# Zekerheid over migreren naar de **Cloud**

IT-auditors geven zekerheid over ICT-vraagstukken. Een vraagstuk waar IT-beslissers en managers op dit moment voor staan, is wat zijn of haar organisatie gaat doen met cloudcomputing. 'Gaan we de cloud in of niet?', is een veelgehoorde vraag. Is het een fundamentele ICT-verandering of slechts een hype die wel overwaait? Iedere gerenommeerde leverancier biedt namelijk ondertussen actief clouddiensten aan. Voor veel beslissers is dit een lastig vraagstuk waar ze graag met een deskundige over praten. IT-auditors kunnen daarom een belangrijke bijdrage leveren aan een zorgvuldige besluitvorming over al dan niet migreren naar de cloud.

CHRIS WAUTERS

Ook als een organisatie haar ICT-voorzieningen (nog) niet in de cloud heeft ondergebracht, is er een goede kans dat er binnen de organisatie al gebruikgemaakt wordt van clouddiensten. Zo is de kans groot dat de medewerkers al intensief gebruik maken van applicaties als Dropbox of Google Docs, of maildiensten in de cloud. Alleen al hierdoor verdient cloudcomputing de aandacht van het management en de IT-auditor.

Laten we eerst definiëren wat we in dit artikel onder cloudcomputing verstaan. Een veelgebruikte definitie van cloudcomputing wordt gegeven door NIST [NIST11]: 'Een model om op afroep, op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare computer resources (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers.'

Cloudcomputing kan het beste beschreven worden aan de hand van een aantal eigenschappen. Zo is een clouddienst direct toegankelijk via internet en eenvoudig schaalbaar. En afnemers van clouddiensten betalen alleen voor het daadwerkelijke gebruik. De in gebruik zijnde ICT-middelen bij deze clouddiensten worden door leveranciers gedeeld, waardoor er efficiënt om wordt gegaan met de aanwezige ICT-capaciteit. De clouddiensten zijn af te nemen in de vorm van infrastructuur, platform en software.[1]

Deze eigenschappen van cloudcomputing zorgen ervoor dat clouddiensten met name relevant zijn wanneer er veranderingen in de ICT van een organisatie op komst zijn. Deze veranderingen kunnen komen vanuit de 'business'. Denk hierbij aan grote wijzigingen, een vraag om adaptief vermogen, of vernieuwende aanpak waar ICT een doorslaggevende rol in speelt. Ook als er grote investeringen in huidige applicaties en/of infrastructuur nodig zijn, is het een goede aanleiding om clouddiensten te overwegen. Op het moment dat cloudcomputing relevant is, moet er een gedegen keuze over worden gemaakt. Het vervolg van dit artikel kan daarbij helpen.

## BESLUITEN OVER CLOUDCOMPUTING

Cloudcomputing wordt vaak gezien als dé oplossing voor problemen in het ICT-domein. Volgens veel leveranciers zijn clouddiensten goedkoper, veiliger en werken ze ook nog beter. In de praktijk blijkt dat de voordelen van cloudcomputing sterk variëren en afhangen van de speci-

fieke situatie. Ook zijn er nadelen: bij het werken in de cloud komen net als bij interne ICT-voorziening zaken kijken zoals beveiliging, kosten en regie. Daarom moet er ook bij cloudcomputing gedegen besluitvorming zijn over de manier waarop een organisatie met cloudcomputing omgaat.

Belangrijk is dat de besluitvorming niet verschraalt tot alleen een kostenoverweging. In tijden van economische neergang en krappe(re) budgetten kan de verleiding namelijk groot zijn om cloudcomputing te omarmen op basis van te verwachten initiële kostenbesparingen. Dit gevaar is vooral aanwezig omdat aanbieders van clouddiensten inspelen op deze zoektocht naar kostenbesparingen. Dit gebeurt veelal door bij hun diensten alleen op eventuele kostenbesparingen en prijsvoordelen te wijzen. In dit artikel wordt nader ingegaan op de factoren die naast het kostenplaatje overwogen moeten worden. Het geeft een overzicht en een denkkader, zonder te pretenderen een volledige checklist te bieden voor de besluitvorming over cloudcomputing.

