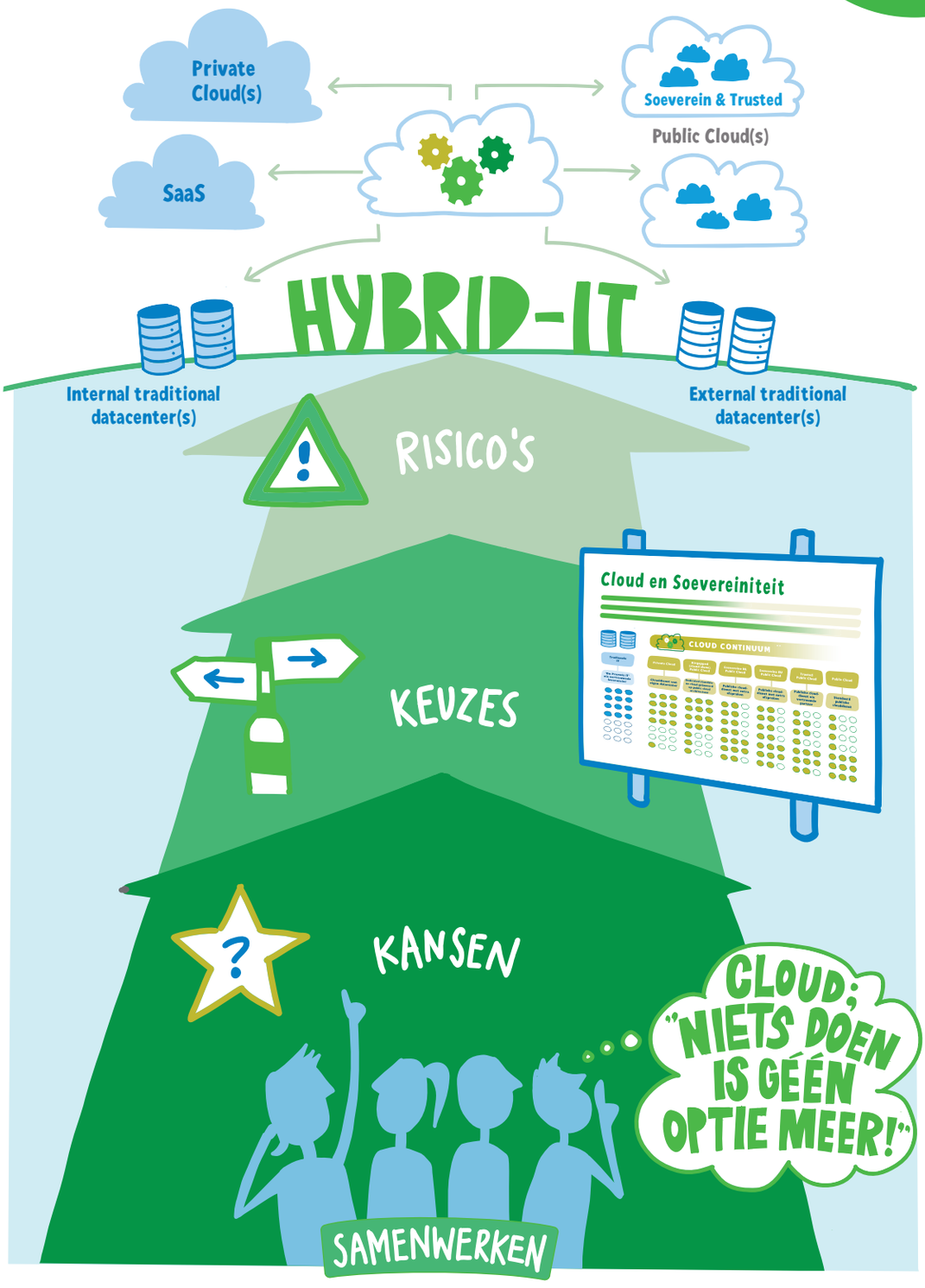
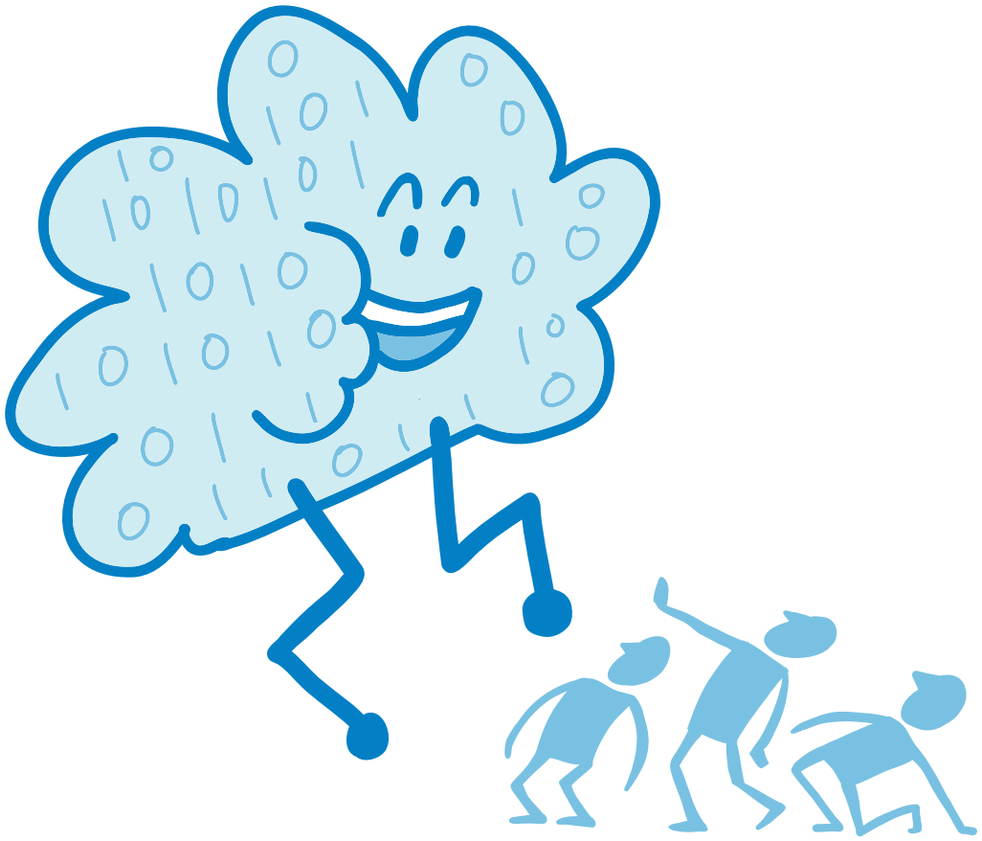
Cloud: ‘Niets doen is géén optie meer!’

