HANDREIKING

CLOUD COMPUTING

TASKFORCE

Bestuur & Informatieveiligheid Dienstverlening

INHOUDSOPGAVE

DEZE HANDREIKING CLOUD COMPUTING VOOR MEDEOVERHEDEN WORDT U AANGEBODEN DOOR:

Erik Jungerius, directeur bedrijfsvoering, provincie Overijssel
Maarten Schurink, gemeentesecretaris, gemeente Utrecht
Paul Spaan, directeur bedrijfsvoering, waterschap Vallei en Veluwe

VOORWOORD

Oktober 2014

Bestuurders en topmanagers van de verschillende overheidslagen, koepelorganisaties en bij informatieveiligheid betrokken gremia hebben de afgelopen twee jaar samen met de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) samengewerkt om de sturing op en de verankering van informatieveiligheid binnen de overheid verder te brengen. Dit initiatief hebben wij als trekkers van deze handreiking vanuit onze respectievelijke overheidsposities met betrokkenheid en enthousiasme gevolgd.

Het op orde brengen van informatieveiligheid vraagt een blijvende inspanning. Net zolang tot we kunnen zeggen dat het onderwerp business as usual is geworden. Als dat natuurlijk al zou kunnen, want er is geen wereld die zich zo snel ontwikkelt als het digitale landschap. Ontwikkelingen als Big Data, Open Data, Cloud Computing, Smart Cities en zo meer, vragen op continue basis om handelingsperspectieven. Perspectieven die ons helpen als overheid niet alleen slim, maar ook alert te zijn… en te blijven. Cloud Computing is een mooi voorbeeld van een onderwerp, waarbij in het licht van informatieveiligheid de behoefte is gegroeid om een gezamenlijk handelingsperspectief te ontwikkelen. Daarbij speelt ongetwijfeld mee dat het gebruik van Cloud Computing inmiddels een ontwikkeling is die in rap tempo ons dagelijks leven binnentreedt (denk aan: streaming van film en muziekdiensten via Netflix en Spotify). In veel overheidsorganisaties wordt bewust, maar vaak ook minder bewust, via derde partijen, dagelijks gebruik gemaakt van Cloud-diensten (denk aan Dropbox). Waarbij de kennis van (veiligheids)risico's niet altijd voldoende aanwezig is.

In de voorliggende handreiking is een aanzet gedaan voor enkele concrete handvatten om de kennis- en gedachtenvorming aangaande het gebruik van Cloud-diensten in het licht van informatieveiligheid verder aan te scherpen. Gebaseerd op de kennis van vandaag en derhalve blijvend in ontwikkeling. Laten we die ontwikkeling vanuit bestuurlijk en ambtelijk perspectief blijven volgen en ook zelf prikkelen, te beginnen door het benutten en verder verspreiden van deze handreiking.

Erik Jungerius, Maarten Schurink en Paul Spaan

ACHTERGROND EN DOEL VAN DE HANDREIKING

Deze handreiking heeft als thema ‘Cloud Computing’. De handreiking is bedoeld voor bestuurders en topmanagers van medeoverheden die de kansen en mogelijkheden die Cloud Computing biedt, willen verkennen en beter willen toepassen. Het is een handreiking voortgekomen uit de concrete behoefte van bestuurders om meer zicht te krijgen op het onderwerp Cloud Computing en de sturing daarop te verbeteren.[1]

? WAAROM?

Cloud Computing is een complex onderwerp, met een diversiteit aan facetten die afhankelijk van de toepassing positief, maar ook negatief kunnen uitwerken. Bovendien kent deze technologie een aantal risico’s waar over de jaren heen nog geen of beperkte mitigerende maatregelen voor zijn bedacht. De risico’s liggen onder meer op het terrein van informatieveiligheid en privacy, welke garanties kunnen bijvoorbeeld op dat vlak afgegeven worden als niet bekend is waar de data staan in de Cloud van de leverancier en wie – naast de eigenaar van de dataset - nog meer onbevoegd bij de data kunnen.

! WAT BIEDT DEZE HANDREIKING U CONCREET?

Deze handreiking voor medeoverheden is een toepasbare ‘wegwijzer’ rondom de toepassing van Cloud Computing met daarbij verwijzingen naar de relevante beleidskaders, normenkaders en huidige richtlijnen waar overheden mee te maken hebben.[2] De handreiking biedt u bovendien een handzaam kader voor gedachtevorming en tot slot een lijst met afwegingen voor een veilige en verantwoorde toepassing van Cloud Computing.

De handreiking is nadrukkelijk *niet* bedoeld als toetsingskader dan wel vervanging van bestaand beleid en strategieën. Het biedt, ook voor overheden die al verder zijn in deze ontwikkeling, wel een kader dat de dialoog over Cloud bevordert.

Niet onbelangrijk; deze handreiking biedt een eerste, niet uitputtend, overzicht gebaseerd op de huidige stand van zaken en beschikbare kennis en documentatie. Cloud Computing ontwikkelt zich snel, net als (de discussie over) de toepassing ervan, en dient dus op regelmatige basis herijkt te worden.

De Europese Commissie/DG Connect heeft een onderzoek gedaan naar de toepassing van Cloud Computing bij verschillende overheden binnen de Europese Unie. Uit dit onderzoek blijkt dat veel verschillende keuzes zijn te maken als het gaat om het toepassen van Cloud Computing binnen de overheid, ieder met eigen voor- en nadelen.[3] Dit bevestigt dat een eenduidig antwoord voor het gebruik van Cloud Computing binnen de overheid vooralsnog niet mogelijk is. DG Connect werkt onder meer samen met overheden en private partijen, aan een Code of Conduct met als doel de markt van Cloud Computing meer open en transparant te maken.

1 De Actie-Agenda Informatieveiligheid is op initiatief van de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) in februari 2014 opgesteld in samenwerking met ruim 50 bestuurders en topmanagers uit overheid en bedrijfsleven.
2 Het Rijk baseert haar huidige beleid en uitvoering ten aanzien van Cloud Computing op de Rijkscloudstrategie (www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing/kamerbrief-over-cloud-computing.pdf) en de i-Strategie (www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/11/15/kamerbrief-informatiseringstrategie-rijk/kamerbrief-informatiseringstrategie-rijk.pdf).
3 Cloud for the public sector Study Report (European Commission, 2013).

SAMENVATTING

Deze handreiking is een voor medeoverheden toepasbare ‘wegwijzer’ rondom de toepassing van Cloud Computing, met daarbij verwijzingen naar de relevante beleidskaders, normenkaders en huidige richtlijnen waar overheden mee te maken hebben. Het biedt ook een semantisch denkkader om hierover het gesprek aan te gaan. De handreiking is nadrukkelijk niet bedoeld als toetsingskader dan wel vervanging van bestaand beleid en strategieën.