## KEN UW ORGANISATIE

Om een goede keuze te maken over het gebruik van clouddiensten, moet de IT-beslisser de eigen organisatie goed kennen. Dit betekent dat de werkprocessen en systemen binnen de organisatie duidelijk in beeld moeten zijn om zo te bepalen wat succesvol bij een leverancier in de cloud kan worden geplaatst en wat niet. Een degelijke beschrijving van de uitgangspunten, principes en samenhang tussen bedrijfsdoelstellingen, processen en ICT speelt hierin een belangrijke rol. Dit vormt de bedrijfs- en ICT-architectuur en betekent dat het volledig duidelijk is wat de verbindingen zijn tussen diensten van de cloudleverancier en de ICT-diensten die de eigen organisatie levert.

Ook een niet te onderschatten aspect in de besluitvorming is hoe medewerkers omgaan met clouddiensten. Medewerkers kunnen er al best veel ervaring mee hebben, maar kunnen ook weerstand hebben tegen de verandering in de manier van werken die bij de clouddiensten horen. Ook kan het zijn dat ze de clouddiensten niet goed of veilig gebruiken. Clouddiensten kunnen een belangrijke 'enabler' zijn om anders te gaan werken. Denk hierbij aan de toepassing van Bring Your Own Device en Het Nieuwe Werken [WAUT12]. Het management dat beslist over cloudcomputing moet wel goed in beeld hebben welke houding (groepen)medewerkers hebben ten opzichte van clouddiensten. De invoering van clouddiensten kan daarom het beste samen met de medewerkers worden ontwikkeld.

## BEZUINIGEN MET CLOUDCOMPUTING?

Van cloudcomputing wordt vaak gezegd dat het grote besparingen oplevert. De vraag is in hoeverre dit ook zo in praktijk is. Op papier zijn er kostenbesparingen mogelijk ten opzichte van lokaal beheerde ICT-voorzieningen. Zo liggen de investeringen in ICT-infrastructuur niet meer bij de eigen organisatie. Ook wordt er niet meer betaald voor softwareproducten waar eigenlijk weinig gebruik van wordt gemaakt. Er geldt immers het 'pay as you go'-principe, waarbij alleen wordt betaald voor het daadwerkelijke gebruik.

De beschikbare ICT-middelen zijn bij cloudcomputing beter af te stemmen dan bij lokaal beheerde ICT. De investeringen in lokaal beheerde ICT-middelen zijn namelijk niet goed af te stemmen op wisselende behoefte van de organisatie. Dit leidt óf tot overinvesteringen met te veel middelen óf juist tot een tekort aan ICT-middelen. De cloudcomputingdiensten zijn daarentegen op elk moment af te stemmen op de daadwerkelijke behoeften. Wanneer er bijvoorbeeld tijdelijk meer opslagruimte of rekenkracht nodig is, kan dit snel en eenvoudig worden afgenomen bij de cloudleverancier. Het financiële voordeel zit in de schaalbaarheid en wordt behaald doordat de afgenomen clouddiensten naar gebruik worden betaald.

Cloudcomputing biedt een gestandaardiseerde ICT-omgeving aan meerdere afnemers. Dit is een belangrijk verschil met lokaal beheerde ICT, waar één afnemer exclusief wordt bediend met een toegesneden ICT-dienstverlening. De combinatie van de grote schaal en de veelal generieke (gestandaardiseerde) diensten waarmee cloudleveranciers werken, zorgen ervoor dat clouddiensten door een lagere kostprijs goedkoper kunnen worden aangeboden aan afnemers.

Kunnen we hiermee aannemen dat het organisatiebudget in alle gevallen gebaat is met het uitbesteden van de ICT naar de cloud? Niet per se. Wanneer we verder kijken dan de theoretische kostenvoordelen kunnen we bijkomende kosten zien bij uitbesteding van ICT-diensten naar de cloud. Er verandert immers veel binnen de organisatie. De eigen hardware die werd gebruikt wordt grotendeels overbodig. In veel gevallen zullen deze middelen nog niet afgeschreven zijn en wanneer ze niet kunnen worden verkocht, leidt dit tot desinvestering en afwaarderen van de resterende boekwaarde. Ook kunnen er wijzigingen nodig zijn in de personele bezetting. Afscheid nemen van personeel leidt tot afvloeiingskosten en een verlies aan ICT-specifieke kennis [CHUN11].