4 tips
van I-INTERIM RIJK



POSITION PAPER, maart 2024

I-INTERIM RIJK



INLEIDING

Het Rijk in de Cloud

Cloud computing is het via het internet gebruiken van hardware, software en gegevens. De datacenters van waaruit deze Clouddiensten geleverd worden, kunnen zich overal ter wereld bevinden. In augustus 2022 heeft de staatssecretaris van BZK besloten dat het Rijk ook gebruik mag maken van Clouddiensten, ook als voorzieningen in deze datacenters zelfs gedeeld worden met andere klanten (wat we Public Cloud noemen).

Het gebruik van Public Cloud neemt toe. De diversiteit aan meningen over wat te doen met de Cloud blijft eveneens groeien. Reden voor professionals van I-Interim Rijk en Defensie om een aantal leveranciers te bezoeken, en zich over de internationale ontwikkelingen te laten informeren door Instituut Clingendael, in de Cloud Tour 2023.

In deze Position Paper delen zij hun bevindingen:

- De Cloud biedt veel kansen, maar er zijn zeker ook risico's aan verbonden.
- Het negeren van Cloudontwikkelingen kent óók risico's, waar je maar beter op kunt anticiperen. Je moet er dus wat mee, ook als beleidsdirectie.
- Het maken van de juiste Cloudkeuzes is een hele puzzel, vanwege de vele opties en vanwege de kansen en risico's.
- Die puzzel kun je alleen goed oplossen als je de juiste expertise in huis haalt en op tijd begint met het leggen. En al helemaal als uw leverancier de Cloud in gaat zonder dat je dat zelf een goed idee vindt.


?
Samenwerking
Flexibiliteit
Innovatie
Schaalbaarheid

TIP 1

Ken uw kansen

Een Cloudgang kan een bewuste keuze zijn vanwege een aantal voordelen, zoals:

Flexibiliteit
Clouddiensten bieden een grotere flexibiliteit. Als de basis er eenmaal ligt, kunnen nieuwe standaard diensten eenvoudiger worden gekoppeld dan bij On Premise-oplossingen. Dat geldt ook voor bijvoorbeeld het beheer van grote datasets, snel plaatsen van testomgevingen en afkoppelen van bestaande diensten. De overheid kan met deze technologie sneller inspelen op sommige ontwikkelingen in de markt en in de samenleving. Dit vergt wel een solide architectuur en goede contracten met marktpartijen.