Cloud Computing is het (veelal) via het internet op aanvraag gebruik kunnen maken van hardware, software en gegevens. Cloud Computing zorgt ervoor dat gewenste dienstverlening of gegevens plaatsonafhankelijk, snel en gemakkelijk beschikbaar zijn.

- ✔ Het verschuiven van grote investeringen naar ‘huren op maat’ en ‘besparen op onderhoudskosten’.
- ✔ Het overal en altijd eenvoudig en zelfstandig kunnen aanvragen van ICT-diensten.
- ✔ Het eenvoudig, snel en flexibel opschalen, dan wel afbouwen van ICT-diensten.
- ✔ De mogelijkheid tot het delen van opslag- en rekencapaciteit met andere interne) gebruikers van de Cloud Computing.

Cloud Computing kent verschillende verschijningsvormen:

- ✔ De Publieke Cloud: dit zijn generieke Cloud-producten die in principe door elke organisatie of elke persoon gratis of via betaling kunnen worden afgenomen.
- ✔ De Private Cloud: dit is een Cloud-infrastructuur die voor/door één organisatie wordt beheerd en die met name interessant is voor organisaties met een grote omvang.
- ✔ De Community Cloud: dit is een gemeenschappelijke Cloud-infrastructuur waar verschillende organisaties uit één branche en met dezelfde belangen de infrastructuur en de Cloud-diensten delen.
- ✔ De Hybride Cloud: afhankelijk van de Cloud-dienst kan gekozen worden voor een combinatie van bovenstaande Cloud-vormen. Hierdoor kunnen dus meer Cloud-vormen met elkaar verbonden worden binnen één organisatie.

Cloud Computing kent enkele specifieke risico's waardoor een overstap niet altijd vanzelfsprekend is. De keuze voor Cloud Computing vraagt per casus om een afweging op strategisch niveau. Lastig aspect bij deze afweging, is dat de voordelen van Cloud Computing in de meeste gevallen duidelijk en vaak kwantificeerbaar zijn in tijd en geld, terwijl de risico's veelal kwalitatief van aard zijn en derhalve aanzienlijk minder zichtbaar. Zo kent het een aantal specifieke risicokenmerken van technische, organisatorische en juridische aard. Cloud-leveranciers maken vaak gebruik van verschillende (gekoppelde) servers om de Cloud-diensten te kunnen leveren. Als afnemer heeft u daardoor mogelijk minder controle en kennis over waar 'de eigen gegevens' precies staan opgeslagen.

Hierbij is het wel van belang een onderscheid te maken tussen het inzetten van Cloud Computing binnen de eigen ICT-infrastructuur, binnen een volledig uitbestede traditionele ICT-infrastructuur (zoals deze door de 'reguliere ICT-leveranciers' wordt geleverd) en binnen een Cloud-gebaseerde ICT-infrastructuur (zoals deze door 'Cloud-leveranciers' wordt geleverd: Amazon, Google, Microsoft, et cetera.). Dat is mede bepalend voor de mate waarin het mogelijk is om controle en kennis te hebben over waar 'de eigen gegevens' precies staan opgeslagen. Daarbij wordt er in alle gevallen gevraagd om passende afspraken en waarborgen.

Samenwerking stelt overheden bovendien in staat om de regie op, controle over en de inkoop van de Cloud te bundelen. Deze bundeling zorgt tevens voor een sterkere positie ten opzichte van de leverancier(s). Bovendien bevordert samenwerking onder meer de uniformiteit van de infrastructuur en bij het gebruik van (beveiligings)standaarden en –normen voor Cloud Computing

Op welke zaken moet u nu letten en welke vragen dient u te stellen als u overweegt de Cloud te gebruiken?

1. Maatwerk

Is maatwerk noodzakelijk of kan mijn organisatie uit de voeten met de standaarddiensten die momenteel door Cloud-leveranciers worden aangeboden? Bent u op de hoogte van welke Cloud-diensten uw organisatie gebruikmaakt en waarvoor?

2. Integriteit en gegevens

Waar zitten voor de gegevens van uw organisatie de belangrijkste risico's ten aanzien van integriteit (onweerlegbaarheid)? En, welke afspraken kunt u maken met uw leverancier om deze te mitigeren?

3. Vertrouwelijkheid van gegevens

Hoe belangrijk is het dat de digitale gegevens van uw organisatie vertrouwelijk blijven en niet door onbevoegden kunnen worden ingezien? In hoeverre zijn hierover afspraken te maken met uw leverancier om deze risico's te mitigeren? Is het mogelijk met versleutelde gegevens te werken?

4. Privacy en land van vestiging leverancier

Uw organisatie moet rekening houden met de privacywetgeving. Weet u waar bij uw Cloud-aanbieder de gegevens opgeslagen staan (ook in het buitenland?) en wie tot die gegevens toegang heeft?

5. Compliancy leverancier

Weet u aan welke wet- en regelgeving, bijvoorbeeld met betrekking tot informatiebeveiliging, uw Cloud-leverancier voldoet? Welk beleid voert uw leverancier uit om veiligheidsrisico's in de Cloud, zoals lekken van informatie, te voorkomen en sluit dit aan bij de normen die voor uw organisatie gelden op het gebied van informatieveiligheid en/of specifiek beleid over het gebruik van Cloud Computing?

6. Continuïteit dienstverlening

Hoe belangrijk is het dat de gegevens van uw organisatie bewaard blijven en hoe erg is het wanneer deze verloren gaan? Is er een uitwijkregeling mogelijk en hoe lang duurt herstel?

7. Controle en zeggenschap over uw gegevens

Weet u zeker dat de gegevens van uw organisatie ook uw gegevens blijven? Of mag uw Cloud-leverancier uw gegevens gebruiken voor andere doeleinden zonder toestemming van uw organisatie?

8. Beschikbaarheid gegevens en dienstverlening

Is 100% beschikbaarheid van uw gegevens altijd gewenst? Wanneer heeft uw organisatie de gegevens nodig en wanneer niet?

9. Overstappen van leverancier

Wilt uw organisatie ooit van Cloud-leverancier kunnen wisselen? En heeft u hiervoor ook de waarborgen, bijvoorbeeld met betrekking tot het migreren van datasets, contractueel geregeld die nodig zijn om over te kunnen overstappen? En heeft u daarvan de kosten in beeld?

