Loop niet met je hoofd in de wolken

Een handreiking over cloudgebruik

Adviescollege ICT-toetsing

Loop niet met je hoofd in de wolken

Een handreiking over cloudgebruik

Clouddiensten spelen een kritieke rol in de ICT van bijna alle overheidsorganisaties. In onze onderzoeken zien we dat bij de businesscase voor een cloudtoepassing de focus ligt op de voordelen, maar dat risico's onderbelicht blijven. Soms zijn die niet scherp in beeld en soms wordt hun impact onderschat. Met deze handreiking wil het Adviescollege ICT-toetsing (AcICT) bestuurders en andere functionarissen zoals CIO's en CTO's binnen de Rijksoverheid een helpende hand bieden bij de afweging van de inzet van cloud. Deze handreiking geeft een basis voor het formuleren of toetsen van de eigen cloudstrategie. Ze is gebaseerd op de kennis en ervaring die we hebben opgedaan in diverse onderzoeken.

Wat bedoelen we eigenlijk met cloud?

Onder 'cloud' verstaan we: een ICT-dienst waarbij **bronnen** (*resources*) zoals processoren, geheugen en opslag **gedeeld** worden tussen **meerdere afnemers** (*tenants*). Deze diensten worden meestal aangeboden via een zogenaamde **publieke** cloud, waarbij een commerciële partij de infrastructuur beheert en meerdere afnemers zoals overheden, bedrijven en particulieren er via internet gebruik van kunnen maken.

Wanneer de infrastructuur fysiek gescheiden is voor gebruik door één organisatie, spreken we van een **private** cloud. Een **hybride** cloud is een combinatie van een publieke en private cloud, waarbij diensten en data verdeeld zijn over beide types. Een **multi**cloud is een combinatie van verschillende (publieke) clouddiensten bij verschillende leveranciers. Een **community**cloud is een cloudinfrastructuur exclusief voor een afgebakende groep afnemers, zoals bijvoorbeeld een overheidsdatacenter dat clouddiensten levert aan (Rijks)overheden.

Clouddiensten worden meestal onderverdeeld in **IaaS** (verhuur van infrastructuurdiensten), **PaaS** (verhuur van een ontwikkelplatform) en **SaaS** (via het internet ontsloten softwarediensten).

Belangrijke kenmerken van cloud zijn:

- Je betaalt voor een dienst bij een leverancier die middelen levert en beheert die bereikbaar zijn via internet of een netwerk.
- De aard van de geleverde oplossing kan sterk verschillen, van software als dienst (bijvoorbeeld kantoorautomatisering) tot infrastructuur of platform als dienst (bijvoorbeeld een beheerd containerplatform).
- Je kunt op- en afschalen door meer of minder middelen af te nemen via een (geautomatiseerde) interface; je betaalt alleen voor wat je afneemt.
- Er is standaardisatie van het aanbod.

Cloud kan voordelen bieden voor een organisatie, zoals lage opstartkosten, snelle beschikbaarheid en flexibiliteit. Maar er zijn ook risico's, zoals minder voorspelbare kosten en grotere afhankelijkheid van leveranciers voor bijvoorbeeld databescherming en geboden functionaliteit.

De mate van digitale soevereiniteit verschilt per cloudtoepassing, afhankelijk van factoren zoals de locatie van de data, de toepasselijke wetgeving, de zeggenschap over en het beheer van de infrastructuur en de eigendomsstructuur van de leverancier.

De keuze voor een specifieke cloudtoepassing raakt de continuïteit van het primaire proces, de bedrijfsvoering en/of de strategische ontwikkelingen van de organisatie. Daarom kan de ICT-afdeling deze keuze niet alleen maken: het is bij uitstek een bestuurlijke verantwoordelijkheid. Voorafgaand aan

besluitvorming is het cruciaal om de voor- en nadelen van de verschillende typen cloudoplossingen en -leveranciers goed tegen elkaar af te wegen. Als input voor deze afwegingen geven wij vier overkoepelende adviezen die helpen bij het opstellen van een goede businesscase.