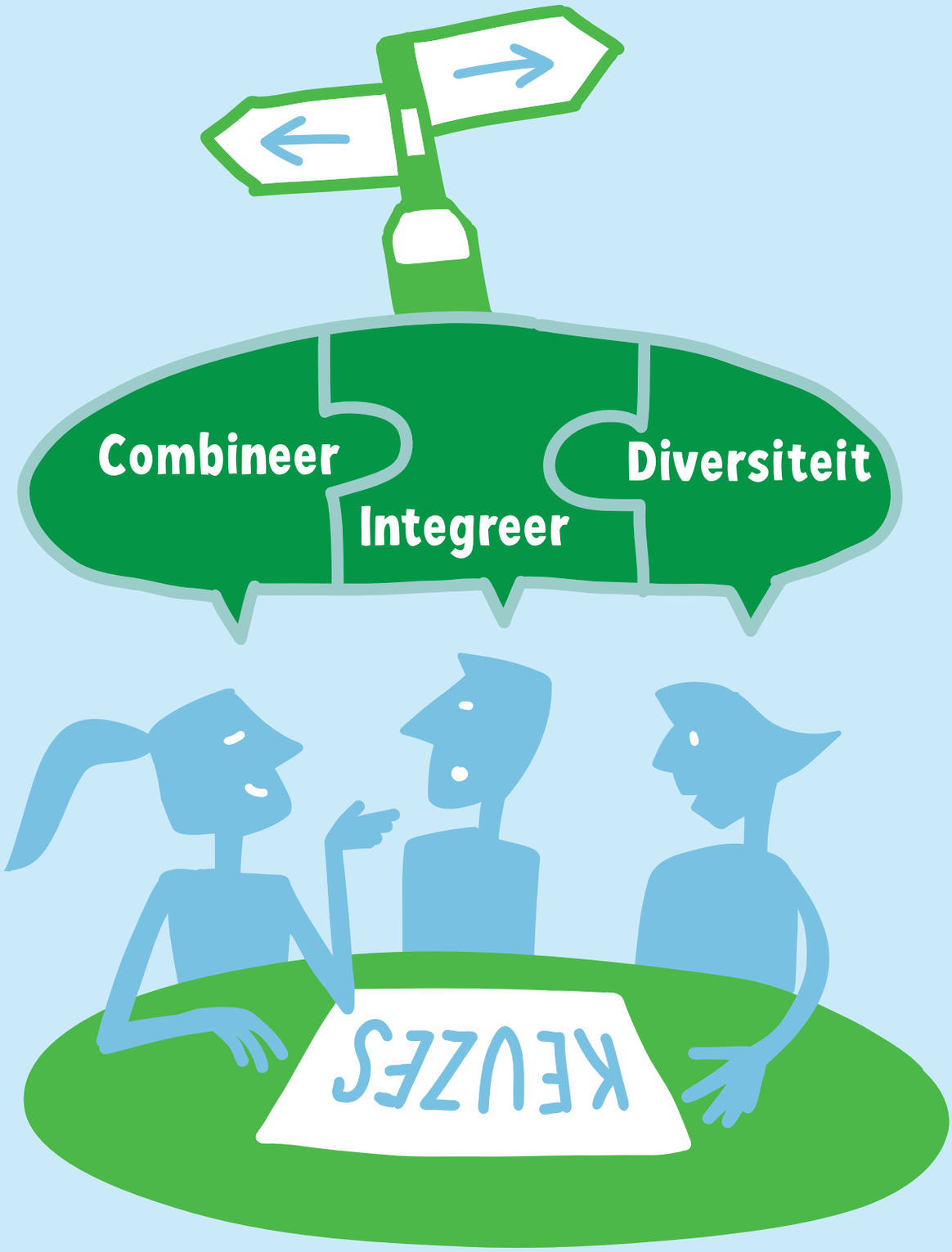
Innovatie
De inzet van Clouddiensten kan leiden tot een versnelling van de inzet van nieuwe diensten. Grote Cloudaanbieders kunnen zich nu eenmaal meer investeringen veroorloven in innovatie, zoals AI (voor zover verantwoord inzetbaar), analytics en andere geavanceerde software, dan de Rijksoverheid. Sommige diensten zijn simpelweg alleen in de Cloud in te kopen.

Schaalbaarheid
Clouddiensten bieden een grotere schaalbaarheid. Cloudleveranciers zijn in staat sneller op te schalen, bijvoorbeeld als een pilot succesvol blijkt of als de performance-eisen verhoogd worden. Inkoop van nieuwe hardware behoort tot het verleden. Om de kosten te beheersen, vergt dit wel goede opschalingsafspraken vooraf met leveranciers.

Financieringsflexibiliteit
Clouddiensten maken veelal een einde aan voorfinanciering. De overgang naar de Cloud elimineert de noodzaak om vooraf grote kapitaalinvesteringen te doen in fysieke hardware en infrastructuur. In plaats daarvan kan de overheid gebruikmaken van Pay-per-Use modellen, waarbij alleen wordt betaald voor wat daadwerkelijk wordt gebruik, waardoor de financiële last gelijkmatiger over de tijd wordt uitgesmeerd. Als keerzijde wordt wel opgemerkt dat de voorspelbaarheid van (variabele) kosten afneemt. Clouddiensten zijn niet per se goedkoper. Iets om ook in de budgettering wel degelijk rekening mee te houden.

Om de kosten te beheersen wordt daarom vaak invulling gegeven aan de rol van Cloudbroker. Ook het bundelen van regie op en inkoop van Clouddiensten kan tot sterke besparingen leiden en draagt in ieder geval bij aan versterking van de opdrachtgeversrol.

Interdepartementale samenwerking
De belangrijke en urgente maatschappelijke opgaven waar we als Rijk voorstaan (stikstof, klimaat, migratie) vergen veelal een interdepartementale en interbestuurlijke aanpak. Hybride samenwerken, informatie en data delen en verwerking/analyse zijn met Clouddiensten sneller in te richten en te gebruiken, dan via de traditionele On Premise omgevingen. Kortom de Cloud faciliteert in algemene zin het interdepartementaal samenwerken.