Ongeacht de vorm van Cloud Computing, is het belangrijk dat u met leveranciers afspraken maakt om de voordelen van Cloud-oplossingen ook echt te kunnen benutten. Een eerste inventarisatie laat zien dat hierbij de volgende vier stuurvragen relevant zijn:

1. **Hoe realiseren we de potentiële voordelen van de Cloud? (schaalbaarheid, flexibiliteit, kostenbesparing, et cetera)**
2. **Hoe borgen we de informatiebeveiliging en privacy in de Cloud?**
3. **Hoe ziet onze exit-strategie eruit, voor als we om welke reden dan ook het contract willen beëindigen en/of de leverancier niet meer kan leveren?**
4. **Hoe kunnen we ons het best verantwoorden over het gebruik van de Cloud?**

Deze vragen zijn in deze handreiking verder uitgewerkt, om met uw eigen organisatie en leveranciers van Cloud-diensten het gesprek aan te kunnen gaan. Dit naast de reguliere vragen, die van toepassing zijn bij het uitbesteden van ICT-diensten, zoals personele en organisatorische consequenties, integratie met bestaande ICT-dienstverlening, et cetera.

CLOUD COMPUTING, WAT IS HET EIGENLIJK?

Cloud Computing, is het (veelal) via het internet op aanvraag gebruik kunnen maken van hardware, software en gegevens.[1] Cloud Computing zorgt ervoor dat gewenste dienstverlening of gegevens plaats onafhankelijk, snel en gemakkelijk beschikbaar zijn. Dit met weinig inspanning van de organisatie zelf en middels geringe interactie met de leverancier. Met behulp van de Cloud Computing kunt u als privépersoon en ook als organisatie snel en gemakkelijk gebruikmaken van bijvoorbeeld e-mail, opslagcapaciteit, diverse softwarepakketten en diverse vormen van dienstverlening.

@ CLOUD COMPUTING, EEN VORM VAN ICT-DIENSTVERLENING?

Een eerste rondvraag laat zien dat bestuurders en topmanagers Cloud Computing vooral aantrekkelijk vinden, omdat het u als overheidsorganisatie lijkt te ontzorgen en te vrijwaren van ICT-taken en -bemensing. Cloud Computing is daarmee vanuit het perspectief van bestuurders en topmanagers vaak onderdeel van een efficiency en van een (out)sourcings-vraagstuk. Het is vanuit dit perspectief onderdeel van de vraag 'of de organisatie de levering en het beheer van ICT-diensten bij externe partijen kan beleggen?'. En in het verlengde van deze vraag, 'op welke manier Cloud Computing hierbij een oplossing kan bieden?'. Het gaat in deze handreiking specifiek om deze laatste vraag te helpen beantwoorden, waarbij de keuze voor Cloud Computing niet vanuit een technisch oogpunt wordt benaderd, maar vooral als een vorm van ICT-dienstverlening met specifieke voor- en nadelen. Daarmee is het meer dan een 'plat' (out)sourcings-vraagstuk.

Hierbij is het wel van belang een onderscheid te maken tussen het inzetten van Cloud Computing binnen de eigen ICT-infrastructuur, binnen een volledig uitbestede traditionele ICT-infrastructuur (zoals deze door de 'reguliere ICT-leveranciers' wordt geleverd) en binnen een Cloud gebaseerde ICT-infrastructuur (zoals deze door 'Cloud-leveranciers' wordt geleverd, bijvoorbeeld Amazon, Google en Microsoft). Dat is mede bepalend voor de mate waarin het mogelijk is om controle en kennis te hebben over waar 'de eigen gegevens' precies staan opgeslagen. Daarbij wordt er in alle gevallen gevraagd om passende afspraken en waarborgen.

DE KARAKTERISTIEKEN VAN CLOUD COMPUTING

In positieve zin heeft Cloud Computing een aantal geheel eigen karakteristieken. Zo zijn door Cloud Computing ontsloten producten en diensten bijvoorbeeld vanuit iedere willekeurige locatie te benaderen door de gebruiker. Met behulp van Cloud Computing kunt u bovendien snel en eenvoudig toegang krijgen tot gegevens en systemen die u voor uw werk nodig heeft. Vaak zijn Cloud-applicaties benaderbaar via pc, tablet en mobiele apparatuur. Andere unieke karakteristieken van Cloud Computing zijn:

- ✔ Het verschuiven van grote investeringen naar 'huren op maat' en 'besparen op onderhoudskosten'. Dit wordt mede mogelijk vanwege het automatisch meten van het Cloud-gebruik, zodat de prijs per eenheid precies bekend is.
- ✔ Het overal en altijd eenvoudig en zelfstandig kunnen aanvragen van ICT-diensten.
- ✔ Het eenvoudig, snel en flexibel opschalen dan wel afbouwen van ICT-diensten.
- ✔ De mogelijkheid tot het delen van opslag- en rekencapaciteit met andere (interne) gebruikers van Cloud Computing.

DE RISICOKENMERKEN VAN DE CLOUD

Cloud Computing heeft ook een aantal specifieke risicokenmerken. Deze risico's zijn niet alleen technisch, maar ook organisatorisch en juridisch van aard. Immers, Cloud-leveranciers maken vaak gebruik van verschillende (gekoppelde) servers om de Cloud-diensten te kunnen leveren. Als afnemer heeft u daardoor minder controle en kennis over waar 'de eigen gegevens' precies staan opgeslagen. Wanneer u als overheidsorganisatie met gevoelige gegevens werkt, is controle hierover uiteraard van groot belang. Mocht u Cloud Computing overwegen, dan is het slim om per casus de risico's af te wegen. In hoofdstuk 3 worden alle risico's besproken en uitgebreid toegelicht.

BIJ CLOUD COMPUTING WORDEN IN HET ALGEMEEN DRIE 'LAGEN' OFWEL SERVICE-MODELLEN ONDERKEND:

Infrastructuur as a Service (IaaS): hierbij wordt de apparatuur van het eigen rekencentrum vervangen door een Cloud-oplossing. Er wordt opslagcapaciteit en rekenkracht naar behoefte afgenomen.

Platform as a Service (PaaS): dit model is een uitbreiding op IaaS. De gebruiker neemt een complete ICT-hardwareomgeving via de Cloud af. Hierin zijn ook elementen als een besturingssysteem, database, et cetera opgenomen. Applicatiesoftware maakt géén deel uit van PaaS.

Software as a Service (Saas): dit model is een uitbreiding op PaaS. Hierbij neemt de gebruiker ook de functionaliteiten van een applicatie af (lees: software), naast de ICT-apparatuur en het ICT-platform.