1. Stel de vraag: wat heeft de organisatie nodig?

Uit de praktijk: Ondoordachte keuze voor cloud leidt tot onnodige risico's

In één van onze onderzoeken zagen we een dienst die een kernsysteem voor de uitvoering van primaire processen naar een publieke cloud wilde brengen. Belangrijkste reden was dat het bestaande hostingplatform beëindigd zou worden door de beherende overheidsdienst. Er was echter vooraf nog geen goede afweging gemaakt:

- Er was niet gekeken naar alternatieve omgevingen, zoals overheidsdatacenters.
- Er was geen analyse gemaakt van de privacyrisico's, terwijl het een privacygevoelig proces betrof.
- Er was niet meegewogen dat deze transitie geen toegevoegde waarde zou bieden voor de gebruikers, terwijl die al lang zaten te wachten op nieuwe functionaliteiten.

Op deze manier liep deze dienst het risico veel energie en geld te besteden aan verplaatsing van een systeem, waardoor nieuwe privacy- en beschikbaarheidsrisico's zouden ontstaan en echte problemen onopgelost bleven. We adviseerden dan ook om eerst de behoefte te bepalen en daarna pas een oplossing te kiezen.

De vraag is of het scala aan diensten dat mogelijk is wanneer je gebruikmaakt van commerciële cloudoplossingen wel nodig is. Het aanbod van grote, veelal Amerikaanse, bedrijven is heel breed: rekencapaciteit, opslag, databases en netwerken met mogelijkheden voor bijvoorbeeld automatisch op- en afschalen van de diensten, betalen naar gebruik en geïntegreerde beveiligingsdiensten. Wegen de voordelen die daarmee behaald worden, wel op tegen de risico's, organisatorische impact, inspanningen en (beheer)kosten? Weeg daarbij mee dat gebruikers in de praktijk vaak maar beperkt voordeel hebben van cloud.

Wij adviseren dan ook om, voordat er voor een specifieke cloudtoepassing gekozen wordt, goed te kijken of deze aansluit bij wat de organisatie nodig heeft. Veelal is bijvoorbeeld dynamisch schalen van dienstverlening niet noodzakelijk of kun je keuzes in de architectuur maken die zorgen voor een eenvoudiger ICT-landschap. Daarnaast beschikt de overheid zelf over voldoende schaal om dezelfde voordelen te kunnen realiseren op IaaS-niveau en is een externe leverancier vaak overbodig.

Bepaal wat de organisatie nodig heeft door uit te gaan van de gewenste functionele en niet-functionele eisen:

a) *Baken de keuzes goed af door eisen helder te formuleren*
Maak vooraf een duidelijke afbakening door functionele en technische eisen in kaart te brengen op basis van de onderliggende bedrijfsprocessen, liefst met behulp van een *solution architectuur.* Door dit te doen beperk je het risico dat je onnodige diensten afneemt of diensten die niet aansluiten bij de eisen en wensen van de gebruikers.

Uit de praktijk: Te brede uitvraag leidt tot overbodige functionaliteit

Een rode draad die we in onze onderzoeken zien, is dat overheidsorganisaties die oplossingen willen verwerven, deze met zeer uitgebreide functionaliteit uitvragen. Vaak gebeurt dit op basis van een marktverkenning, waarbij leveranciers een integrale publieke cloudoplossing in de markt willen zetten. De vraag of een clouddienst wel echt nodig is, wordt dan onvoldoende gesteld. Alternatieve opties, zoals met eigen servers werken, zijn niet overwogen of niet goed onderzocht.