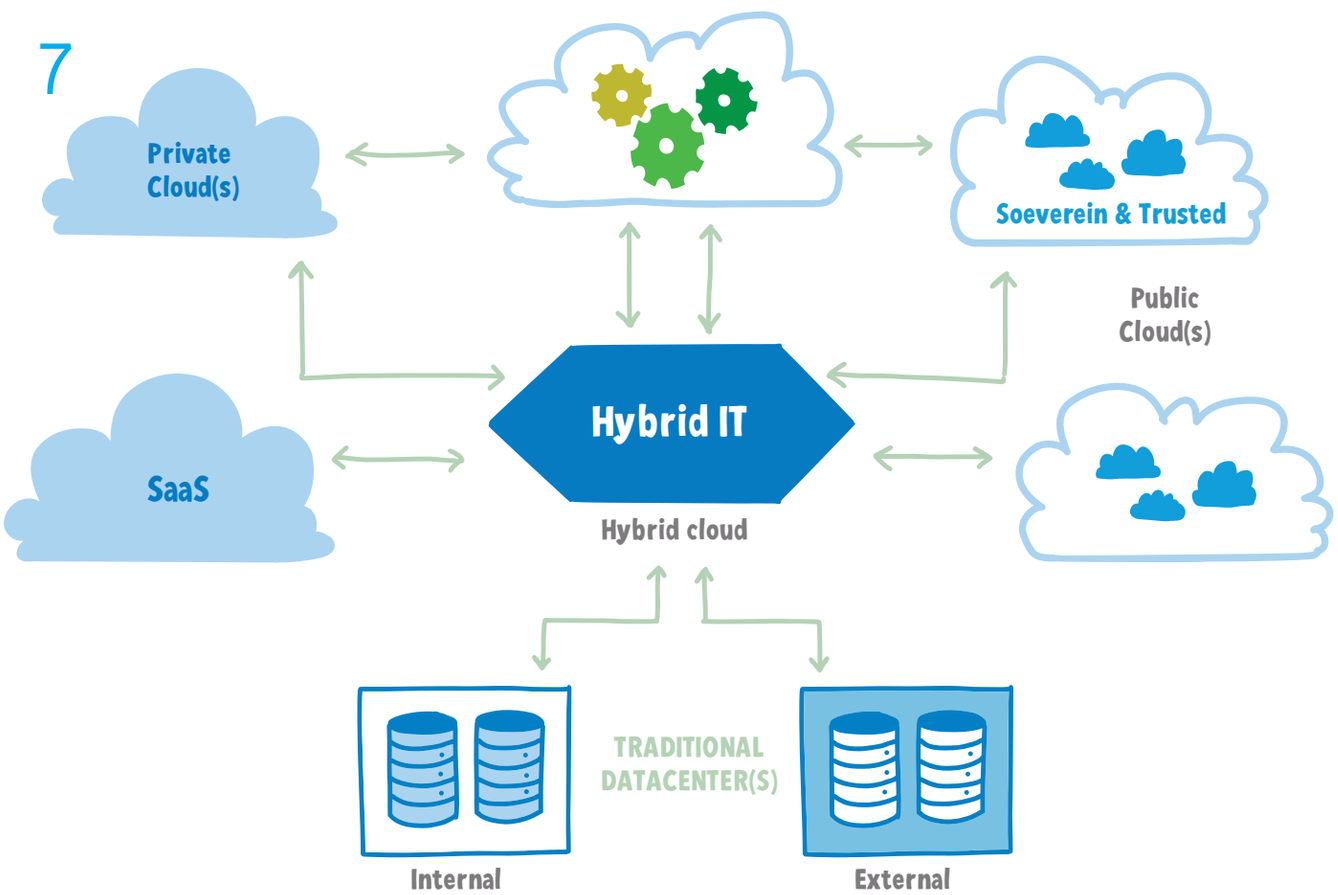

Combineer
Integreer
Diversiteit
KEUZES

TIP 2

Combineer en integreer

De “keuze voor de Cloud” is geen alles-of-niets keuze. Sterker nog, de mogelijkheden Clouddiensten te combineren, maken dat per Clouddienst een andere keuze kan worden gemaakt. Veel IT-landschappen zullen “hybride” worden. Dat wil zeggen dat ze gaan bestaan uit hard- en software (On Premise of via Clouddiensten) die verschillende diensten met veschillende “karakteristieken” samenvoegt tot één dienst aan burgers, bedrijven en eigen medewerkers.

Hybride landschappen
In een hybride landschap worden de ingekochte Clouddiensten gecombineerd met diensten vanuit de eigen datacenters. Dit vergt de inzet van een Cloud Broker, die service integratie en orkestratie verzorgt. Dit is veelal uw IT-organisatie of shared service center (SSC), omdat die het beste weet hoe de diensten uit uw eigen datacenters werken, en uw klantbehoefte vaak goed snapt. Een schets is hieronder opgenomen.



Diversiteit in karakteristieken
Er is een zeer grote verscheidenheid aan Public Clouddiensten. Daarbij is er een aantal grote spelers, vaak hyperscalers uit Amerika. Deze leveren een zeer breed pallet aan de meest attractieve, innovatieve en kostenefficiënte oplossingen. Deze partijen zijn dominant op de markt en vaak al in zekere mate aanwezig in het I-domein, zoals het domein van werkplek- en email-oplossingen.

Voor een aantal informatiesystemen binnen de overheid gelden echter strenge voorwaarden voor wat betreft veiligheid, privacy en soevereiniteit (zie onderstaande inzet). De bekende hyperscalers kunnen vaak niet aan de benodigde eisen voldoen. Ook niet met de inzet van quantum-proof encryptie op de data.

Gelukkig zijn er op de markt meerdere vormen van Clouddiensten en Cloud leveranciers beschikbaar. We raden aan te letten op de volgende factoren:

- De mate van invloed op de wijze waarop privacy en security wordt ingericht.
- Geografie en jurisdictie van opslag en verwerking van de data.
- Eigenaarschap van de cloud-dienst en overdacht. beheerverantwoordelijkheden
- De belangen van andere klanten die gebruik maken van dezelfde clouddienst.