ONTWIKKELINGEN DIE HET GEBRUIK VAN CLOUD COMPUTING BEÏNVLOEDEN:

- **Naarmate Het Nieuwe Werken (plaats- en tijdonafhankelijk) meer gemeengoed gaat worden, zal de behoefte aan samenwerkingshulpmiddelen toenemen. Deze tools worden vaak aangeboden als een Cloud-dienst.**
- **Veel leveranciers van software gaan over van het installeren van software bij de klant naar een Cloud-aanbieding, een zogenaamde Software as a Service/ SaaS-oplossing.**
- **Er wordt door overheden veelvuldig in ketens samengewerkt met zowel publieke als private partijen die van Cloud Computing gebruik kunnen maken. De gegevens die met deze organisaties worden uitgewisseld, verplaatsen op deze manier, wanneer daar geen afspraken over worden gemaakt, 'als vanzelf' naar de Cloud.**

CLOUD COMPUTING KENT VERSCHILLENDE VERSCHIJNINGSVORMEN:

- **De Publieke Cloud:** dit zijn generieke Cloud-diensten die in principe door elke organisatie of persoon gratis of via betaling kunnen worden afgenomen.
- **De Private Cloud:** dit is een Cloud-dienst die voor/door één organisatie wordt beheerd en die met name interessant is voor organisaties met een grote omvang.
- **De Community Cloud:** dit is een gemeenschappelijke Cloud-dienst waar verschillende organisaties uit één branche en met dezelfde belangen de infrastructuur en de Cloud-diensten delen.
- **De Hybride Cloud:** afhankelijk van de Cloud-dienst kan gekozen worden voor een combinatie van bovenstaande Cloud-vormen. Hierdoor kunnen dus meer Cloud-vormen met elkaar verbonden worden binnen één organisatie.

In hoofdstuk 3 gaan we – vanuit het perspectief van de overheid - dieper in op de voor- en nadelen van bovenstaande verschijningsvormen.

1 In het geval van de Rijkscloud is toegang mogelijk via Rijksoverheidsnetwerk (RON2.0).

DE VOOR- EN NADELEN VAN CLOUD COMPUTING

De voor-en nadelen van Cloud Computing leggen we u uit aan de hand van een drietal perspectieven:

A WAT IS HET VERSCHIL TUSSEN CLOUD COMPUTING EN MEER TRADITIONELE VORMEN VAN UITBESTEDING?

Tussen uitbesteding op basis van Cloud Computing en uitbesteding op basis van meer traditionele vormen zit in de kern eigenlijk weinig verschil als het gaat om de voor- en nadelen voor uw organisatie. Ontzorging, kostenbesparing, meer efficiency en flexibiliteit zijn vier van de belangrijkste voordelen waarom organisaties vaak denken aan uitbesteding. Bovendien kan een voordeel zijn dat u zo als organisatie expertise in huis haalt, al dan niet gekoppeld aan mensen (beschikbaarheid), waarover u in uw eigen organisatie niet beschikt of kunt beschikken.
Hebben we het over de nadelen, dan gaat het bij uitbesteding vooral om:

- ✔ De grotere afhankelijkheid van uw organisatie van (het functioneren van) de leverancier (beheer en beheersing).
- ✔ De gevolgen voor ICT-personeel binnen uw eigen organisatie (HRM).
- ✔ De consequenties in geval uw leverancier failliet gaat en het hierbij horende continuïteitsvraagstuk (dienstverlening).
- ✔ De vraag hoe u uw verantwoordelijkheid over de uitbestede gegevens succesvol handen en voeten geeft.

Voor reguliere ICT-outsourcing geldt net zo goed als voor uitbesteding middels Cloud Computing, dat het risico dat vertrouwelijke informatie kan worden gelekt altijd aanwezig is. Een verschil tussen beide is er overigens ook. In geval van Cloud Computing beoordeelt u in principe of de dienst die wordt geleverd voldoet aan uw eisen, terwijl bij reguliere ICT-uitbestedingen de leverancier gevraagd wordt om, vaak op maat, te leveren naar de wensen van uw organisatie.

B WAT ZIJN DE SPECIFIEKE RISICO'S VAN CLOUD COMPUTING?

Dit neemt niet weg dat de Cloud Computing ook enkele specifieke risico's heeft waardoor een overstap niet altijd vanzelfsprekend is. De keuze voor Cloud Computing vraagt per casus om een afweging op strategisch niveau. Lastig aspect bij deze afweging is, dat de voordelen van Cloud Computing in de meeste gevallen duidelijk en vaak kwantificeerbaar zijn in tijd en geld. Terwijl de risico's veelal kwalitatief van aard zijn en derhalve aanzienlijk minder zichtbaar.

Reden te meer om de risico's voor u onder elkaar te zetten, zodat u in uw afweging 'Wel/Geen Cloud Computing', per casus kunt bekijken hoe de balans voor u doorslaat:

1. Maatwerk

Wilt u een specifieke dienst die perfect aansluit bij uw organisatie? Dan is dit met Cloud Computing lastig te bereiken, althans in de traditionele 'besproken' vorm. Het van grond af aan bouwen van een eigen private Cloud aan de hand van voorbesproken wensen en eisen is relatief kostbaar. Terwijl juist lagere kosten ook een potentieel voordeel is van Cloud Computing.

Een tussenvorm die veel voorkomt is het afstemmen van bestaande Cloud-oplossingen op de wensen van uw organisatie. Cloud Computing is over het algemeen modulair opgebouwd. Binnen de modules zijn aanpassingen mogelijk, maar ook hier zijn extra kosten aan verbonden.

Momenteel geldt dat veel commerciële Cloud-oplossingen als standaarddiensten worden aangeboden en ontwikkeld zijn voor een groot aantal klanten. Het is hierbij vaak niet of beperkt mogelijk om specifieke aanpassingen te doen. De Cloud-aanbieder bepaalt in deze gevallen hoe het product of de dienst eruit ziet en het is aan u om te kijken of dit is wat voor u bruikbaar is.

2. Integriteit

Stel u zelf de vraag hoe belangrijk het is dat de digitale gegevens van uw organisatie onveranderd blijven. En dat u erop kunt vertrouwen dat wat uw organisatie schrijft, uitgeeft of doorgeeft ook correct is. Waar zitten voor uw gegevens de belangrijkste risico's? En, welke afspraken kunt u maken met uw leverancier om deze te mitigeren?

3. Vertrouwelijkheid

Hoe belangrijk is het dat de (categorieën van) digitale gegevens van uw organisatie vertrouwelijk blijven en niet door onbevoegden kunnen worden ingezien? In hoeverre zijn hierover afspraken te maken met uw leverancier om deze risico's te mitigeren? Is het mogelijk met versleutelde gegevens te werken?

4. Privacy en land van vestiging

Moet uw organisatie rekening houden met privacywetgeving? Buitenlandse overheden kunnen zich toegang verschaffen als de Cloud-leverancier in hun land op enige manier actief is. Bij veel Cloud-aanbieders is het niet altijd duidelijk waar de gegevens opgeslagen staan en wie tot die gegevens toegang heeft. Dit neemt niet weg dat sommige Cloud-leveranciers wel garanties kunnen bieden omtrent de opslaglocatie van de data. Kortom, onderzoek dit grondig en kijk of uw leverancier een dienst aanbiedt die voldoet en blijft voldoen aan de geldende privacywetgeving. Behalve Nederlandse wetgeving zijn in ieder geval de Patriot Act en Foreign Intelligence Surveillance Act (FISA) hierbij relevant.

