

Voorbereiden op een cloudtransitie: “no regrets” stappenplan



Inhoud	Aanleiding en context	03
	Stappenplan voor het voorbereiden op een cloudtransitie	04
	Stap 1: Inventariseer gebruikte cloudapplicaties	05
	Stap 2: Voer een risicoanalyse uit	05
	Stap 3: Ontwikkel een transitiestrategie	06
	Stap 4: Stel een sourcing strategie op	07
	Stap 5: Versterk governance	07
	Stap 6: Overige voorbereidende werkzaamheden	09
	Afsluiting	10
	Neem contact op	11

Aanleiding en context



Nabeel Siddiqie
Cybersecurity Partner
Eraneos

nabeel.siddiqie@eraneos.com

Het is een strategische kwetsbaarheid die veel organisaties in Nederland momenteel delen: een dagelijkse afhankelijkheid van de dienstverlening van Amerikaanse cloudserviceproviders (CSP's) zoals Microsoft, Amazon en Google. De ongekennde concentratie van kritieke IT-infrastructuur bij een handvol buitenlandse partijen brengt afhankelijkheden en risico's met zich mee die niet langer genegeerd kunnen worden. Gezien de geopolitieke verschuivingen van de afgelopen maanden en de toenemende focus op digitale soevereiniteit, is het onverantwoord om de ogen te sluiten voor de potentiële gevolgen. De zorgen over onze digitale soevereiniteit, continuïteit van clouddienstverlening en het waarborgen van de privacy zijn verder opgespeeld – de Tweede Kamer nam op 19 maart 2025 een aantal moties aan, waarin de politieke wil wordt benadrukt om minder afhankelijk te worden van Amerikaanse CSP's.

Tegelijkertijd groeit ook binnen Europa de aandacht voor digitale autonomie. Initiatieven zoals GAIA-X¹ en de European Alliance for Industrial Data, Edge and Cloud² zijn erop gericht om een soeverein en transparant Europees cloud-ecosysteem te ontwikkelen. Deze beweging benadrukt dat cloud-soevereiniteit niet alleen een nationale, maar ook een Europese strategische prioriteit is. Organisaties doen er goed aan om hun transitiestrategie in lijn te brengen met deze ontwikkelingen, en waar mogelijk aan te sluiten bij Europese CSP's of initiatieven die interoperabiliteit en controle over data waarborgen.

Of dit allemaal betekent dat de overheid binnenkort volledig afstapt van Amerikaanse CSP's is lastig voor te stellen. In veel gevallen zijn er geen goede alternatieven, dat is precies het probleem. Toch is het goed dat organisaties – zowel binnen de publieke als private sector – nu nadenken over de potentiële gevolgen van een “cloudtransitie” en hoe ze zich hierop kunnen voorbereiden. De Rijksoverheid onderkent in haar Cloudbeleid³ het belang van het hebben van een exit-strategie.

In dit stuk zetten we uiteen welke stappen organisaties nu al kunnen zetten om zich voor te bereiden op een mogelijke cloudtransitie.

¹ <https://gaia-x.eu>

² <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance>

³ Rapport het Rijk in de Cloud - <https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2025/01/15/het-rijk-in-de-cloud/Het+Rijk+in+de+cloud.pdf>

Stappenplan voor het voorbereiden op een cloudtransitie

Organisaties met voldoende interne kennis en capaciteit kunnen hiermee zelfstandig aan de slag.



Wachten totdat zich een dwingende aanleiding voordoet van een cloudtransitie, bijvoorbeeld doordat een CSP eenzijdig de dienstverlening beëindigt, vergroot de kans op verstoringen van kritieke bedrijfsprocessen. Het is daarom raadzaam om nu al stappen te zetten die altijd bijdragen aan de weerbaarheid: “no regrets” acties. Ook als de organisatie voorlopig niet daadwerkelijk migreert, helpen de maatregelen in dit stappenplan om afhankelijkheden inzichtelijk te maken en risico's te verkleinen.