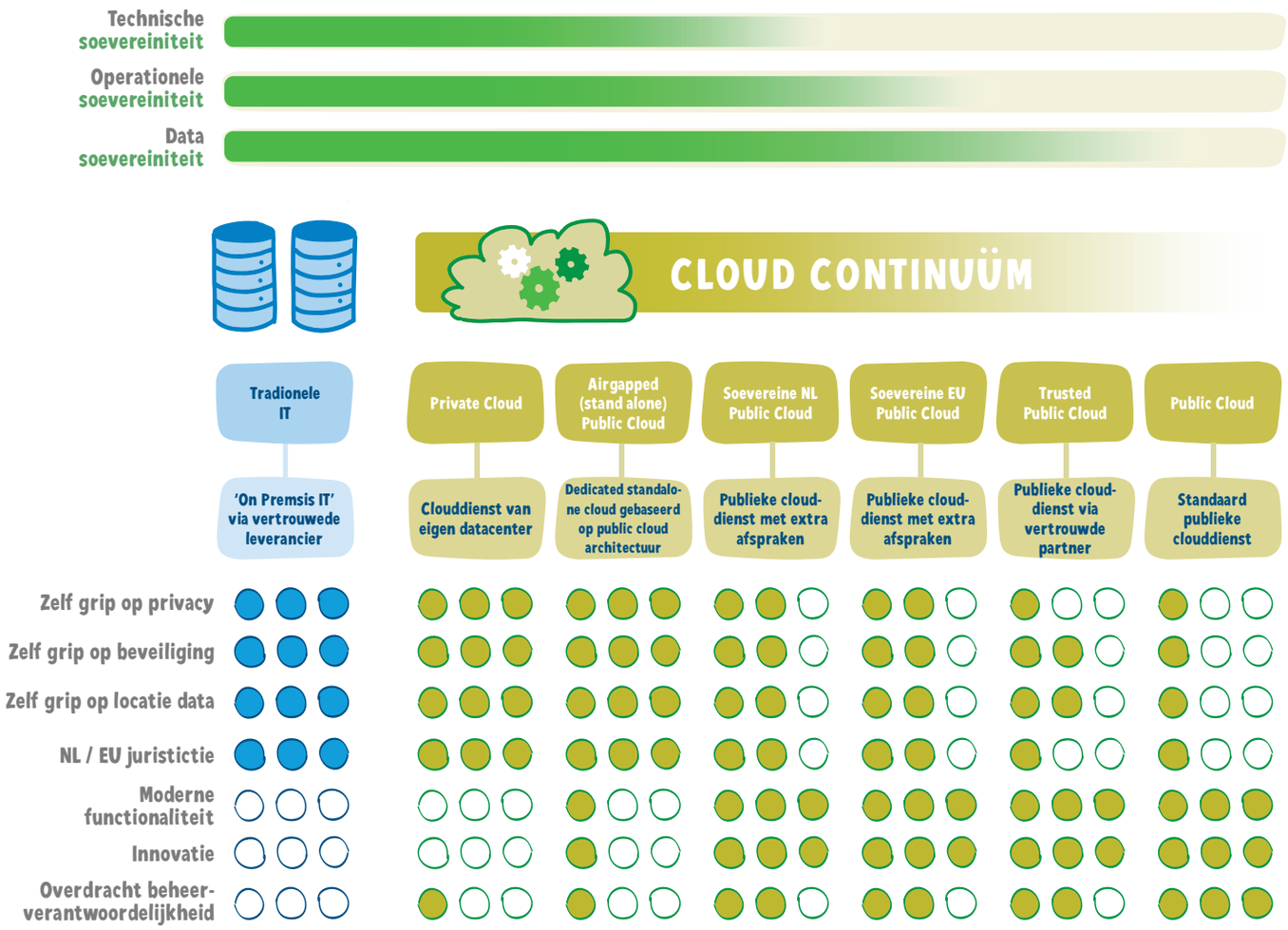
Met onderstaand Cloud Continuüm geven we een handzaam model om snel in te kunnen schatten wat wel of niet passend is voor een specifieke vraag geen afweging.

Speciale aandacht willen we geven aan Soevereiniteit. Een steeds belangrijker thema en voor de Public Cloud een groeiende uitdaging.

Digitale soevereiniteit, het zelfbeschikkingsrecht over digitale data en infrastructuur, is een steeds prominenter thema in de politiek en beleidsvoering. Geopolitieke spanningen en de discussie over strategische autonomie binnen de EU benadrukken de noodzaak om controle te houden over onze digitale identiteit. De toenemende adoptie van Public Clouddiensten door de (Rijks)overheid brengt echter nieuwe risico's met zich mee, aangezien deze diensten afhankelijkheden creëren van externe IT-leveranciers.

Deze afhankelijkheden kunnen de digitale soevereiniteit op verschillende manieren bedreigen. Onbevoegde toegang tot data, ondoorzichtige werking van algoritmes en vendor lock-in zijn slechts enkele voorbeelden. Het is dan ook cruciaal om maatregelen te nemen om digitale soevereiniteit en data-autonomie te waarborgen in de Public Cloud.