5. Compliancy

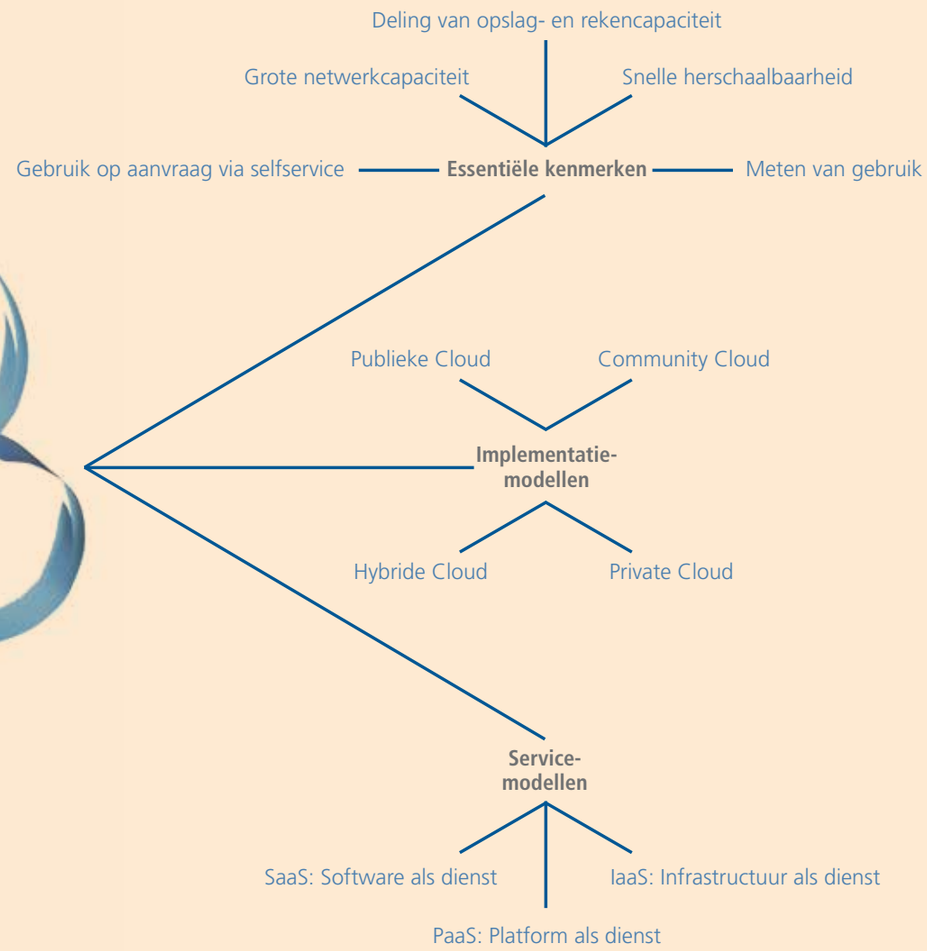
Stel u zelf de vraag aan welke wet- en regelgeving en gangbare informatiebeveiligingsnormen uw Cloud-leverancier voldoet (ISO 27001, PCI, HIPAA). Geef daarbij specifieke aandacht aan het informatieveiligheidsbeleid van uw Cloud-leverancier. Welke beleid voert uw leverancier uit om veiligheidsrisico's in de Cloud, zoals lekken van informatie, te voorkomen? Sluit dit beleid aan bij de normen die voor uw organisatie gelden op het gebied van informatiebeveiliging (baselines per overheidslaag) en/of specifiek beleid over het gebruik van Cloud Computing in uw overheidslaag?

6. Continuïteit

Hoe belangrijk is het dat de gegevens van uw organisatie bewaard blijven en hoe erg is het wanneer deze verloren gaan? Is er een uitwijkregeling mogelijk? Of is er de optie van een onafhankelijke derde partij die een back-up beheert?

SERVICE DELIVERY EN CLOUD-VORM

Cloud Computing
is het (veelal) via het internet op aanvraag gebruik kunnen maken van hardware, software en gegevens.



Dit figuur is afkomstig uit het document 'Gesloten Rijkscloud. Functionele doelarchitectuur' (2013).

7. Controle en zeggenschap over uw gegevens

Weet u zeker dat wat van uw organisatie is, ook in de Cloud van uw organisatie blijft? De gegevens van uw organisatie moeten ook uw gegevens blijven. Uw Cloud-leverancier mag uw gegevens uiteraard niet gebruiken zonder toestemming van uw organisatie.

8. Beschikbaarheid

Wanneer een calamiteit zich voordoet, heeft uw organisatie het systeem en de gegevens direct nodig of mag er een bepaalde (recover)tijd overheen gaan? Aan 100% beschikbaarheid hangt een prijskaartje. Voor sommige processen en systemen van uw organisatie kan het overigens noodzakelijk zijn in verband met calamiteiten om 100% beschikbaarheid te hebben.

9. Overstappen

Wilt uw organisatie ooit van Cloud-leverancier kunnen wisselen? Realiseert u zich dan dat overstappen kosten met zich meebrengt, maar ook dat uw organisatie wellicht moet bewijzen dat geëxporteerde gegevens juist zijn (gewaarmerkte kopie of back-up). Overigens, en niet onbelangrijk, er zijn geen standaarden die volledige interoperabiliteit garanderen.

C WAT ZIJN DE SPECIFIEKE VORMEN VAN CLOUD COMPUTING?

Uw organisatie heeft uiteraard altijd de verantwoordelijkheid om per casus een zorgvuldige en eigen afweging te maken aangaande de voor- en nadelen van Cloud Computing. Op hoofdlijnen is per Cloud-vorm echter wel een richting aan te geven wat betreft de afweging tussen voor- en nadelen. Het land van vestiging en privacy, continuïteit en informatieveiligheid spelen hierbij een belangrijke rol.

Geen Cloud

Als uw gegevens dermate vertrouwelijk zijn en dat u ten koste van alles wilt voorkomen dat u afhankelijk bent van een derde partij, kunt u beter niet de overstap naar Cloud Computing maken. Ook wanneer u wilt voorkomen dat de continuïteit van uw ICT-diensten afhankelijk raakt van derden, is gebruik van Cloud Computing af te raden. Waarschijnlijk maakt u dan eenzelfde keuze ten aanzien van eventuele outsourcing van ICT-diensten.

Houd er echter wel rekening mee dat de keerzijde van het niet gebruiken van Cloud Computing veel van uw eigen organisatie vraagt in termen van capaciteit, financiën, personeel, et cetera. Zo kan er toch een positieve business case ontstaan om Cloud Computing in te zetten binnen de bestaande infrastructuur (van de eigen organisatie of van een reguliere ICT-leverancier) op te nemen, mits voorzien van de juiste afspraken en veiligheidswaarborgen.