Een alternatieve reden die organisaties soms aandragen om een publieke cloud te gebruiken, is de inzet van AI-toepassingen. We zien echter ook dat nog onvoldoende nagedacht is over wat het doel daarvan is. De organisatie vraagt daarom dan maar generieke AI-functionaliteit uit. In plaats daarvan kan door gefaseerd aan te besteden de focus worden verlegd naar de inzet van specifieke AI-functionaliteit op het moment dat dit opportuun is.

b) *Differentieer op basis van informatiebeveiligingseisen*
De inzet van clouddiensten stelt bijzondere eisen als het gaat om informatiebeveiliging. Binnen een organisatie kunnen de eisen op het gebied van beveiliging, toegang en (data)compliance verschillen per type informatie en processen. Het is daarom belangrijk om de inzet van clouddiensten te differentiëren per organisatieonderdeel en type informatie, en alternatieve of hybride oplossingen te verwerven als blijkt dat de standaardoplossing niet voldoet. Zeer gevoelige gegevens (zoals staatsgeheime informatie) mogen niet in een publieke cloudomgeving worden opgeslagen, terwijl dit voor minder gevoelige informatie en standaardprocessen met de juiste maatregelen wél kan. De mate van beveiliging hangt niet alleen af van dataclassificatie, maar ook van juridische eisen zoals de AVG, toegangsrechten en wie verantwoordelijk is voor beheer en gebruik. Ga niet alleen uit van wat mag, maar ook van wat verantwoord is gegeven de risico's.

c) *Bepaal vooraf hoe de beoogde oplossing ingepast gaat worden*
De keuze voor het soort cloudoplossing bepaalt ook de mate van integratie. Grote cloudleveranciers bieden namelijk vaak geïntegreerde totaaloplossingen, waarmee organisaties snel een cloudomgeving kunnen opzetten. Ook hier is het de vraag of zo'n totaaloplossing echt nodig is; de afnemer kan ook een uitvraag per functioneel onderdeel doen (zoals kantoortoepassingen, chat of videobellen). Een geïntegreerde oplossing vergemakkelijkt weliswaar de implementatie en kan functionele voordelen bieden, maar ze leidt tot extra afhankelijkheid van één leverancier (zie ook advies 2). Oplossingen met een combinatie van leveranciers vereisen vaak wel meer eigen integratie en beheer, maar verkleinen afhankelijkheden en leveren mogelijk beter passende oplossingen. Kiezen voor de meest passende oplossing per functionaliteit verhoogt zo de wendbaarheid van een organisatie.

d) *Accepteer kleinere nadelen wanneer dit leidt tot grotere strategische voordelen*
Maak een afweging tussen grotere strategische voordelen (zoals digitale soevereiniteit) en kleinere nadelen op onderdelen (zoals acceptatie van verminderde functionaliteit). Geef hierbij de strategische (veelal langetermijn-) voordelen voldoende gewicht en stuur niet uitsluitend op lokale optimalisatie. Een concreet voorbeeld hiervan is het inleveren van functionaliteit of gebruiksgemak in kantoortoepassingen vanwege de eisen die worden gesteld aan digitale soevereiniteit.

2. Voorkom grote afhankelijkheden van één leverancier

Uit de praktijk: Grote leveranciersafhankelijkheid door keuze voor één cloudleverancier

Bij een onderzoek zagen we dat de organisatie gekozen had om zoveel mogelijk oplossingen van één leverancier af te nemen. Het ging onder meer om de werkplek met kantoorautomatisering, authenticatie en autorisatie van medewerkers, en het archief. Deze vergaande afhankelijkheid van één leverancier maakte een exit binnen een redelijke termijn ingewikkeld of zelfs onmogelijk. Wij adviseerden om te kijken naar *best-of-breed*-oplossingen waarbij per functioneel vraagstuk gezocht wordt naar de beste leverancier.

Een belangrijk nadeel van alle cloudtoepassingen is de grote afhankelijkheid van de aanbieder. Bij alle externe dienstenleveranciers speelt dit, maar het geldt bij uitstek voor een geïntegreerde oplossing (zie advies 1). Het gevolg daarvan is dat weggaan bij een leverancier duur en technisch lastig uit te voeren is. Hierdoor neemt de wendbaarheid van de organisatie af en kunnen leveranciers, zonder grote gevolgen voor henzelf, de voorwaarden veranderen en de prijzen verhogen.