Wat betekent migratie naar de cloud voor kosten op de lange termijn? Wanneer we kijken naar applicaties met een lange levensduur zien we dat de kosten van lokaal beheer in het begin hoog zijn, maar op de lange termijn afnemen. De hardware raakt dan afgeschreven en beheerkosten worden lager doordat kinderziekten die ▸

zich bij aanvang voordoen zijn verholpen. De kosten voor cloudcomputing blijven hetzelfde over de hele looptijd van de applicatie en kunnen hiermee op termijn hoger uitvallen dan bij lokaal beheerde ICT. Het is hierdoor belangrijk om inzicht te hebben in de vermoedelijke looptijd van een specifieke applicatie om iets te kunnen zeggen over het verschil in kosten tussen eigen beheer en het afnemen van clouddiensten. Aan de andere kant kunnen er op de lange termijn ook weer bijkomende kosten optreden vooral wanneer de organisatie de ICT in eigen beheer heeft. Denk hierbij aan benodigde upgrades en bijkomende kosten wanneer de looptijd van de ondersteuning van de software ten einde komt. Oude applicaties vereisen ook specifieke expertise, deze wordt met de tijd schaars en daarmee duur. Kort gezegd zijn er vele, soms moeilijk voorzienbare, factoren die van invloed kunnen zijn op de kosten van zowel cloudcomputing als ICT in eigen beheer. Een goede kostenafweging vereist gedegen onderzoek naar de bovengenoemde factoren.

## JURIDISCH EN BELEIDSMATIG KADER

Om een goede keuze te maken over het gebruik van clouddiensten moet de IT-beslisser rekening houden met vigerend beleid en wet- en regelgeving. Vanuit verschillende rechtsgebieden (bijvoorbeeld Nederland, EU, Verenigde Staten et cetera) kunnen beperkingen aan het gebruik van cloudcomputing worden gesteld, zoals beperking van export van data, eisen aan beveiligingsmaatregelen, en eisen in relatie tot compliance en uitvoeren van audits. Niet voldoen aan wet- en regelgeving kan leiden tot juridische consequenties, sancties van toezichthouders, verlies van bestaande certificeringen, maar ook financiële schade en imagoschade.

Vanuit juridisch perspectief is een aantal punten van belang. Ten eerste is het belangrijk om inzicht te hebben in geldende wet- en regelgeving, standaarden, richtlijnen en certificeringen waaraan de organisatie moet voldoen. Daarbij is het ook van belang om te weten binnen welke rechtsgebieden de gegevens in de clouddienst worden opgeslagen. Een derde punt is dat de cloudleverancier door het toelaten van externe, onafhankelijke audits moet kunnen aantonen te voldoen aan geldende eisen vanuit wet- en regelgeving. [NCSC12]

De meest relevante wetgeving met betrekking tot cloudcomputing gaat over privacy (zoals in Nederland de Wet bescherming persoonsgegevens). Wanneer persoonlijke data op servers op afstand (in andere landen en/of continenten) belanden, kunnen organisaties de controle hierover verliezen. De vraag hierbij is wel altijd in hoeverre dit ook voor alle gegevens een daadwerkelijk probleem is, of slechts voor een klein deel van de gegevens.

> De Rijksoverheid heeft een cloudstrategie geformuleerd waarin staat dat er gekozen wordt voor een gesloten (interne) cloud onder beheer van de overheid zelf. Deze keuze wordt vooral gemaakt om privacy en betrouwbaarheid te kunnen waarborgen. Dit komt tegemoet aan de politieke wens om cloudcomputing te gebruiken, maar zorgvuldig met beveiliging om te gaan. Organisaties in de publieke sector zullen hier met name rekening mee moeten houden. [TK11-1] [TK11-2]

## VERSCHUIVENDE BEDREIGINGEN

Cloud computing roept veel vragen op rond het thema beveiliging. Het is niet perse veiliger of minder veilig dan ICT in eigen beheer. Bij migratie naar de cloud veranderen bedreigingen op het gebied van onder andere privacy, data-integriteit en de continuïteit van infrastructuur. Op deze veranderingen moet op een juiste manier worden ingespeeld.[2]

Omdat cloudtechnologie afhankelijk is van een internetverbinding, is de continuïteit van clouddiensten afhankelijk van de continuïteit van een internetverbinding. Een goede en betrouwbare internetleverancier is hiermee van vitaal belang.

Een tweede belangrijk punt dat verandert op gebied van beveiliging heeft betrekking op de medewerkers in de eigen organisatie. Door gebruik van cloudcomputing kan in principe iedereen toegang krijgen tot gegevens en systemen van een organisatie. Dit zorgt ervoor dat beheer van gebruikers en toegangscontrole van vitaal belang is. Medewerkers delen bijvoorbeeld documenten via internet maar kunnen hierdoor allerlei beveiligingsrisico's nemen (denk aan virussen, malware en extern opgeslagen inlogcodes).