Cloud en Soevereiniteit

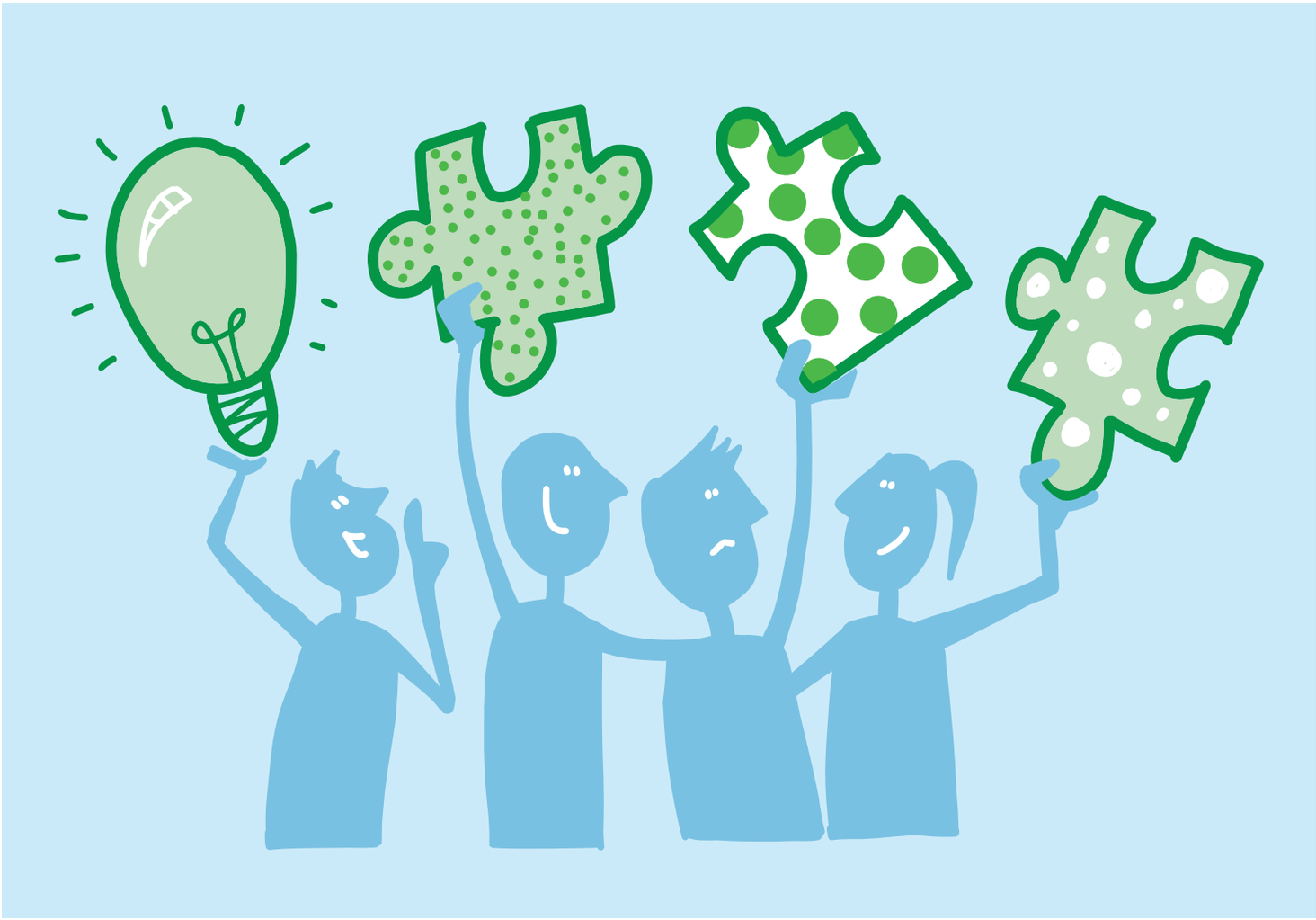


We kunnen digitale soevereiniteit grofweg opdelen in drie domeinen: Data soevereiniteit, Operationele soevereiniteit en Technische soevereiniteit.

Data soevereiniteit omvat de controle over de locatie, opslag, en toegankelijkheid van data. Dit kan worden gewaarborgd door middel van encryptie, data residency eisen, en strikte toegangsbeperkingen, maar ook door de keuze van de Cloudleverancier.

Operationele soevereiniteit focust op de controle over de werking van de Cloudomgeving. Dit behelst aspecten zoals security patching, log management, en incident response. Transparantie en controle over de operationele processen zijn hierbij cruciaal.

Technische soevereiniteit richt zich op de keuze van de Cloudtechnologie en de infrastructuur. Open source-oplossingen, vendor-neutrale platforms, en gedecentraliseerde architecturen kunnen hierbij helpen om vendor lock-in te voorkomen.



TIP 3

Werk samen, ook met leveranciers

In veel gevallen heeft u voor de vernieuwing van de IT niet zoveel te kiezen. Steeds meer leveranciers kiezen er namelijk voor hun diensten uitsluitend via de Cloud te leveren. Dan kunt u maar beter voorbereid zijn. Verken de marktontwikkelingen voor u relevante segmenten van leveranciers en zet een reële, gezamenlijke koers uit. Strategisch Leveranciersmanagement, categoriemanagement en inkoop hebben hier een essentiële rol in. Een Cloudgang doe je tenslotte niet zomaar. Het is niet “alleen maar” een technologisch feestje. Het vergt ook een verandering in denken, handelen, werkwijzen en organiseren van veel meer afdelingen en disciplines in je organisatie. Het is daarom van belang dat een diverse groep van uw professionals zelfstandig en in samenspraak met leverancier(s) te maken keuzes afweegt en met de juiste voorstellen komt.