Wij adviseren dan ook om de afhankelijkheden zo klein mogelijk te houden:

- Ontwerp de oplossing zoveel mogelijk onafhankelijk van een specifieke implementatie of leverancier: maak gebruik van open standaarden en waar mogelijk opensourcesoftware.
- Bepaal vooraf welke soort diensten extern wordt afgenomen (IaaS, Paas en/of SaaS), en welke diensten de organisatie in eigen beheer houdt. De aard van de dienst bepaalt immers mede de mate van afhankelijkheid.
- Weeg de keuze af tussen een marktpartij, een overheidspartij of overheidsdatacenter (communitycloud).
- Bepaal hoe je data en diensten kunt meenemen, uitgewerkt per onderdeel van de oplossing.
- Zorg voor een uitgewerkte exitstrategie vóórdat je instapt bij een bepaalde leverancier, opdat je binnen afzienbare tijd afscheid kunt nemen. Een exitstrategie heeft betrekking op zowel het meenemen van data als op het voortzetten van de functionaliteit.
- Werk een plan uit voor wanneer de aanbieder de dienstverlening abrupt stopt.
- Maak een expliciete afweging tussen het implementeren en testen van noodvoorzieningen en het accepteren van verminderde functionaliteit.
- Maak met de leverancier afspraken voor de langere termijn over prijzen en voorwaarden.

3. Zorg voor voldoende kennis in de eigen organisatie

Uit de praktijk: Vertraging bij inrichting cloudplatform door gebrek aan ervaring

Een organisatie die een SaaS-systeem introduceerde dat gegevens van burgers opslaat, besloot om dat systeem binnen het eigen rekencentrum te laten draaien op een privaat cloudplatform. Gegeven de gevoeligheid van de data was dit een goede keuze. Omdat de organisatie het platform nog moest inrichten en daar weinig ervaring mee had, liep het project echter substantiële vertraging op. Wij adviseren dan ook om bij beslissingen over cloudtoepassingen rekening te houden met de capaciteit van de eigen ICT-organisatie en zo nodig maatregelen te treffen.

Een nadeel van de overgang naar clouddiensten is dat dit vraagt om kennis die een organisatie niet altijd al in huis heeft. Daarnaast bestaat het risico dat kennis sluipenderwijs uit de organisatie verdwijnt. Dit is overigens niet alleen bij clouddiensten aan de orde: veel overheidsorganisaties ondervinden bij meer traditionele vormen van uitbesteding vergelijkbare effecten.

Het gevolg van het ontbreken van kennis is dat het moeilijk is om de leverancier effectief aan te sturen, maar ook om van hem afscheid van te nemen. Ook wordt het lastig om voldoende zicht te houden op functionele en architectuurvraagstukken, informatiebeveiliging en compliance. Want de cloudleverancier is dan wel verantwoordelijk voor de implementatie en het leveren van de gevraagde functionaliteit, maar de afnemer blijft zelf verantwoordelijk voor een aantal randvoorwaarden en (technische) koppelingen tussen systemen.

Wij adviseren om actief kennis in huis te ontwikkelen, te halen en te houden op de volgende gebieden:

- contract- en leveranciersmanagement, waaronder een uitgewerkte exitstrategie en afspraken over beschikbaarheid van de dienstverlening
- technische architectuur, inclusief die van de uitwijk- en back-upvoorzieningen
- informatiehuishouding, waaronder ook archivering
- toegangsbeheer en informatiebeveiliging
- logging en monitoring van incidenten via systemen voor Security Incident en Event Management (SIEM) en opvolging door een Security Operational Center, intern dan wel extern
- auditing en compliance conform wet- en regelgeving (zoals AVG, BIO2, archiefwet en Woo)

Om de samenwerking met externe partijen te stroomlijnen, bundelen grote organisaties deze kennis vaak centraal, bijvoorbeeld in een (virtueel) multidisciplinair team.