Ook de beheersbaarheid van processen en systemen verandert bij de invoering van cloudcomputing in de organisatie. De mogelijkheden voor beheersing en controle worden namelijk goeddeels bij de cloudleverancier ondergebracht. De leverancier moet aan gestelde beveiligingseisen en eisen met betrekking tot gegevensbescherming voldoen. Hoewel er wordt uitbesteed, blijft een organisatie nog steeds verantwoordelijk voor de eigen gegevens en moet daardoor toezien op een correcte werkwijze van de cloudleverancier. Het beheer van gebruikers, incidentbeheer en het beheer van wijzigingen zijn eveneens belangrijke aandachtspunten bij cloudcomputing. De relatie met een cloudleverancier moet hiervoor goed worden bewaakt.

## CLOUDREGIE

Uit de verschuivende bedreigingen blijk onder andere dat het belangrijk is om een goede relatie met de cloudleverancier te onderhouden. Gebruikmaken van clouddiensten verschilt niet fundamenteel van een andere vorm van uitbesteding. Heldere afspraken tussen een

(overheids-)organisatie en haar (cloud)dienstverleners zijn essentieel om deze uitbesteding goed in te richten.[3]

De regieorganisatie heeft een tweeledige functie ten opzichte van de (cloud)dienstverlener: enerzijds stuurt ze de dienstverlener aan en anderzijds controleert ze de dienstverlener [WAUT08]. Een Service Level Agreement (SLA) helpt de regieorganisatie deze rol goed te vervullen. In de SLA staat namelijk beschreven wat voor diensten worden geleverd en hoe dit gebeurt. Er zijn verschillende punten van belang in een SLA met een cloudleverancier. Het is vooral belangrijk dat de service level aansluit bij wat er vanuit de organisatie nodig is: bedrijfskritische processen stellen hogere eisen aan clouddiensten, dan processen die minder belangrijk zijn voor een organisatie. Bij cloudleveranciers die gratis diensten leveren, zijn er weinig mogelijkheden om invloed uit te oefenen. Wel is het van belang om voorwaarden voor eigendom, gebruikersrecht, beveiliging en fysieke locatie van de data goed te kennen voordat er van de gratis dienst gebruik wordt gemaakt.

Een duidelijke SLA is dus een belangrijke voorwaarde om regie te houden.[4] In de SLA moet onder meer rekening gehouden worden met 'dataportabiliteit', het moet mogelijk zijn om data over te zetten naar een andere cloudleverancier zodat het risico op *vendor lock in* kan worden verminderd. Hierbij is het dataformaat van belang. Dit kan het beste een open standaard zijn. Verder is aansprakelijkheid belangrijk, zo moet bijvoorbeeld duidelijk zijn wat onder overmacht verstaan wordt en is het verder van belang om te weten wat in de algemene voorwaarden van een clouddienstverlener over aansprakelijkheid staat. Kwaliteit van levering is het derde punt waar de SLA duidelijkheid over moet geven. Hierbij is het van belang om te zorgen dat er een leveringsverplichting is voor de cloudleverancier en geen inspanningsverplichting. Deze leveringsverplichting vereist een zeer precieze omschrijving en het moet duidelijk zijn hoe deze verplichting gemeten wordt. Ook de methode om gebruikerstevredenheid te meten, dient duidelijk beschreven te zijn. Een laatste aandachtspunt is de beschikbaarheid: hoe hoger, hoe beter. Voor al deze wijzen van kwaliteitsmonitoring moet bovendien duidelijk beschreven zijn welke procedure wordt gevolgd bij onenigheid. [TEUN12]

Om de kwaliteit van levering te stimuleren kan gebruikgemaakt worden van *incentives*. Zo kunnen boeteclausules in de SLA opgenomen worden als er niet wordt geleverd, hierbij is het gevaar echter dat de cloudleverancier met de boeteclausules de juridische aansprakelijkheid afkoopt. Het gebruik van bonussen voor het behalen van service levels werkt in dit geval beter. 'Beveiliging en privacy' zijn ook belangrijk om in de SLA op te nemen. Hierin moet bijvoorbeeld duidelijk staan welke partij verantwoordelijk is voor een backup van de data, waarbij het dataformaat wederom van belang is. Ook is het belangrijk dat de clouddienstverlener uitwijkmogelijkheden heeft als er zich een calamiteit voordoet in één van de datacenters. Dan moet de clouddienstverlener uit kunnen wijken naar een andere locatie. Wat betreft pricacy en veiligheid is het cruciaal om te weten of de data binnen de EU opgeslagen staat en is het nuttig om periodieke audits op dit vlak te eisen. Wederom is het belangrijk om ondubbelzinnig vast te leggen dat de data juridisch, en enig eigendom van de organisatie is en niet van de cloudleverancier of derden.

Naast alle bovengenoemde punten in de SLA is het voor de regieorganisatie nodig om een exitstrategie te hebben voor het geval er voor gekozen wordt van een andere (cloud) dienstverlener gebruik te maken. Met name dataportabiliteit en kennis van de eigen organisatie zijn hiervoor van belang. Een *fallback scenario* met een alternatief voor de huidige clouddienstverlener mag dan ook niet ontbreken bij de regieorganisatie.

## CONCLUSIE

Eigenlijk kan niemand meer om de cloud heen. Ook IT-auditors niet. Cloudcomputing is niet de oplossing voor alles, maar betekent een andere manier van inrichten van ICT die veranderingen op verschillende gebieden met zich meebrengt. IT-auditors kunnen een belangrijke bijdrage leveren aan een zorgvuldige afweging over cloudcomputing. De keuze voor cloudcomputing mag namelijk niet verschralen tot uitsluitend een financiële afweging. Er moet goed nagedacht worden over de kosten, risico's en kansen van een eventuele migratie naar de cloud. Hiernaast moet rekening gehouden worden met de eigen organisatie, qua werkprocessen, systemen en medewerkers. Het juridisch en beleidsmatig kader waarbinnen cloudcomputing zich bevindt, moet ook zorgvuldig meegewogen worden in de besluitvorming. De verschuiving van bedreigingen die gepaard gaat met gebruik van cloudcomputing moet duidelijk zijn en de regie op de clouddienstverlener moet goed ingericht worden. Zeker als de IT-auditor gesprekspartner is van het management, kan het management een genuanceerd besluit nemen over welke onderdelen van de organisatie in aanmerking komen voor cloudcomputing en onder welke voorwaarden. Cloudcomputing kan de organisatie veel brengen, als je maar voldoende zekerheid hebt en bewust kiest. ■

*Dank gaat uit naar Koen Wortmann en Marcel van der Steen, managementtrainees van PBLQ HEC en medeauteurs van het oorspronkelijke artikel in TIEM.*

**Noten**

1 Deze vormen staan bekend als IaaS, PaaS en SaaS. Bij IaaS (Infrastructure as a Service) levert een leverancier hardwarecapaciteit via het internet. Bij PaaS (Platform as a Service) biedt een leverancier een computer- en softwareplatform waarop de klant zelf diensten en voorzieningen kan ontwikkelen. Bij SaaS (Software as a Service) worden applicaties via het internet aangeboden.

2 Bron: NCSC Whitepaper, Cloudcomputing & Security (2012).

3 Het aansturen van een (cloud)dienstverlener wordt aangeduid met regievoering, wat door een regieorganisatie wordt gedaan. In [WAUT08] staat uitgebreid beschreven waar bij uitbesteding rekening mee gehouden dient te worden.

4 Een meer uitgebreid overzicht van punten die in een SLA moeten terugkomen staat beschreven in [TEUN12]

**Literatuur**


[CHUN11] Mike Chung, Is Cloudcomputing goedkoper? in: *Automatiseringgids* - 23 november 2011.

[TK11-1] Tweede Kamerbrief betreft: Cloud Strategie - 20 april 2011.

[TK11-2] Tweede kamerbrief betreft: I-strategie Rijk - 12 november 2011.

[NIST11] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing* - September 2011.

NCSC12] Nationaal Cyber Security Centrum, *Cloudcomputing & Security, Whitepaper*, januari 2012.

[TEUN12] Fred Teunissen, 14 juridische aandachtspunten in de cloud in: *Automatiseringgids* - 30 maart 2012.

[WAUT08] Chris Wauters, Marcel Spruit & Mark Vermeulen, *Opgeruimd staat netjes? Uitbesteden van ICT in de publieke sector* - april 2008.

[WAUT12] Chris Wauters & Lancelot Schellevis, De impact van Bring Your Own in: *TIEM 2.0, 45.* (juli 2012).



**Ir. C.L. (Chris) Wauters RE** is senior adviseur/auditor en als sectormanager lid van het managementteam van PBLQ HEC. Dit artikel is een bewerking van een artikel dat wordt gepubliceerd in TIEM 2.0, nr. 46.