Private Cloud

Als uw organisatie 'in control' wil blijven over de gegevens en de onderliggende informatietechnologie, dan is het een overweging om te kiezen voor een eigen Cloud, de zogenaamde Private Cloud. Doordat de Private Cloud uitsluitend door één organisatie wordt gebruikt, kan er relatief veel controle over uitgeoefend worden. Een Private Cloud kan in eigendom en beheer zijn van de eigen organisatie, een derde partij of een combinatie hiervan. Het opzetten van een Private Cloud, mogelijk met behulp van een externe leverancier, vergt overigens wel expertise binnen de eigen organisatie. Het vraagt onder meer specifieke kennis om de juiste wensen te formuleren en waarborgen te realiseren, zodat u ook echt de dienst geleverd krijgt die u wilt. Realiseert u zich dat behalve de kosten die verbonden zijn aan het binnenshuis halen en behouden van deze kennis, ook de kosten voor beschikbaarheid en continuïteit uitsluitend door de eigen organisatie worden gedragen. Daar staat uiteraard tegenover het voordeel dat u precies de vestigingslocatie van de hardware weet waar uw gegevens op staan.

Community Cloud

De Community Cloud is feitelijk de Private Cloud voor een groep gelijkgestemden (lees: meer dan één organisatie). De zogenaamde Community Cloud, waaraan diverse organisaties (al dan niet vooraf georganiseerd) deelnemen, biedt de mogelijkheid om makkelijk op te schalen naar meer participanten. De kosten per gebruikseenheid worden daardoor voor elke deelnemer steeds kleiner. Uiteraard mits hierover de juiste afspraken zijn gemaakt en waarborgen zijn gerealiseerd. Organiseer bijvoorbeeld een Community van overheden om zo samen met gelijkgestemden een Community Cloud op te zetten. Met aanvullende afspraken

en investeringen is het mogelijk om aan te wijzen welke hardware door welke gebruiker van de Community Cloud wordt gebruikt. Het is natuurlijk hoe dan ook mogelijk om gezamenlijk de voor de Community gebruikte set van hardware aan te wijzen en daarmee ook waar de gegevens staan. Houd er wel rekening mee dat het organiseren van gezamenlijk opdrachtgeverschap zeker niet makkelijk is. In hoofdstuk 4 zal nader worden ingegaan op het onderwerp 'Samenwerken als overheid'.

Public Cloud

Bij de Public Cloud is de door uw organisatie gebruikte hardware niet aan te wijzen. U weet niet precies waar uw gegevens opgeslagen zijn. Bovendien kunnen de gegevens vrij stromen tussen landen, waarbij ze ingezien, hergebruikt en verwerkt kunnen worden door derde partijen. Daartegenover staat dat de diensten vaak gratis of heel goedkoop zijn. Als u zeker weet dat het hanteren van deze diensten niet tot extra risico's (denk aan: risico's voor de integriteit en beschikbaarheid van data) leidt, dan wel deze te mitigeren zijn, bijvoorbeeld door zelf data te versleutelen, kunt u gebruik maken van alle vormen van Cloud, zelfs ook de Public Cloud. Daarbij is het dan wel zaak om scherp te blijven op de gewenste waarborgen. Is er bijvoorbeeld een exit-strategie en is deze onderdeel is van de algemene voorwaarden? Of is deze niet relevant gezien de aard en vertrouwelijkheid van de gegevens?

Hybride Cloud

Uit het bovenstaande blijkt dat meerdere vormen van Cloud Computing bestaan. Een groot voordeel van Cloud Computing is, dat deze in de meeste gevallen gebaseerd is op internettechnologie. Met als voordeel dat alle Cloud-oplossingen, mits gebaseerd op open standaarden, aan elkaar gekoppeld kunnen worden. Dit noemen we hybride Cloud-oplossingen. Het nadeel van deze hybride Cloud is dat het de mogelijkheid creëert om een deur open te zetten van een Private Cloud naar bijvoorbeeld een Public Cloud. Dit kan vooral gevolgen hebben voor de privacy en informatieveiligheid van uw gegevens. Mogelijke koppelingen tussen verschillende Cloud-vormen vergen dus zeker uw aandacht.

SAMENWERKEN ALS OVERHEID

In dit hoofdstuk is aandacht voor het realiseren van samenwerking in het licht van Cloud Computing, zodat de voordelen ook echt ten gunste komen van overheden. Samenwerking stelt overheden bovendien in staat om de regie op, controle over en de inkoop van de Cloud te bundelen. Deze bundeling zorgt tevens voor een sterkere positie ten opzichte van de leverancier(s). Bovendien bevordert samenwerking onder meer de uniformiteit van de infrastructuur en bij het gebruik van (beveiligings)standaarden en –normen voor Cloud Computing.

Het samenwerken door overheden kan concreet invulling krijgen middels een zogenaamde Cloud Broker. In de functie van Cloud Broker zijn alle kennis en kunde van de deelnemende overheden, zowel over informatieveiligheid en privacy als aangaande het aanbesteden, verzameld. De Cloud Broker is een intermediair tussen de vraag van betrokken overheden en het aanbod van Cloud-leveranciers. In de onderhandelingen met de ICT-leveranciers kan de Cloud Broker door een sterkere onderhandelings- en kennispositie, ervoor zorgen dat de voordelen van de Cloud makkelijker worden gerealiseerd voor overheden. De functie van Cloud Broker kan zowel door een publieke als een private organisatie ingevuld worden. De Cloud Broker helpt overheden om de voordelen van de Cloud ook echt uit te nutten en tegelijkertijd te voldoen aan alle geldende normen en kaders. Dit leidt tot ontzorging van de betrokken overheden. Ook bevordert deze manier van werken het optreden als één overheid. In de praktijk kan deze functie van Cloud Broker ook ingevuld worden door bijvoorbeeld een Shared Service Organisatie (SSO), maar ook een ICT-consultancy organisatie kan deze rol op zich nemen.[1] Overigens is het belangrijk om hier nogmaals te benoemen dat ook voor de Community Cloud niet alle risico's gemitigeerd worden. Ook bij het gebruik van de Community Cloud blijft het risico bestaan dat de continuïteit verstoord wordt, of dat bijvoorbeeld gegevens gelekt worden.

In 2011 heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) een Cloud-strategie gelanceerd die in eerste instantie betrekking had op de Rijksoverheid en tevens kaders biedt voor andere overheden.[2]
De Rijksoverheid werkt momenteel aan de realisatie van haar Rijkscloud. De Rijkscloud wordt door de Rijksoverheid zelf ingericht. Zij voert de regie en beheer en reguleert de toegang tot de Rijkscloud en de gegevens daarin. Vanuit de Rijkscloud kunnen door Rijksoverheden diensten als gegevensopslag, servercapaciteit, infrastructuurcapaciteit en gebruiksdiensten, zoals e-mail, werkplekomgeving, samenwerkingsfunctionaliteit en specifieke applicaties worden betrokken.