Het ontwikkelen van kennis kan door strategisch personeelsbeleid, opleidingen en certificeringen, en het stimuleren van samenwerking tussen ICT-teams en (externe) experts. Ook kan het helpen om in de samenwerking met leveranciers duidelijke afspraken te maken over kennisoverdracht, beschikbaarheid van relevante documentatie (zoals architectuurdocumenten), standaardconfiguraties, processen (zoals wijzigingenbeheer, inrichting van logging en monitoring, en incidentrespons-procedures). Op deze wijze blijft de organisatie wendbaarder, behoudt ze regie en kan ze effectief gebruikmaken van de clouddiensten, ondanks de intrinsieke afhankelijkheid van externe partijen.

4. Zorg voor structurele risicoanalyse

Uit de praktijk: De meerwaarde van vroege risicoafweging

Bij een organisatie die bezig was met de introductie van onder andere een documentmanagementsysteem en een samenwerkingsomgeving, constateerden we dat een initiële integrale risicoanalyse ontbrak. Hierdoor kon de organisatie niet vaststellen of de beoogde ICT-voorziening veilig genoeg werd. Op ons advies heeft de organisatie deze risicoanalyse alsnog uitgevoerd, met aandacht voor onder andere statelijke actoren. Daaruit bleek de oplossing niet te voldoen, wat geleid heeft tot een andere, veiligere keuze. Hoe eerder deze risicoafweging wordt gemaakt, hoe minder (kostbare) tijd verloren gaat.

Structurele risicobeheersing bij clouddienstverlening baseert zich op twee afzonderlijke integrale analyses. Een *initiële* risicoanalyse is input voor de afweging over het wel of niet inzetten van een clouddienst en in welke vorm. Een *continue* (periodiek geüpdatete) risicoanalyse is nodig zolang de dienstverlening loopt, voor risico's die er zijn of die kunnen ontstaan. Dit kun je niet overlaten aan de leverancier, omdat de organisatie zelf verantwoordelijk blijft voor de risico's en de leverancier bovendien niet volledig onafhankelijk is bij de beoordeling daarvan.

Wij adviseren bij de initiële risicoanalyse in ieder geval de volgende aspecten mee te nemen:

- **Gegevensbescherming en informatiebeveiliging**. De overheid verwerkt gevoelige data van burgers en bedrijven. Deze moeten erop kunnen vertrouwen dat deze data altijd adequaat beschermd zijn. Dit geldt bij commerciële cloudaanbieders ook voor risico's als gevolg van extraterritoriale wetgeving (zoals de Amerikaanse CLOUD Act en FISA) die buitenlandse overheden toegang kan geven tot in de cloud opgeslagen gegevens. Dat de bescherming van gegevens niet vanzelfsprekend is, bleek uit het nieuws dat informatie van ambtenaren is verstrekt aan een buitenlandse overheid[1]. Voor meer adviezen over grip krijgen op digitale veiligheid verwijzen we naar onze Handreiking strategische digitale veiligheid.
- **Auditeerbaarheid en controleerbaarheid**. De afnemer moet in staat zijn om onafhankelijk te controleren of de leverancier voldoet aan de gestelde eisen. Dit vraagt om voldoende transparantie, medewerking aan audits en beveiligingstests, en om continue aandacht voor monitoring en toezicht zolang de dienstverlening loopt. Zo moet een organisatie die een cloudplatform gebruikt voor de opslag van persoonsgegevens jaarlijks een onafhankelijk auditrapport (bijv. SOC 2, type II) ontvangen en continu inzicht hebben in logging, toegangsbeheer, kwetsbaarheidsscans en beveiligingsincidenten. Daarnaast moeten periodieke penetratietesten en configuratiecontroles van de cloudomgeving aantonen dat de getroffen beveiligingsmaatregelen effectief zijn.
- **Continuïteit en beschikbaarheid**. De clouddienst moet aantoonbaar betrouwbaar en beschikbaar zijn, inclusief de mogelijkheid om hem in noodsituaties gecontroleerd te kunnen afschalen of beëindigen. Zo moet een organisatie die een belangrijk systeem naar de cloud brengt vooraf maatregelen treffen om

[1] Techbedrijven deelden namen Nederlandse ambtenaren met VS: 'Ontzettend zorgelijk' (nos.nl, 22 mei 2026)

de continuïteit van de dienstverlening te waarborgen. Dat kan bijvoorbeeld door afspraken te maken over herstelprocedures, back-ups, beschikbaarheidseisen en een eventuele beëindiging of overgang naar een andere oplossing.
- **Voldoen aan wet- en regelgeving**. De inzet van clouddiensten moet voldoen aan alle relevante wet- en regelgeving, waaronder privacywetgeving en sectorspecifieke normen. Bedenk hierbij ook dat een veilige omgeving voor gebruikers en data het doel is, niet het voldoen aan beleid. Voldoen aan beleid ontslaat je niet van de verantwoordelijkheid om een gedegen eigen risicoanalyse uit te voeren.

De genoemde risico's moet je expliciet maken. Hierbij zul je sommige risico's mitigeren en sommige restrisico's accepteren. Daarnaast zullen er afhankelijkheden blijven bestaan. De besluitvorming hierover en acceptatie hiervan moeten op bestuurlijk niveau plaatsvinden, en transparant en uitlegbaar zijn.

Ook als de contracten zijn gesloten en de dienstverlening loopt, vragen de hierboven genoemde aspecten om structurele aandacht. De omgeving van de organisatie verandert voortdurend, zoals door geopolitieke verschuivingen en veranderingen in wet- en regelgeving. Ook kunnen er veranderingen zijn bij de leverancier. Daarom zijn reguliere en onafhankelijke audits en beveiligingstests blijvend nodig.

Bijlage A
Stel deze vragen bij de keuze voor cloudgebruik:

1. Is er scherp gedefinieerd welk probleem de organisatie probeert op te lossen en waarom de beoogde oplossing de best passende is (op basis van onder meer functionele en technische eisen).

2. Is er een businesscase die de verschillende alternatieven (ook niet-cloud) in beeld brengt en tegen elkaar afweegt op de voor- en nadelen en risico's?

3. Is er een analyse gedaan die helder maakt welke organisatieonderdelen en processen gebruik gaan maken van cloudtoepassingen en is het voor elk organisatieonderdeel duidelijk welke eisen van toepassing zijn op het gebied van informatiebeveiliging, toegang en (data)compliance?

4. Is een noodoplossing noodzakelijk en is die tijdig beschikbaar als de dienstverlening (abrupt) ophoudt en is er een exitstrategie gericht op het meenemen van data en het elders voortzetten van de functionaliteit bij het veranderen van dienstverlener?

5. Voldoet de leverancier/oplossing aan de auditing- en compliance-eisen, conform wet- en regelgeving (AVG, BIO-2, archiefwet, Woo, Cbw, Wwke, CRA, ABRO)?

6. Is er een risicoanalyse gemaakt waaruit blijkt welke mitigerende maatregelen er zijn genomen en welke restrisico's geaccepteerd worden in het geval van ernstige incidenten?

7. Is er op strategisch niveau voldoende aandacht voor kennisontwikkeling en -behoud, zodat de cloudleverancier effectief aangestuurd kan worden en exitstrategieën realistisch zijn?

8. Welke mate van digitale autonomie en soevereiniteit is noodzakelijk/wenselijk bij de keuze voor een bepaalde cloudoplossing?

Deze publicatie is een uitgave van:

Adviescollege ICT-toetsing
info@adviescollegeicttoetsing.nl
www.adviescollegeicttoetsing.nl
Postbus 16292 | 2500 BG Den Haag

september 2026

Adviescollege
ICT-toetsing