De aanlooptijden zijn lang. Dus als je contract binnenkort afloopt, zijn er IT-voorzieningen end-of-life of zie je innovatieve kansen, maar is een On Premise oplossing onwaarschijnlijk: goede voorbereiding en actie is nu noodzakelijk. En dat is teamwork!

Let goed op dat u de juiste kennis en specialisten aan boord heeft, anders gaat u alsnog de 'mist' in. Elke professional heeft zijn eigen, onmisbare bijdrage aan de te maken afwegingen bij het wel of niet overgaan naar de Cloud.

Strategen en Architecten
- Actualiseer uw IT-Sourcing-strategie en -architectuur om Hybride IT te ondersteunen.
- Definieer duidelijk de rolverdeling tussen On Premise en Cloud-gebaseerde resources.
- Ontwikkel een roadmap voor de migratie van workloads naar de Cloud.
- Ontwikkel een multi-vendor strategie om een vendor lock-in te vermijden.

Cloud Competence Center (CCC):
- Richt een Cloud Competence Center (CCC) op om kennis te delen en expertise te ontwikkelen binnen de organisatie. Dit is breder dan alleen IT, betrek dus ook non-IT-professionals om een breed perspectief te garanderen.
- Investeer ook in opleiding en ontwikkeling van uw IT-personeel om de nodige kennis en vaardigheden te verwerven voor Hybride IT-beheer.
- Het gaat daarbij om de expertisegebieden Cloudcomputing, infrastructuurbeheer, security en applicatieontwikkeling.

Monitoring en Security Specialisten:
- Implementeer een robuuste monitoringoplossing voor uw gehele IT-omgeving, inclusief Clouddiensten.
- Zorg voor strikte securitymaatregelen om uw data te beschermen, ongeacht waar deze zich bevinden.
- Volg de best practices voor security in de Cloud, zoals o.a. ook door het NCSC wordt uitgebracht.

Risicomanagers
- Ontwikkel een exit-strategie om te voorkomen dat u vast komt te zitten bij een bepaalde Cloud-leverancier.
- Mensen die de Centrale Voorzieningen goed kennen:
- Maak gebruik van centrale of gedeelde voorzieningen zoals Identity and Access Management (IAM) om flexibiliteit, consistentie en controle te garanderen.
- Implementeer een API-strategie om de integratie tussen verschillende Clouddiensten te stroomlijnen.

Directies die u voorgingen
- Deel kennis en ervaringen met andere organisaties die de overstap naar Hybride IT maken.
- Werk samen waar mogelijk om te profiteren van schaalvoordelen en beste practices.

De juiste Interne IT-leverancier(s):
- Bepaal de rol van de interne IT-leverancier in de context van Hybride IT.
- Maak gebruik van hun expertise voor migratie, integratie en beheer van Clouddiensten.


Vendor Lock In
Exitstrategie
Gegevens-
bescherming
NODIG:

TIP 4

Dek risico's goed af

Door diensten af te nemen van veelal grote internationale leveranciers – die in veel gevallen niet onder Nederlandse jurisdictie vallen – maakt het Rijk zich óók afhankelijk van anderen. Dat brengt een aantal risico's met zich mee, waaronder Vendor Lock-in: Organisaties kunnen zo afhankelijk worden van een specifieke leverancier, dat er weinig tegen te doen valt als die minder goed, minder flexibel of duurder wordt. Het is dan lastig over te stappen naar een ander. Dit kan de kwaliteit en de continuïteit van de dienstverlening van de Rijksoverheid in gevaar brengen.

Geopolitieke Risico's: Inbreuken op Clouddiensten door statelijke actoren en cybercriminelen vormen een voortdurende bedreiging. Dit risico is gedurende de gehele levenscyclus van de clouddienst aanwezig, van ontwikkeling en fabricage tot beheer en gebruik. Dit kan de soevereiniteit van organisaties – in geval van internationale dreigingen – aantasten.

Datasoevereiniteit: Cloudoplossingen van marktpartijen kunnen leiden tot internationale datastromen en opslag van informatie buiten de landsgrenzen. Dit brengt risico's met zich mee ten aanzien van inmenging en inzage door andere overheden, die op basis van hun eigen wetgeving legitiem toegang kunnen claimen.

Gegevensbescherming: Het borgen van een adequate beveiligingsniveau en naleving van soevereiniteitsprincipes is een cruciale verantwoordelijkheid bij de migratie naar de Cloud. Organisaties die de Cloud in gaan, moeten dit "op afstand" goed zien te beheersen.

Het Rijkscloudbeleid biedt een kader voor het gebruik van Public-Cloud-oplossingen door de Nederlandse Rijksoverheid. Het beleid stelt aanvullende eisen, waaronder een exit-plan en mitigatie van de in de risicoanalyse benoemde risico's.

Een van de specifieke risico's t.a.v. Cloud heeft rechtstreeks betrekking op inkoop- en leveranciersmanagement. De huidige Nederlandse en Europese wet- en regelgeving en de geldende inkoopvoorwaarden (ARBIT) zijn nog niet expliciet aangepast aan de vernieuwende clouddienstverlening. Vanuit enthousiasme bij overheden over de kansen die Clouddiensten bieden voor het versnellen van innovatie, is het risico aanwezig of zelfs verleidelijk om cruciale stappen over te slaan of per abuis over het hoofd te zien. De selectie en verwerving van Clouddiensten vraagt om een andere wijze van inkopen, waarbij rekening moet worden gehouden met het opstellen van Cloud-, security- en privacy architecturen, uitvoeren van risicoanalyses en aanpassen van begrotingen gebaseerd op software en licenties (CAPEX) naar abonnementen en datagebruik (OPEX).

Het is noodzakelijk om als organisatie serieus in de benodigde skills te investeren. Enerzijds om te waarborgen dat verwerving en uitwerking plaatsvinden vanuit eigen expertise en anderzijds om de juiste gesprekken te kunnen voeren met leveranciers van Clouddiensten. Deze kennis is heden ten dage schaars en moeilijk herkenbaar. Het niet op voorhand rekening houden met de aanwezige risico's kan in de uitvoering van projecten leiden tot late "tegenreacties" van degenen die risicobeheersing juist van groot belang achten. Vaak ontstaan hierdoor vertragingen, kostprijsverhogingen, kwaliteitshiaten of frustraties die vermijdbaar zijn of vooraf al te mitigeren zijn.

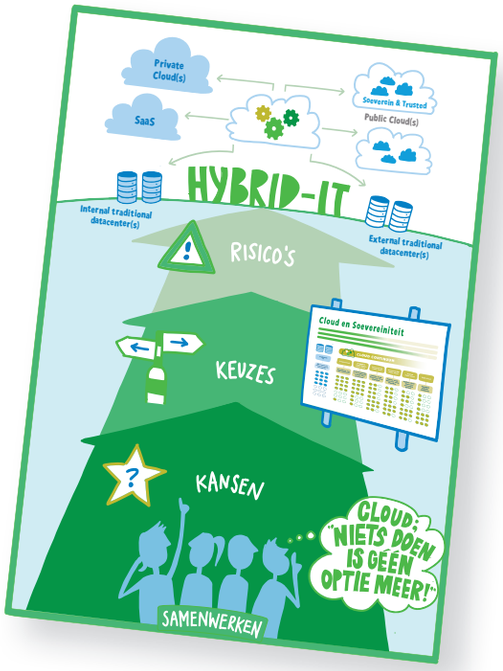
Vroegtijdige beoordeling van voor- en nadelen in de volle breedte moet een vereiste zijn bij het selecteren en verwerven van Clouddiensten. Het vraagt om een gezonde realiteitszin tussen aangedragen kansen uit de markt en aanwezige kennis om die kansen te kunnen beoordelen.

Het opdrachtgeverschap moet helder worden bezien vanuit de verbinding met de interne organisatie v.w.b. wensen en eisen, maar ook aansluiten op het actuele aanbod van innovatieve Clouddiensten door individuele leveranciers of consortia van leveranciers.

De selectie en verwerving van Clouddiensten is al geen sinecure, echter ook de implementatie van Clouddiensten vraag om serieus stevig projectmanagement waarbij expertise en ervaring op het gebied van Clouddiensten onontbeerlijk is.

Tenslotte is het wenselijk om een open houding ten aanzien van het eindresultaat te waarborgen: "On Premise" kan de beste oplossing zijn, juist als je wilt innoveren. En "Cloud" kan de beste oplossing zijn, juist als security belangrijk is. Van essentieel belang is om te beseffen dat hier ook geldt dat het verrichten van goed voorwerk met de juiste expertise – alvorens over te gaan tot selectie, verwerving en implementatie van Clouddiensten – het halve werk is!
Als het gaat om Clouddiensten, is iedere afweging maatwerk!

Conclusie



Cloud: 'Niet doen is geen optie meer!', dat is de boodschap. Eerder vroeger dan later zal zich een Cloud vraagstuk aandienen, als dit niet al het geval is. Met alle uitdagingen van dien. Hier grip op krijgen vraagt van begin af aan om een reële strategie, goede samenwerking en de juiste kennis. Wacht daarom niet af, begin en schroom niet ons te bellen.

TIP 1
Ken uw kansen

TIP 2
Combineer en integreer

TIP 3
Werk samen, ook met leveranciers

TIP 4
Dek de risico's goed af

Deze Position Paper is met dank aan de deelnemers en dragers van de Cloud Native Technology Tour 2023 tot stand gekomen:

Deelnemers:
- Emma Gieben-Malenstein (MinDEF)
- Ewoud Halewijn (I-Interim Rijk)
- Gert Jan Landwaart (MinDEF)
- Jurre Heesbeen (Rijks ICT Gilde)
- Leontine Douma (MinDEF)
- Nico-Dirk van Loo (I-Interim Rijk)
- Pieter Lindhout (I-Interim Rijk)
- Richard Raats (I-Interim Rijk)
- Rob Tardijn (I-Interim Rijk)
- Robert Heer (I-Interim Rijk)
- Roshni van Zeijst (MinDEF)
- Ted Straathof (I-Interim Rijk)

Lezingen door:
- Equinix
- KPN
- Microsoft
- Oracle
- Servicenow
- Salesforce
- Instituut Clingendael

Colofon Tekst Pieter Lindhout | Ontwerp Buro BRAND

I-INTERIM RIJK

Als u meer informatie wilt, laat het ons weten via:

www.rijksorganisatieodi.nl/i-interim-rijk

i-interimrijk@rijksoverheid.nl

070 - 700 05 50