€ RUIMTE VOOR DE MARKT

Een keuze voor samenwerking met een Cloud-leverancier laat vrij wie de realisatie en het beheer van de Cloud het meest optimaal kan uitvoeren. In het algemeen geldt dat, als de markt kan leveren, dit ook aan de markt wordt gelaten. Voor Cloud Computing gaat dit eveneens op. Op Europees niveau wordt in dialoog met de markt verkend hoe in de behoeften van de overheden kan worden voorzien. Met als voorwaarde dat u als overheidsorganisatie de strakke regie houdt over het geheel en daarmee invulling geeft aan uw eindverantwoordelijkheid.

In Nederland bestaan diverse samenwerkingsverbanden die Cloud-dienstverlening aanbieden of dat aan het voorbereiden zijn. Denk aan: Servicepunt71 (SSO voor gemeenten), Dimpact (samenwerkingsverband van gemeenten), Equalit (SSO in het zuiden des lands) en de RUD Zeeland, die een eigen Cloud-platform heeft ingericht op de Wet Algemene Bepalingen Omgevingsrecht (WA BO)-taken voor gemeenten, waterschappen en provincies.

1 Zie ook: www.pianoo.nl/sites/default/files/documents/documents/vnghandreikingkingcloudcomputing-ssclowres.pdf.
2 Zie: https://www.forumstandaardisatie.nl/sites/default/files/FS/2014/1028/kamerbrief-over-cloud-computing.pdf

BELANGRIJKE WAARBORGEN EN AFSPRAKEN MET LEVERANCIERS

Ongeacht de vorm van Cloud Computing, is het belangrijk dat u met leveranciers afspraken maakt om de voordelen van Cloud-oplossingen ook echt te kunnen benutten. Om u hierbij te helpen bevat dit hoofdstuk een eerste overzicht met belangrijke waarborgen[1] en afspraken. Dit overzicht is niet uitputtend en kan vanzelfsprekend op basis van nieuwe inzichten aangepast worden. Voor nu is het doel om u een handzaam hulpmiddel te bieden.

+ REALISATIE VAN DE VOORDELEN VAN CLOUD COMPUTING

1. Eis het gebruik van open standaarden	Gebruik van open standaarden is belangrijk om de diverse vormen van Cloud Computing onderling te kunnen laten interacteren en vooral met de bestaande ICT-infrastructuur en interface van uw eigen organisatie.[2]
2. Maak afspraken over de verwerkings-capaciteit	De schaalbaarheid van de verwerkingscapaciteit moet worden gewaarborgd door afspraken vast te leggen aangaande de kosten, het tijdbestek en de omvang van het opschalen.
3. Maak afspraken over het aantal gebruikers en autorisaties	De schaalbaarheid in termen van aantal gebruikers kan gewaarborgd worden door afspraken te maken met de leverancier over de betaling van een 'flat-rate' tot een x-aantal gebruikers.
4. Maak afspraken over toegang tot de eigen gegevens	Maak afspraken met de leverancier over toegang tot uw gegevens. Dit betreft niet alleen de opgeslagen gegevens, maar ook de zogenaamde *current state* of *transactions*.
5. Maak afspraken over transparantie aangaande door-ontwikkelingen	Het is belangrijk om afspraken te maken met de leverancier(s) die transparantie aangaande doorontwikkeling van Cloud Computing bevorderen. Dit mede omdat uw bedrijfsprocessen aangepast kunnen zijn op een specifieke versie van Cloud Computing.

BORGEN VAN PRIVACY EN INFORMATIEVEILIGHEID BIJ CLOUD COMPUTING

1. Maak afspraken aangaande de locatie van opslag van gegevens en privacybescherming	Overheidsorganisaties zijn verantwoordelijk voor de bescherming van gegevens. Hiervoor moeten zij voldoen aan wet- en regelgeving. De leverancier dient hier ook aan te voldoen en dient hier ook op aangesproken te worden.
2. Maak afspraken over het omgaan met kwetsbaarheden en 'lekken'	Het is belangrijk om afspraken te maken over het melden van (nieuwe) kwetsbaarheden en een eventueel lek. Vergeet hierbij ook niet om afspraken te maken over de wijze waarop de eigen organisatie hierover, geïnformeerd wilt worden.
3. Maak afspraken over verstoringen van de dienstverlening	Maak voor 'worstcasescenario's' (vernietiging datacenter e.d.) afspraken met de leverancier. Het gaat hier vooral over procesafspraken, waaruit duidelijk blijkt op welke manier en door wie geëscaleerd kan worden.

BEPALEN VAN EEN EXIT-STRATEGIE

1. Houd zeggenschap over de eigen gegevens	Het is wenselijk om contractueel vast te leggen dat uw gegevens bij beëindiging van de dienstverlening direct tot uw beschikking komen en ook hoe dit gebeurt. Immers, om uw gegevens over te kunnen zetten naar een nieuwe Cloud Computing of een ander systeem, dienen de gegevens aangeboden te worden in een open format dat leesbaar en bruikbaar is voor uw organisatie.
2. Zorg voor een volledige overdracht	Er mogen natuurlijk geen gegevens achterblijven in de Cloud nadat de dienstverlening is stopgezet. Hiervan dient adequaat bewijs geleverd te worden aan u als opdrachtgevende organisatie. Ook dit dient bij de start van de dienstverlening contractueel vastgelegd te worden.
3. Laat fall-back scenario's ontwikkelen	Na het beëindigen van het contract met uw Cloud-leverancier, moet uw organisatie de afgenomen ICT-diensten zelf leveren. Door voorbereid te zijn op een eventuele 'exit' kan uw organisatie de consequenties makkelijker opvangen.

VERANTWOORDEN OVER HET GEBRUIK VAN CLOUD COMPUTING

1. Richt een monitor in	De prestaties van Cloud-diensten en het waarborgen van de afspraken kunnen in beeld gebracht worden door een monitor in te richten die aansluit bij de gemaakte afspraken vastgelegd in een Service Level Agreement (SLA).
2. Maak afspraken over inhoud en frequentie van de rapportage	In de rapportages zijn de gegevens over het functioneren van de Cloud Computing geaggregeerd, waardoor de prestaties beter zijn te vergelijken met afspraken die in de SLA zijn vastgelegd. Tip is om ook met uw leverancier af te spreken dat deze proactief rapporteert over dreigingsbeelden en de hiertegen genomen maatregelen.
3. Waarborg de mogelijkheid voor (externe) audits	De beheerder van de Cloud Computing moet net als uw eigen organisatie verantwoording afleggen over de veiligheid van de Cloud Computing. Houd hier rekening mee bij de inrichting van de Cloud door duidelijke en concrete afspraken te maken over de auditing van producten en diensten.
4. Neem functioneren van Cloud Computing op in reguliere verantwoording	Het verantwoorden over het functioneren van de Cloud Computing kan door dit te integreren in de reguliere verantwoording over ICT. Het helpt daarbij om de Cloud expliciet op te nemen in de verantwoording, met een onderbouwing van de gerealiseerde voordelen en de bestaande risico's. Daarnaast is het wenselijk om het voldoen aan privacywetgeving en de eisen omtrent de opslag van gegevens extra toe te lichten in deze verantwoording.