Organisaties met voldoende interne kennis en capaciteit kunnen hiermee zelfstandig aan de slag. Tegelijk kan het inschakelen van externe expertise aantrekkelijk zijn om valkuilen te vermijden en het proces te versnellen. Wij staan organisaties daar graag in bij. De belangrijkste les is: begin gelijk. Door proactief de onderstaande stappen te volgen, bereiden organisaties zich voor op een soepele overgang, mocht een exit van een Amerikaanse CSP op enig moment wenselijk óf noodzakelijk zijn.

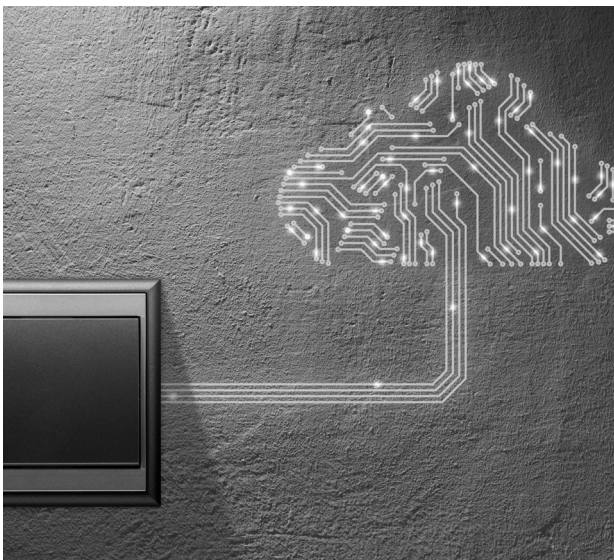
De onderstaande aanpak bestaat uit vijf stappen (in lijn met best-practices en compliance-eisen). Deze stappen kunnen grotendeels parallel worden doorlopen. Waar relevant, verwijzen we naar bestaande kaders en standaarden.

Stap 1: Inventariseer gebruikte cloudapplicaties

Effectieve voorbereiding op een mogelijke migratie is pas mogelijk wanneer inzichtelijk is wat in de cloud draait en wat de potentiële impact van verstoringen kan zijn. De eerste stap is daarom een inventarisatie van alle cloudapplicaties, diensten en onderliggende infrastructuur. Per cloudapplicatie dient relevante informatie verzameld te worden, zoals de opgeslagen data, de geboden functionaliteiten en de koppelingen met andere systemen.

Deze inventarisatie omvat technische componenten (virtual machines, databases, functies, etc.) en processen. Bepaal welke bedrijfsprocessen afhankelijk zijn van cloudapplicaties. Identificeer daarbij de kritieke bedrijfsprocessen en hun cloud-ondersteuning; deze bepalen de migratievolgorde en urgentie. Waardeer assets op gevoeligheid en kritiekheid. Vragen hierbij zijn: welke data is vertrouwelijk of privacygevoelig? Welke applicaties zijn cruciaal voor de continuïteit van de bedrijfsvoering en welke kunnen uitval verdragen? Om de inventarisatie efficiënter en actueler te maken, kunnen organisaties gebruikmaken van geautomatiseerde tooling, zoals Cloud Management Platforms (CMP's), asset discovery tools of "infrastructure-as-code" oplossingen. Denk aan tools zoals Azure Migrate, AWS Application Discovery Service of CMDB-integraties met ServiceNow. Deze helpen bij het in kaart brengen van afhankelijkheden, netwerktopologie en datastromen – cruciale input voor exit- en migratieplanning.

Samengevat, levert deze eerste stap een up-to-date cloud asset register op, inclusief data- inventarisatie en -classificatie. Dit dient als het fundament voor een transitieplanning.



Stap 2: Voer een risicoanalyse uit

Een gedegen voorbereiding vereist verder inzicht in risico's. Daarom is de tweede stap het in kaart brengen van de scenario's en bijhorende risico's van gedwongen of geplande cloudtransitie. Denk bijvoorbeeld aan grootschalige privacyerschendingen, significante prijsstijgingen, (dreiging van) service-uitval bij de provider, of beleidswijzigingen in Nederland die Amerikaanse cloudgebruik beperken. Voor ieder scenario dient per cloudapplicatie de potentiële impact op de organisatie en de waarschijnlijkheid dat het scenario zich voordoet te worden bepaald. De risico's kunnen daarbij naar ernst worden gekwalificeerd, zodat gelijk kan worden opgemaakt welke (meer) prioriteit verdienen.

Een cruciaal onderdeel van de risicoanalyse is het risico op vendor lock-in. In hoeverre komt de beschikbaarheid van data en diensten in gevaar bij een overstap naar een andere omgeving? In het verlengde daarvan: hoe snel kan een migratie worden uitgevoerd, welke afhankelijkheden zijn er, en welke bedrijfsprocessen of externe partijen worden geraakt? Door deze elementen mee te nemen kunnen verschillende exitscenario's worden opgesteld, zoals een noodstop versus een geleidelijke transitie, en kunnen per scenario restrisico's worden vastgesteld.

Naast risico's is het raadzaam om de potentiële kosten van een exit in kaart te brengen – de zogeheten Total Cost of Exit (TCoE). Denk hierbij aan kosten voor datamigratie, licentie-aanpassingen, tijdelijke dubbele infrastructuur of benodigde personele inzet. Het inschatten van deze kosten helpt bij het opstellen van realistische scenario's en voorkomt verrassingen bij daadwerkelijke uitvoering. Ook versterkt het de business case voor tijdige voorbereiding.

De uitkomst van deze tweede stap is een duidelijk inzicht in de risico's van een cloudtransitie en een globale kosteninschatting.



Cloudapplicaties zijn divers en vereisen een eigen aanpak. Sommige diensten zijn eenvoudig over te zetten, andere vragen om ingrijpende aanpassingen.

Stap 3: Ontwikkel een transitiestrategie

Met een helder beeld van het cloudlandschap (stap 1) en de transitierisico's per applicatie (stap 2), kan de organisatie zich richten op de praktische aanpak van een cloudtransitie. Deze stap draait om het ontwikkelen van een concrete strategie voor het verlaten van een cloudapplicatie – of dit nu geleidelijk is of in een noodscenario gebeurt. Tegelijkertijd moet worden nagedacht over alternatieven: waarheen migreren en hoe een (hernieuwde) lock-in voorkomen? Dit wordt vastgelegd in een sourcingstrategie.

Cloudapplicaties zijn divers en vereisen een eigen aanpak. Sommige diensten zijn eenvoudig over te zetten, andere vragen om ingrijpende aanpassingen. Het is daarom verstandig om vooraf migratiepaden te definiëren (verplaatsen, aanpassen, vervangen, afstoten). Ook afhankelijkheden zijn belangrijk: welke API's, data-uitwisselingen of geïntegreerde diensten moeten mee? En hoe worden kritieke processen beschermd tegen onderbrekingen? Een gefaseerde aanpak – eerst de minst complexe systemen – kan risico's spreiden.

Het is bovendien raadzaam deze plannen⁴ te oefenen, door bijvoorbeeld eenmaal per jaar een subset van applicaties en data te migreren naar een andere omgeving en weer terug. Complexere strategieën kunnen bijvoorbeeld met een table-top oefening getoetst worden. Dergelijke oefeningen onthullen hiaten, en geven inzicht in hersteltijden. Bevindingen dienen te worden gedocumenteerd en het plan moet worden verbeterd waar nodig.⁵

Na deze stap heeft de organisatie een concreet beeld van de wijze waarop cloudapplicaties kunnen worden afgebouwd, inclusief herstelplannen en migratiepaden.

⁴ ISO/IEC 27001:2022 – Annex A.5.23

⁵ NIST SP 500-322: Cloud Computing Reference Architecture - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf>

Stap 4: Stel een sourcing strategie op

Parallel aan de transitie-voorbereiding is het cruciaal om de toekomstige sourcing te overwegen. Welke alternatieven zijn er na een cloudtransitie, en hoe wordt hernieuwde vendor lock-in voorkomen?

Om lock-in te beperken en wendbaarheid te vergroten, kan een organisatie een multi-cloud- of dual-vendorstrategie implementeren. Dit houdt in dat diensten over meerdere CSP's worden verdeeld, met aandacht voor data- en workload-portabiliteit. Het hanteren van een sourcingportefeuille helpt bij het beoordelen en periodiek evalueren van CSP's op criteria als kosten, compliance, datasoevereiniteit en technologische innovatie. Dit resulteert in een gestructureerde aanpak voor weloverwogen sourcingkeuzes.

Een cloudtransitie impliceert niet noodzakelijk een volledig afscheid van de cloud. Het kan ook een overstap naar een andere provider betreffen, bijvoorbeeld een Europese CSP met betere garanties op het gebied van soevereiniteit en compliance. Bij de selectie van een nieuwe CSP zijn juridische en compliance-eisen, technische capaciteiten, kosten en toekomstbestendigheid⁶ cruciale aandachtspunten.

Na deze stap beschikt de organisatie over inzicht in niet alleen hoe de cloud te verlaten, maar ook waarheen eventueel gemigreerd kan worden – met behoud van grip op strategische en operationele eisen.

Stap 5: Versterk governance

De transitie- en sourcing-strategie zijn geen eenmalig documenten, maar vormen een integraal onderdeel van continue governance. Het is essentieel dat de aandacht hiervoor wordt verankerd in beleid, processen en controles. Deze vijfde stap omvat een aantal cruciale aspecten voor het versterken van de governance.

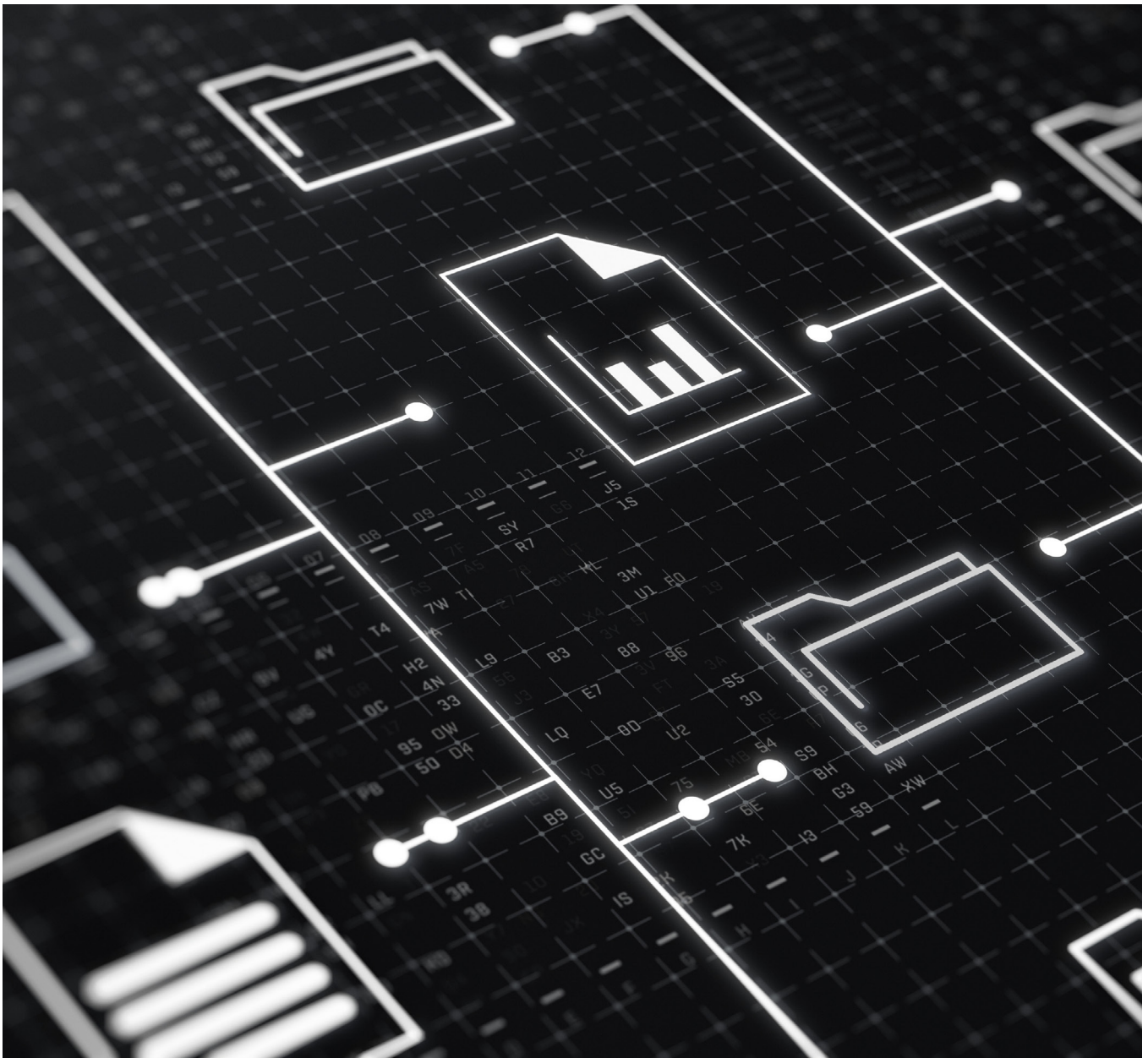
Beleid en governance: Allereerst dient gezorgd te worden voor integratie in bestaand beleid en architectuurgovernance. Bij ieder (nieuw) cloudinitiatief moet dan de vraag worden gesteld hoe de cloudapplicatie vervangen kan worden, indien nodig. Dit kan worden uitgewerkt in cloudbeleid en architectuurprincipes. Organisaties kunnen bijvoorbeeld vastleggen dat bij iedere (nieuwe) cloudoplossing een exitplan moet worden opgesteld. Het BIO-normenkader⁷ positioneert de exit-strategie expliciet als onderdeel van bedrijfscontinuïteitsmanagement en ook de “Digital Operations and Resilience Act” (DORA) benadrukt het belang ervan, wat aangeeft dat dit een bestuurlijk aandachtspunt is.

Procurement speelt een belangrijke rol, met name bij het borgen van exit-afspraken in contracten en het implementeren van inkoopvoorwaarden die soevereiniteit ondersteunen. Daarnaast moeten business units actief worden betrokken bij het prioriteren van cloudapplicaties en het beoordelen van risico's. Zij hebben het beste zicht op de impact op processen en dienstverlening.

Transitie- en sourcingstrategieën moeten worden verankerd in het bredere sourcing lifecycle management. Dat betekent dat bij contractverlengingen, leveranciersevaluaties en nieuwe inkooptrajecten structureel wordt gekeken naar het transitiepotentieel van de dienst. Organisaties kunnen bijvoorbeeld werken met een maturitymodel om periodiek te beoordelen in hoeverre een cloudomgeving potentieel heeft voor transitie. Dit zorgt voor continue verbetering en helpt te voorkomen dat afhankelijkheden opnieuw ontstaan.

6 ENISA – Guidelines for SMEs on Secure Use of Cloud Computing - <https://www.enisa.europa.eu/publications/cloud-computing-security-for-smes>

7 Richtlijn voor Nederlandse overheden, benoemt exit-strategieën als onderdeel van continuïteit - <https://www.informatiebeveiligingsdienst.nl/bio/>



Cloud-neutrale architecturen: organisaties kunnen een ontwerp- en ontwikkelingsaanpak implementeren waarbij systemen en applicaties niet afhankelijk zijn van specifieke CSP's.

Bewustwording: Tot slot is bewustwording binnen de organisatie cruciaal. Beleidsmakers en bestuurders moeten het strategisch belang inzien, terwijl operationele teams moeten weten hoe te handelen bij een exit en hoe omgegaan moet worden met sourcing van nieuwe CSP's. Periodieke sessies of table-top oefeningen kunnen helpen iedereen scherp te houden.

Door aandacht voor transitie en sourcing te integreren in de governance cyclus, voldoet de organisatie niet alleen aan diverse normenkaders, maar versterkt ook de algehele digitale weerbaarheid. Een organisatie met een solide exit-strategie zal ook bewuster omgaan met leveranciersmanagement in het algemeen – wat bijdraagt aan betere beslissingen over toekomstig cloudgebruik.

Stap 6: Overige voorbereidende werkzaamheden

Er zijn aanvullende voorbereidende werkzaamheden die de organisatie kan uitvoeren.

Contractuele borging: Het is raadzaam om de huidige contracten met CSP's te analyseren op bepalingen rondom beëindiging. Veel cloudcontracten focussen op onboarding en dagelijkse dienstverlening, maar offboarding is even cruciaal. Idealiter bevat de overeenkomst een expliciete exit-strategie met exit-triggers, opzegtermijnen, migratietijd en leveranciersondersteuning bij dataportabiliteit.

Bestaande contracten dienen te worden gecontroleerd op dergelijke bepalingen. Als deze ontbreken, moet worden onderzocht of aanvullende clausules kunnen worden opgenomen bij heronderhandeling of verlenging. Nieuwe contracten zouden standaard exit-voorwaarden moeten bevatten; dit dient te worden opgenomen in inkoopvoorwaarden en -beleid. Contractuele vastlegging van exit-afspraken voorkomt misverstanden en verlaagt de drempel voor migratie indien nodig.

Back-ups buiten de cloud: Vendor lock-in kan worden beperkt door regelmatige back-ups buiten de cloud op te slaan, bijvoorbeeld on-premise. Belangrijk is dat deze back-ups in een portabel formaat zijn, zodat ze bij een exit direct kunnen dienen als bron voor herstel.

Cloud-neutrale architecturen: organisaties kunnen een ontwerp- en ontwikkelingsaanpak implementeren waarbij systemen en applicaties niet afhankelijk zijn van specifieke CSP's. Dit wordt aangeduid als cloud-neutrale architectuurprincipes. Het doel hiervan is het behouden van flexibiliteit, zodat organisaties zonder grote aanpassingen kunnen migreren tussen clouds, over kunnen stappen naar een hybride omgeving, of zelfs terug kunnen keren naar on-premises infrastructuur.

Escrow als maatregel: Escrow van broncode kan een laatste redmiddel zijn bij plotselinge uitval van een CSP. Periodieke controle van escrow-regelingen op actualiteit, volledigheid en bruikbaarheid is essentieel. Voor kritieke SaaS-diensten zonder escrow kunnen alternatieven worden overwogen, zoals maandelijkse data-exporten bij een notaris. Het doel is te voorkomen dat de organisatie zonder middelen komt te zitten bij het wegvallen van een CSP.

Fallback-omgeving: Het definiëren van een fallback-omgeving voor het geval de primaire cloud niet beschikbaar is, is raadzaam. Dit kan variëren van een minimale on-premises omgeving voor essentiële diensten tot infrastructuur-as-code scripts voor een alternatieve cloud. Volledige redundantie is kostbaar, maar de organisatie moet wel weten hoe snel een omgeving operationeel kan worden gemaakt. Praktische tests zijn hierbij essentieel.

Juridische controle: Contracten met CSP's dienen ook aandacht te besteden aan data residency en de juridische controle over data. Door bijvoorbeeld expliciet vast te leggen dat data binnen de EU wordt opgeslagen en verwerkt, verkleinen organisaties hun blootstelling aan buitenlandse wetgeving zoals de U.S. CLOUD Act. Voor sectoren met strenge regelgeving – zoals zorg, overheid of financiële instellingen – is dit een essentieel aandachtspunt binnen zowel contractering als risicobeheersing.

Deze maatregelen vormen een veiligheidsnet. Mocht de toegang tot een Amerikaanse CSP abrupt wegvallen, dan kan de organisatie blijven functioneren – zij het mogelijk in afgeslankte vorm – met behoud van essentiële gegevens. Dit is niet alleen cruciaal voor noodsituaties, maar versterkt ook de onderhandelingspositie richting CSP's in normale omstandigheden. De organisatie is immers in staat de diensten van de CSP te verlaten indien noodzakelijk, wat een prikkel vormt voor goede dienstverlening.

Afsluiting

Door bovenstaande stappen te nemen, bouwen organisaties aan een solide voorbereiding op een eventuele transitie uit Amerikaanse cloudomgevingen. Dit stappenplan is gericht op "no regrets"-acties: ze leveren direct waarde op in de vorm van beter inzicht, minder afhankelijkheid en hogere compliancy, ongeacht of een migratie uiteindelijk plaatsvindt of niet. Organisaties sluiten hiermee als het ware een verzekering af tegen toekomstige onzekerheid in het cloudlandschap.

De urgentie om dit op te pakken is duidelijk, met toenemende zorgen over vendor lock-in en datasoevereiniteit en expliciete eisen vanuit beleid en standaarden om transitieplanning op orde te hebben. Tegelijk is de aanpak beheersbaar: veel van deze stappen liggen in het verlengde van normale IT-governance en beveiligingspraktijken en zijn al onderdeel van reguliere beleid en best-practices.

Tegelijkertijd biedt een transitie-voorbereiding ook de kans om bredere sourcingvraagstukken opnieuw te beoordelen: past de huidige cloudstrategie nog bij de ambities van de organisatie? Zijn er betere combinaties mogelijk van publieke, private of hybride modellen? Door transitieplanning structureel te koppelen aan sourcing- en architectuurbeleid, ontstaat een toekomstbestendige en wendbare cloudaanpak.

Met deze aanpak in de hand kunnen beleidmakers, IT-managers en CISO's direct aan de slag om hun organisatie digitaal autonoom en veerkrachtiger te maken. En hoewel veel voorwerk intern kan worden gedaan, is het inschakelen van specialistische ondersteuning waar nodig een verstandige investering om het tempo en de diepgang te vergroten, bijvoorbeeld bij het automatiseren van assetinventarisaties of het ontwerpen van cloud-neutrale architecturen.

Kortom, de boodschap van dit stuk is een oproep tot actie: bereid nú een transitie voor. Door nu te handelen, houden organisaties in de toekomst tegen lagere risico's en kosten alle opties open in een voortdurend veranderende cloudomgeving. Zelfs als een daadwerkelijke transitie nooit nodig blijkt, levert deze proactieve voorbereiding blijvende waarde op in de vorm van betere beslissingen omtrent cloud, scherpere contracten en een bewuster leveranciersmanagement op de lange termijn. Het resultaat is dat organisaties in control blijven, ongeacht de ontwikkelingen in het cloudlandschap. Wees klaar voor een transitie: ook als die hopelijk nooit nodig zal zijn. Eraneos staat klaar om organisaties hierin te begeleiden.

Neem contact op:



Nabeel Siddiqie
Cybersecurity Partner
Eraneos

nabeel.siddiqie@eraneos.com



Michel Dieben
Senior Manager - Cybersecurity
Eraneos

michel.dieben@eraneos.com



Neem
contact op

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

Michel Dieben
Senior Manager - Cybersecurity
Eraneos
michel.dieben@eraneos.com

Eraneos Netherlands
De Passage 126-136
1101 AX Amsterdam
+31 20 305 3700
info.nl@eraneos.com
eraneos.nl