1 Daarbij is nog wel de vraag welke waarborgen er worden getroffen, voor het geval dat de Cloud-leverancier zijn verplichtingen niet meer na kan komen. Welke rol kunnen andere leveranciers daar mogelijk in spelen?
2 Open standaarden betekent echter niet per definitie dat interactie met een andere Cloud-vorm of uw eigen ICT-omgeving mogelijk is, maar het vormt wel de basis.

BIJLAGE: BRONNEN HANDREIKING CLOUD COMPUTING

Titel	Link
The NIST Definition Of Cloud Computing	www.nist.gov/itl/cloud/index.cfm
Cloud Standards Coordination Final report (2013)	eurocloudnl.eu/wp-content/uploads/2013/12/ETSI-CSC-Deliverable-008-Final_Report-V1_0.pdf
Establishing Trusted Cloud in Europe	ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe
Cloud Service Level Agreement Standardisation Guidelines	ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
Zienswijze CBP over Cloud Computing	www.cbpweb.nl/Pages/med_20120910-zienswijze-cbp-cloudcomputing.aspx
Wet bescherming persoonsgegevens	wetten.overheid.nl/BWBR0011468/geldigheidsdatum_23-07-2014
CBP Richtsnoeren Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer augustus 2009 beveiliging van persoonsgegevens	www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
CIP Beveiligingsbeleid Cloud-diensten (4 april, 2014)	www.cip-overheid.nl/wp-content/uploads/2014/04/Beveiligingsbeleid-clouddiensten-CIP-DEF-v2_3-excl-ARD.pdf
Bewerkersovereenkomst: Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)	www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0218-bewerkersovereenkomst- v1.0.pdf.pagespeed.ce.qJrVrC1I4W.pdf

Titel	Link
Cloud Computing: Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)	www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1111-cloud-computing-gemeenten.pdf
White Paper NCSC 'Cloud Computing & Security'	www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloud-computing.html
ICT Beveiligingsrichtlijnen voor webapplicaties	www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
Internationale open standaarden voor een veilige Cloud	www.forumstandaardisatie.nl/uploads/RTEmagicC_Open_security_standards.png.png
Toe te passen open standaarden voor de Cloud, mits relevant qua functioneel en organisatorisch toepassingsgebied, volgens de Nederlandse 'Pas Toe Leg Uit-lijst'	www.forumstandaardisatie.nl/uploads/RTEmagicC_pas_toe_of_leg_uit_-lijst.jpg
Toe te passen open standaarden voor de Cloud volgens de Europese onderzoeken	www.forumstandaardisatie.nl/uploads/RTEmagicC_Presentatie1.jpg

INTERESSANTE BRONNEN VOOR DE MEESTE ACTUELE INFORMATIE OVER CLOUD COMPUTING ZIJN ONDER MEER:

Titel	Link
National Institute of Standards and Technology	www.nist.gov
Europese Commissie/ DG Connect	ec.europa.eu/dgs/connect/en/content/dg-connect
Europese Commissie/ Cloud for Europe	www.cloudforeurope.eu
CIP	www.cip-overheid.nl
NCSC	www.ncsc.nl
IBD	www.ibdgemeenten.nl

COLOFON

Deze handreiking is tot stand gekomen dankzij de inspanningen van:

DE LEDEN VAN DE KLANKBORDGROEP:

Ton van Bergeijk, Standardization Consultant normcommissie
NC 381038 'Cloud Computing', NEN
Frank van Dam, IT-architect, Ministerie van Economische Zaken
Rob van Dorsten, programmamanager, Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties (BZK)
Frans Hooft van Huysduynen, senior adviseur informatievoorziening,
Provincie Utrecht
Frank Kerkhoven, bestuurslid, VIAG
Marcel Koers, senior enterprise architect, CIP
Thomas Kruse, strategisch adviseur bedrijfsvoering, Gemeente Utrecht
Peter de Leeuw, programmamanager Architectuur en Standaarden,
Het Waterschapshuis
Peter Leijnse, senior architect, Logius
Andres Steijaert, programmamanager, Surfnet

DE AUTEURS:

Arjan de Jong, beleidsmedewerker, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Henri Rauch, strategisch adviseur, KING
Marijke Salters, senior adviseur, College en Forum Standaardisatie
Lancelot Schellevis, beleidsadviseur, College en Forum Standaardisatie

DE EINDREDACTEURS:

Sonja Kok, communicatieverantwoordelijke en woordvoerder, Taskforce BID
Douwe Leguit, manager, Taskforce BID
Eric Warners, beleidsadviseur, Taskforce BID
Henk Wesseling, bestuurlijk hoofd, Taskforce BID

Het Forum Standaardisatie is blij met het verschijnen van de Handreiking Cloud Computing voor bestuurders en topmanagers. Deze handreiking biedt een kader voor overheden om samen een handelingsperspectief te ontwikkelen voor het toepassen van Cloud Computing. Cloud-oplossingen hebben volgens ons de Toekomst, maar we zien tegelijk het risico dat er silo's ontstaan. Silo's die onderling geen informatie kunnen uitwisselen. Digitale samenwerking kan daarom ons inziens niet zonder het gebruik van open standaarden. Cloud-oplossingen zijn daarop geen uitzondering; ook hiervoor zijn open standaarden nodig. Het Forum Standaardisatie ziet de handreiking als extra stimulans om het gebruik van open standaarden voor Cloud-oplossingen te blijven bevorderen.

Nico Westpalm van Hoorn
Voorzitter Forum Standaardisatie

EEN HANDREIKING VOOR BESTUURDERS EN TOPMANAGERS VAN MEDEOVERHEDEN

BEZIEN VANUIT HET PERSPECTIEF VAN INFORMATIEVEILIGHEID

GERICHT OP ALLE WETENSWAARDIGHEDEN AANGAANDE CLOUD COMPUTING

TE BENUTTEN TIJDENS HET KEUZEPROCES

ÉN NA DE CLOUD-KEUZE, VOOR EEN VEILIGE EN VERANTWOORDE OMGANG MET CLOUD COMPUTING

www.taskforcebid.nl

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN