

[Checklisten]

1.F.21. Denken over cloud computing.

DOEL

Na doorlopen van deze checklist heeft u zeven aandachtspunten bij cloud computing voor uw organisatie op een rij gezet. Deze zeven aandachtspunten betreffen:

- Het soort cloud computing, waarvan u gebruik maakt;
- De wetgeving rond en standaardisatie aspecten bij cloud computing;
- De business case voor cloud computing;
- De implementatie van cloud computing;
- De sturing en organisatie bij het werken met cloudcomputing;
- De beeindiging van cloud computingdiensten en
- De impact van cloudcomputing op de organisatie.

TOEPASSINGSGEBIED

De checklist sluit aan bij de checklisten 1.C.20, De toekomstgerichtheid van onze ICT-voorzieningen, 1.C.21 en bij Corporate governance, government governance, IT governance, compliance en in-control. Voorts past de checklist bij 2.A.7, Inzicht in de informatieportfolio.

De checklist is van belang voor elke organisatie die de mogelijkheden en de impact van cloud computing eens globaal voor zijn organisatie wil onderzoeken.

AUTEURSGEGEVENS

Theo Thiadens is lector ICT-governance aan de Fontys Hogeschool in Eindhoven. Van zijn hand is onder meer het boek *Sturing en organisatie van ICT-voorzieningen* (2e druk, 2008) verschenen. Het boek kent een vertaling in het Engels (*ICT governance, management and organization*). Het boek verscheen in 2007 in het Chinees. Hij doceert op diverse universiteiten en bij verschillende leergangen vakken op het terrein van informatie- en ICT-management. Hieronder vallen onder meer de Open Universiteit, Avans plus, de Erasmus Universiteit, de Universiteit van Tilburg en de Rijksuniversiteit Groningen.

Theo Thiadens is lid van de architecture board van de BISL/ASL Foundation en lid van de redactiecommissie van het blad *Finance and Control*. Tot 1 september 2001 was hij werkzaam in diverse functies bij de Koninklijke Marine, Foxboro, IBM, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het Kadaster, de IB-Groep en de Politie. Hij is te bereiken via de website www.ict-management.com.

INLEIDING

Deze checklist zet eerst in het kort de theorie ten aanzien van cloud computing op een rij. Daarna volgt de checklist.

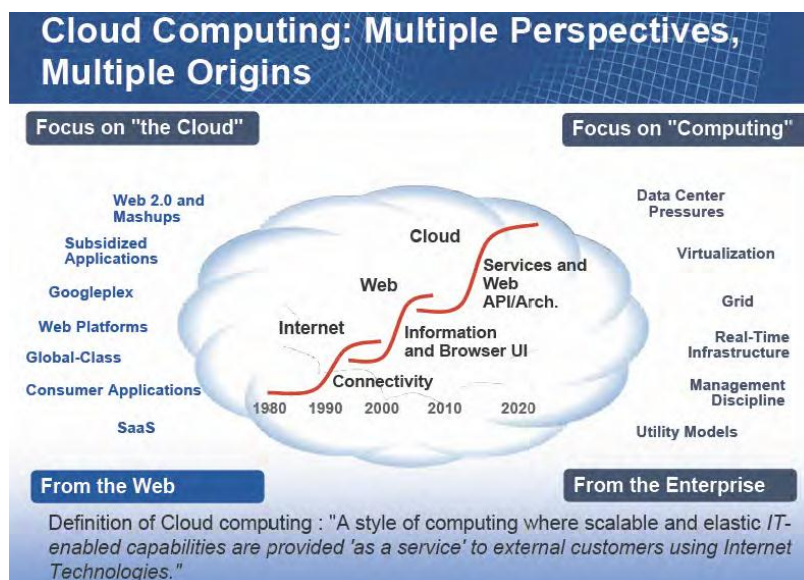
DE THEORIE

1. Definities van cloudcomputing, clouds en clouddiensten.

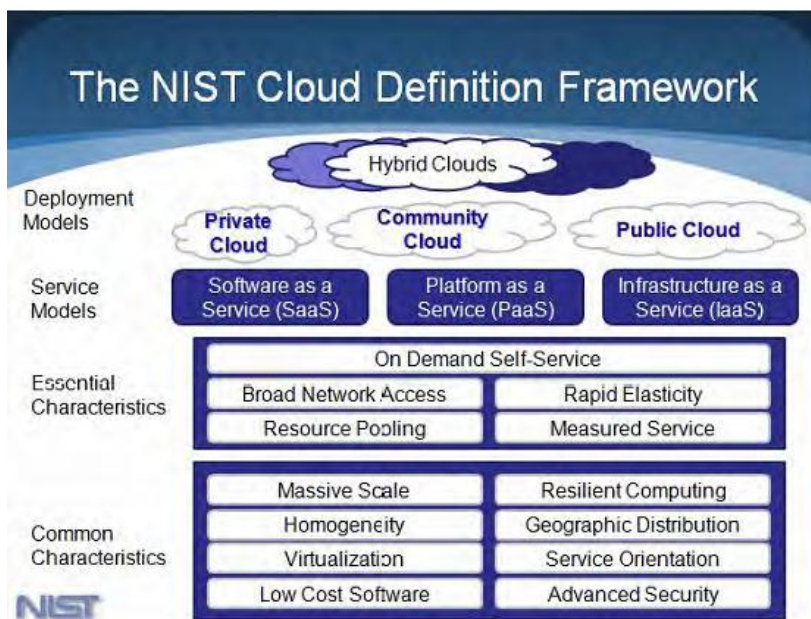
Cloudcomputing is het resultaat van een evolutie in (figuur 1):

- de technologie van het "web", welke leidt tot data transport naar de meest gunstige plek van afhandeling;
- de technologie nodig om organisaties te ondersteunen met ICT. Hierbij ligt het accent op opslag- en verwerking van gegevens. Deze opslag van gegevens en deze verwerking van gegevens is het meest doelmatig te organiseren in grote rekencentra.

Een handige definitie van cloud computing geeft het National Institute for Standards and Technology (NIST). Het NIST heeft het NIST cloud definition raamwerk vormgegeven. (figuur 2) Dit raamwerk geeft drie wijzen van leveren van cloud diensten aan. Deze wijzen zijn het leveren van Software as a service (SaaS), het beschikbaar stellen van een Platform as a service (PaaS) en het leveren van Infrastructure as a Service (IaaS). Deze cloud diensten (Mell & Grance, 2009b) hebben een vijftal essentiële en een achttal gemeenschappelijke eigenschappen. De essentiële eigenschappen zijn:



Figuur 1 : Cloud computing: de resultante van twee ontwikkelingen (Prentice,2010)



Figuur 2 : Het NIST cloud computing definition framework.

- a. On-demand self-service: Cloud computing middelen, zoals verwerkings- en opslag-capaciteit kunnen door de klant eenzijdig onder bepaalde voorwaarden opgevraagd en beschikbaar gemaakt worden zonder menselijke interactie van de cloud computing provider (Nederlands: aanbieder). Met zijn creditcard kan iemand dus online thuis een heel rekencentrum beschikbaar krijgen.
- b. Broad network access: Mogelijkheden in de vorm van diensten zijn beschikbaar via een netwerk en toegankelijk middels een gestandaardiseerde gebruikersinterface welke het gebruik van heterogene toegangsapparatuur bevordert. M.a.w. diensten zijn niet alleen via standaard computers, maar ook via mobiele apparatuur zoals een laptop, PDA's, mobiele telefoon of smartphone beschikbaar.
- c. Resource pooling: De verschillende fysieke en virtuele middelen worden door de cloud computing provider gebundeld. Dit om meerdere klanten op basis van hun vraag naar deze middelen met behulp van een multi-tenant aanpak op een dynamische wijze te kunnen bedienen. De klant heeft daarbij over het algemeen geen controle of kennis over de exacte locatie waar de middelen (bv opslag, verwerking, geheugen, netwerk bandbreedte, virtuele machines) vandaan komen. De klant kan dit inzicht wel verkrijgen indien dit noodzakelijk is in verband met juridische aspecten (bijv. indien data de landgrenzen niet mag overschrijden). Op een hoger abstractie niveau (bijv. land, staat of datacenter) kan dit inzicht dan veelal worden gegeven.
- d. Rapid elasticity: De hoeveelheid middelen kan snel omhoog of omlaag worden bijgesteld naar gelang de vraag. In sommige gevallen kan dit zelfs automatisch. Voor de klant lijken oneindig veel middelen beschikbaar en kunnen deze middelen elk moment worden aangewend, indien de klant daarom vraagt.
- e. Measured Service: Cloud systemen controleren en optimaliseren automatisch het gebruik van de middelen en maken gebruik van een meetinrichting met een bepaald niveau van abstractie naar gelang het soort dienst (bv opslag, verwerking, bandbreedte en actieve gebruikersaccounts). Hiermee kan het gebruik van de middelen kan worden gemonitord en gecontroleerd. Tevens is dit de basis van het rapporteren over het gebruik van de cloud diensten.

De drie modellen voor clouddiensten zijn:

- a. Infrastructure as a Service (IaaS): dit is de mogelijkheid voor de klant om te worden voorzien in

infrastructuur bestaande uit de verwerkings-, opslag- en netwerkvoorzieningen. Hierdoor is de klant in principe in staat om willekeurige applicatiesoftware, mits geschikt voor een bepaald door de aanbieder van clouddiensten aangegeven besturingssysteem in te zetten en uit te voeren. Voorbeelden hiervan zijn Amazon's Elastic Computer Cloud (EC2) en Amazon's Simple Storage Service (S3), maar ook IBM, Microsoft Windows Azure en andere traditionele IT-leveranciers bieden dit soort diensten aan.

- b. Platform as a Service (PaaS): De mogelijkheid om op de cloud infrastructuur van de provider gebruik te maken van de door de klant zelf geparametriseerde of zelf gemaakte of door de klant aangeschafte toepassingen. Deze toepassingen zijn gemaakt met behulp van softwareplatformen, programmeertalen en hulpmiddelen welke ondersteund worden door de aanbieder van cloud diensten. De meest bekende voorbeelden van deze vorm van cloud computing zijn Force.com van Salesforce.com, de Google App Engine en het Microsoft Azure Services platform (bijv. Live services, .NET services, SQL services).
- c. Software as a Service (SaaS): De mogelijkheid om gebruik te maken van applicaties welke draaien op een cloud infrastructuur. De applicaties zijn toegankelijk vanaf verschillende apparaten bij de vrager van clouddienste door middel van bijvoorbeeld een thin client-interface, zoals een webbrowser. De klant hoeft de onderliggende cloud infrastructuur met inbegrip van netwerk, servers, besturingssystemen, en opslag niet te beheren. Dit geldt ook voor individuele toepassingsmogelijkheden. Mogelijke uitzondering hierop zijn enkele gebruikersspecifieke configuratie instellingen waarvoor beheer wel noodzakelijk is. De bekendste vormen van SaaS zijn Salesforce.com, Google (bijv. Gmail, Calendar, Docs, Sites), Microsoft (bijv. Office Live, Office Sharepoint Online, Dynamics CRM Online) maar ook instant messaging van MSN, en VoIP van Skype.

De vier door het NIST onderscheiden leveringswijzen zijn:

- a. Public cloud: De cloud infrastructuur wordt aan het algemene publiek of aan een grote industriegroep ter beschikking gesteld en is eigendom van een organisatie die de clouddiensten verkoopt (Mell & Grance, 2009a).
- b. Private cloud: De cloud infrastructuur wordt uitsluitend geëxploiteerd voor slechts één organisatie. Deze kan worden beheerd door de organisatie zelf of door een derde partij en kan op de locatie van een organisatie fysiek zijn geplaatst of op een locatie buiten de organisatie (Mell & Grance, 2009a). Tot dit type cloud heeft het algemene publiek geen toegang.
- c. Hybrid cloud. De cloud infrastructuur is een samenstelling van twee of meer soorten clouds (private, commodity, of public) waarbij de unieke entiteiten blijven bestaan, maar onderling met elkaar verbonden zijn door gestandaardiseerde of merkgebonden technologieën die gegevens- en applicatie portabiliteit mogelijk maken zoals bijvoorbeeld cloud bursting voor load-balancing tussen clouds (Mell & Grance, 2009a).
- d. Community cloud: De cloud infrastructuur wordt gedeeld door verschillende organisaties en ondersteunt een gemeenschap specifiek gedeelde zorg (bijvoorbeeld een cloud voor organisaties op het terrein van de zwaailichten). Deze cloud kan worden beheerd door de organisaties zelf of door een derde partij. Zij kunnen zijn geplaatst op de locaties van een van de organisaties of op een locatie buiten de organisaties (Mell & Grance, 2009a).

2. Wetten, regels en normen én actiepunten voor de overheden.

Bij cloud computing kan men te maken hebben met privaatrechtelijke aspecten, publiekrechtelijke wetgeving en met opkomende standaards en normen.

2.1. Privaatrechtelijke aspecten bij cloudcomputing.

Wanneer men te maken heeft bij cloudcomputing met privaatrecht, zoals bij het sluiten van sluiten, dan moet

men beseffen, dat:

- a. van toepassing zijnde wetgeving geografisch gebonden is en dat cloud computing vaak leidt tot een gegevenstransport over landsgrenzen en een opslag en verwerking van gegevens in een ander land. De wetgeving van dit land is dan van toepassing als naar de letter van het contract gekeken wordt.
- b. bij het maken van het contract helder moet zijn, waar de aanbieder van de clouddiensten:
 - de gegevens opslaat en verwerkt;
 - wie de gegevens verwerkt of benadert: dit kunnen meerdere cloud platforms zijn. Deze kunnen op diverse geografische locaties zijn geplaatst;
 - of de gegevens geëncrypted moeten worden (en kunnen worden)?
 - hoe lang de gegevens na beëindiging van een contract bewaard worden.
- c. de leveranciers van cloud diensten vaak clausules hebben als:

"Google and partners do not warrant that:

- *Google services will meet your requirements;*
- *Google services will be uninterrupted, timely, secure or error free;*
- *the results that may be obtained from the use of Google services will be accurate or reliable;*
- *the quality of any products, services, information or other material purchased or obtained by you through Google services will meet your expectations."*

Dat betekent dat bij het sluiten van het contract aandacht moet worden gegeven aan:

- de wijze van backup/herstel van gegevens en het herstel bij emergencies;
- de service niveaus en de gevolgen van niet beschikbaarheid van het internet;
- de continue beschikbaarheid van diensten om de organisatie te ondersteunen;
- het behandelen van gegevens bij beëindiging of faillissement van de aanbieder;
- beveiligingsstandaards en de wijze van handelen bij een probleem met de beveiliging van ICT;
- de rechten van een klant bij overname/fusie;
- boetes bij niet beschikbaarheid of magere respons;
- het recht van de klant op het doen van of ter beschikking krijgen van door derden uitgevoerde audits en de rechten om te handelen bij overmachtssituaties.

2.2. Aandachtspunten op het terrein van het publiekrecht.

Besef op het terrein van publiek recht, dat:

- a. Cloud computing gevolgen heeft voor de *privacy van persoonsgegevens* en voor de *vertrouwelijkheid van gegevens van organisaties*. De wettelijke bescherming van persoonsgegevens kan per land wisselen en is voorts afhankelijk van de voorwaarden voor dienstverlening en het beleid op het terrein van privacy van de cloud aanbieder. Deze aanbieder kan voorts binnen de wettelijke mogelijkheden de voorwaarden naar eigen inzicht aanpassen
- b. Bij sommige soorten informatie en bij sommige soorten gebruikers van cloud computing *de situatie verandert*, wat betreft rechten op privacy en vertrouwelijkheid van de klant én de verplichtingen van de dienstaanbieder op dit terrein, als de aanbieder besluit de informatie van deze gebruikers te plaatsen op een cloud in een ander land of op de cloud van een leverancier van cloud diensten.
- c. Cloud computing aanbieders kunnen *door overheden plichten worden opgelegd*. Men kan hen verplichten informatie te leveren. Men kan hen verplichten actief na te lopen op criminele activiteiten.
- d. *De wetten van overheden lopen vaak achter*. Hierdoor komt toepassing van oude wetten op nieuwe technologische mogelijkheden voor.

2.3. Standaards.

Een overzicht van de standaards op het terrein van cloud computing ziet men op:

(http://cloud-standards.org/wiki/index.php?title=Main_Page) Belangrijke standaards, die men in de praktijk tegenkomt zijn:

- a. Standaards op het terrein van security (www.cloudsecurityalliance.org) als bijvoorbeeld FISMA, NIST 800-53 en ISO 27001. Deze standaarden betreffen alle de beveiliging van ICT voorzieningen.
- b. Standaards op het terrein van auditing (<http://www.cloudaudit.org>): Het doel van deze standaards is onder meer om te komen tot een gemeenschappelijke aanpak, welke cloud aanbieders in staat stelt om de audit, het beheer, de beoordeling en het zekerstellen van hun IaaS, PaaS en SaaS omgevingen automatisch te verrichten.
- c. Standaards van algemene standaardisatie organisaties, zoals het NIST.

3. De business case voor cloud computing.

Donkers (2011) heeft de artikelen, welke tot juli 2010 zijn verschenen in de wetenschappelijke literatuur nagelopen op de voor- en nadelen van cloud computing. De frequentie, waarin in deze literatuur bepaalde voor- en nadelen van cloud computing werden genoemd, ziet men in figuur 3. Deze frequentie kan als een mate van belang van een voor- of nadeel gezien worden. Kijkende naar figuur 3 valt op dat redenen om cloud computing toe te passen vooral financiële redenen zijn. De belangrijkste technische reden is de schaalbaarheid van cloud computing. Met andere woorden het snel en eenvoudig kunnen bij- of afschakelen van cloud computing diensten. Daarnaast speelt de toegang tot diensten welke voorheen ontoegankelijk waren (door technische of financiële onmogelijkheden) een belangrijke rol.

	Totaal
Redenen om cloud computing toe te passen (voordelen):	
· Verbeterde toegankelijkheid van diensten (b.v. toegang tot mogelijkheden welke in huis niet gegeven worden, on demand schaalbaarheid)	17
· Andere (technische) redenen c.q. voordelen (b.v. reductie hardware kosten, capaciteit rekencentrum, capaciteit geheugen, frequentie software updates)	28
· Financiële redenen c.q. voordelen (b.v. reductie hardware kosten, reductie aantal ICT medewerkers en/of administratiekosten)	32
Redenen om cloud computing NIET toe te passen (risico's \ nadelen):	
· Operationele risico's	77
· Contingentie risico's (ISO/IEC 24762:2008 Disaster recovery services en BS 25999:2006/2007 business continuïteit en BS 25777:2008 informatie en communicatie technologie continuïteit management)	34
· Beveiligingsrisico's (ISO/IEC 27002:2005 voorheen 17799 :2005). Deze zijn grotendeels vergelijkbaar met de beveiligingsrisico's van een in-house oplossing	36
· Diensttoetreding risico's	8
· Lopende het gebruik risico's	14
· Privacy risico's	65
· Compliance (naleving) risico's.	15

Figuur 3 : Voor- en nadelen uit de literatuur (tot juli 2010) aangevuld met Lute (2009).

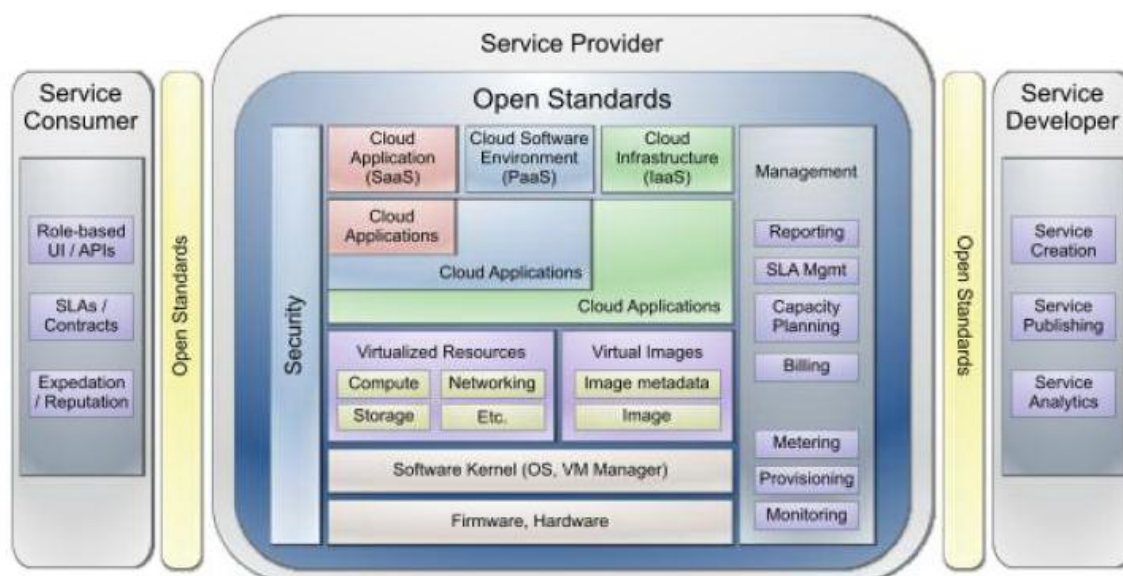
4. Implementatie van cloud computing.

Er zijn verschillende visies op de implementatie van cloud computing diensten. Een van deze visies is die van Lute c.s. (2009). Zij hebben de visie, dat organisaties bij het omgaan met cloud computing drie stadia doorlopen. Deze zijn:

- a. **Stadium 1:** het ontwikkelen van een interne cloud. In deze fase staan centraal:
 - a.1. het virtualiseren, optimaliseren en centraliseren van ICT omgevingen;
 - a.2. het volledig uitnuttend van de mogelijkheden van virtualisatie met aandacht voor beschikbaarheid, flexibiliteit en kostenreductie centraal en tenslotte het zorgen voor monitoring en beheer.
- b. **Stadium 2:** het doen van een pilot met een externe cloud. Nu er overzicht is van infrastructuur en applicaties en duidelijk wat men conform de SLA verwacht, kan men proeven doen met externe clouddiensten. Nu wordt achtereenvolgens:
 - b.1. : het projectteam voor de pilot gekozen;
 - b.2. : de externe cloud dienst leverancier, de voor de pilot geschikte applicatie, wordt deze op de cloud geplaatst en worden de doelen én de evaluatie criteria vastgelegd. In deze fase wordt duidelijk welke hulp men nodig heeft om de gewenste cloud met de juiste eigenschappen van de service qua beschikbaarheid, security en authenticatie te realiseren.
- c. **Stadium 3:** het geven van een road map voor de organisatie naar het op grote schaal gebruiken van cloud diensten.

5. Organiseren en sturen van cloud diensten.

Om clouddiensten te leveren en van clouddiensten gebruik te kunnen maken richten vragers, resp. aanbieders van deze diensten een organisatie in. In de literatuur gaan Ahronityz c.s. (2010) op de onderwerpen, die bij het inrichten van zo'n organisaties aan de orde komen. Hun schematische weergave van onderwerpen is in figuur 4 weergegeven. In de checklist zullen vragen over de inrichting van de organisatie voor cloud computing aan de kant van de vrager van cloud computing diensten en aan de kant van de aanbieder van cloud computing diensten aan de orde komen.



Figuur 4 : Van belang zijnde onderwerpen bij klant, leverancier en ontwikkelaar bij cloud diensten.

6. Het beëindigen/vermindere van het gebruik van cloud computing diensten.

Bij beëindigen van clouddiensten komen technische en organisatorische aspecten aan de orde. Technische aspecten betreffen het kunnen verplaatsen van de ICT voorzieningen van de ene naar mogelijke het eigen rekencentrum of naar een andere cloud; het eventueel moeten converteren van gegevens hiervoor en de zorg voor het verwijderen van de eigen gegevens op de oorspronkelijke cloud. Bij het kunnen verplaatsen van zijn ICT is het onder meer van belang dat de cloud leverancier standaard gebruikt. Bij het converteren van gegevens moeten er garanties zijn dat men geen gegevens verliest en/of te maken krijgt met corruptie van gegevens. Bij het verwijderen van data moet men er zeker van zijn, dat alle data verwijderd is.

Naast technische onderwerpen, spelen bij beëindiging van een dienst ook nog andere onderwerpen, zoals bijvoorbeeld juridische. Bij sommige contracten, zoals die bij het gebruik door deskundigen van de Amazon S3 laaS dienst is op- en afschalen van een dienst eenvoudig. Bij andere clouds zoals de Microsoft SaaS diensten, Salesforce diensten of AFAS diensten heeft men te maken met contract, dat voor een bepaalde termijn gesloten is.

7. De impact van het gebruik van cloud diensten.

Mogelijkheden als cloud technologie kunnen tot simplificaties van organisaties leiden en tot het gebruik van nieuwe mogelijkheden. Fingar (2009) geeft hier in figuur 5 enige voorbeelden van.

Organisatie 1.0	Organisatie 2.0
Kent hiërarchie	Is platter
Kent fricties in afstemming	Gestroomlijnde processen
IT-gedreven technologie inzet	Gebruikers gedreven inzet
Teams op één plaats aanwezig	Teams wereldwijd & 24*7
Informatiesystemen zijn voor gestructureerde informatie	Ook sociale platformen.
Proprietary standaarden	Meer open standaarden
Gepland	On demand werken
Lange time to market	Korte time to market
Informatie op need to know basis	Uitgangspunt transparante informatievoorziening.

Figuur 5:

Andere wijzen van werken
bv. met cloud maakt andere
organisatie mogelijk.

DE CHECKLIST.

a. DEFINITIES.

Bij cloud computing wordt een onderscheid gemaakt tussen private clouds, hybrid clouds, community clouds en public clouds. Vanuit deze clouds worden diensten geleverd

1. Wat is uw definitie van cloudcomputing? In hoeverre past deze in de definities van het NIST?
2. Van welke soorten cloud computing maakt uw organisatie gebruik? Betreft het hier private, hybrid of public cloud computing?
3. Vindt u het onderscheid tussen clouds en cloud services juist? En waarom?

b. PRIVAATRECHTELIJKE EN PUBLIEKRECHTELIJKE ASPECTEN, VOORTS NORMEN.

De vragen in dit onderdeel zijn onderverdeeld in categorieën:

- B1 Privaatrechtelijke aspecten;

- B2. Publiekrechtelijke aspecten
- B3. Normen.

B1 PRIVAATRECHTELIJKE ASPECTEN.

Bij het gebruiken van clouds of clouddiensten hangt het van de soort dienst af, welke contracten gesloten worden en welke SLA's daarbij horen. In feite probeert men in een contract en de daarbij horende SLA de dienst qua performance vast te leggen en risico's voor zover deze ex ante te voorzien zijn uit te sluiten. Deze vraag gaat in op de onderwerpen welke in een contract over clouddiensten of over het gebruiken van de cloud worden vastgelegd. De vragen betreffen:

DE GELEVERDE DIENST.

1. Hoe is de geleverde cloud dienst of het gebruik van de cloud gespecificeerd?
2. Zijn er aanpassingen gemaakt om de standaard dienst beter te laten aansluiten bij de wensen van de gebruiker of de organisatie? Zo ja, welke?
3. Zijn er bepalingen opgenomen ten aanzien van de versie(s) van de programmatuur en haar updates? Zo ja, welke?
4. Zijn er afspraken gemaakt over de protocollen van communicatie? Zo ja, welke?
5. Zijn er afspraken over gegevensformaten van de leverancier? (Men wil bijvoorbeeld zijn database kunnen benaderen met business intelligence tools. Dan moet je wel weten wat de data lay-out is). Zo ja, welke?
6. Zijn er afspraken gemaakt over schaalbaarheid en prijs? Zo ja, welke?

DE LICENTIES.

1. Zijn er afspraken gemaakt wat betreft de **licenties** nodig om de dienst of de cloud te gebruiken? Zo ja welke? Wie is hier aansprakelijk? En zo ja, waarvoor?

DE ORGANISATIE VAN DE DIENST.

1. Zijn er in de overeenkomst of in de SLA nadere afspraken gemaakt over:
 - betrokken contactpersonen en zo ja, welke?
 - escalatie procedures en zo ja, welke?
 - boete clausules en zo ja, welke?
 - zijn er wat betreft de te leveren diensten afspraken gemaakt op het terrein van rapportage? Zo ja welke en met welke frequentie wordt gerapporteerd en tussen wie?

DE BETROUWBAARHEID VAN DE DIENSTVERLENING.

1. Zijn in de contracten bepalingen opgenomen om:
 - de beschikbaarheid van de dienst of de cloud? Zo ja welke? Het betreft hier de beschikbaarheid en de bereikbaarheid (anywhere?) van een dienst of de cloud; van de infrastructuur, qua verwerking, netwerk, opslag en databases;
 - toegankelijkheid van de dienst of de cloud? Zo ja welke? Het gaat hier om de netwerken om de dienst te bereiken, de snelheid van toegang en de snelheid van de response van de server.
 - robuustheid van de dienst of de cloud. Zo ja welke? Het betreft hier de frequentie van niet beschikbaarheid, waaronder de continuïteit ondanks het optreden van een reeks van faalmogelijkheden.
 - herstel van de dienst of de cloud na outage, en zo ja, welke? Dit betekent het snelle herstel van de dienst of de cloud als er een falen of geplande outage is opgetreden. Een

geplande outage is bv. het doen van upgrades.

- reparatie van gegevens of transacties en zo ja, hoe? Het betreft hier het herstel van databases en transacties welke werden onderbroken bij een ongepland falen.

Besef dit komt voor: Gmail viel in 2008-2009 6 maal uit binnen 8 maand. Rackspace had uitval in juni, juli en november 2009.

DE INTEGRITEIT VAN DE DIENST.

1. Zijn de in de contracten of de SLA's bepalingen opgenomen ten aanzien van de te leveren continue kwaliteit van:

- inhoud van de dienst;
- versies van de dienst;
- interfaces met andere programmatuur;
- programmatuur versies en verplichte updates;

Besef dat een klant afhankelijk is van de provider voor onderzoek, correcties, prioriteit van zijn inspanningen en het geven van informatie over de reden van mogelijke problemen.

HET BEHEER VAN DE DIENST.

Bij het leveren van een dienst wil de klant graag, waarbij mogelijke gebreken snel worden ontdekt, gemeld, onderzocht, opgehelderd en dan hersteld. Ook kan zij wensen, dat kleine aanpassingen worden aangebracht zonder invloed op fit, betrouwbaarheid of integriteit en tegen redelijke kosten. Zijn hiervoor afspraken vastgelegd? Zo ja, welke?

DE KOSTEN VAN DE DIENST.

Zijn er in het contract afspraken gemaakt over de kosten nu en de kosten op termijn? Zo ja, welke? En wat zijn hierbij de uitzonderingen?

RISICOS BIJ HET GEBRUIK VAN DE DIENST (zie ook ISO/IEC 24762:2008;BS25999:2006/2007/2008)

1. Grotere onderbrekingen van de dienst of de cloud: de betekenis van "grotere" hangt van de klant af, maar zijn hier afspraken over gemaakt en zo ja, welke?
2. Terugtrekken van de dienst of de cloud: wat zijn de afspraken ten aanzien van bv.
 - escrow
 - gegevens backup
 - zekerheid, dat de gegevens en de applicaties niet onderwerp zijn van de boedel en zo door een curator kunnen worden achtergehouden.
3. Verlies van gegevens: ook al blijft de leverancier in business, dan nog is er een mogelijkheid van verlies van gegevens. Wat zijn hier de afspraken over? Zie bv. het verlies van gegevens van T-mobiles Sidekick klanten.
4. Flexibiliteit: De leverancier van services en clouds moet verzekeren, dat:
 - zijn programmatuur, protocollen en gegevensformaten forward compatible zijn, zodat migratie naar nieuwe niveaus van dienstverlening mogelijk is;
 - zijn programmatuur, protocollen en gegevensformaten backwards compatible zijn, zodat gebruik van legacy mogelijk is;
 - men bij gebruik van zijn dienst of cloud zo mogelijk eenvoudig over kan gaan naar een concurrent.
 Welke bepalingen zijn over deze drie onderwerpen vastgelegd?

VEILIGHEID (Zie ook ISO/SEC 27002:2005)

1. Veiligheid van de dienst of de cloud: dit betekent dat de dienst of de cloud bestand is tegen omgevingsdreigingen en activiteiten van derden, welke de betrouwbaarheid of de integriteit van de dienst of de cloud betreffen. Zijn er op dit terrein bepalingen opgenomen en zo ja, welke?

2. Veiligheid van de gegevens: dit betekent dat de gegevens bestand zijn tegen omgevingsdreigingen en activiteiten van derden, welke de betrouwbaarheid of de integriteit van de dienst of de cloud betreffen. Zij er op deze terrein bepalingen opgenomen en zo ja, welke? Besef dat er bij Amazon EC2 al is geconstateerd dat er een botnet command en een control module in de software werd geplaatst.
3. Authenticatie: eenvoudige toegang tot de klant en tegelijk geen toegang tot onbevoegden. Zijn hier afspraken over vastgelegd en zo ja welke?
4. Gevoeligheid voor denial of service aanvallen: zijn hier waarborgen tegen gegeven en zo ja, welke?

OMGAAN MET BUSINESS- EN WETGEVINGSRISICO'S.

1. Overname door derden: zijn hier wijzen van werken over vastgelegd en zo ja, welke?
2. Privacy, dit betreft:
 - a. niet toegestane handelingen op het terrein van toegang tot gegevens, gebruik van gegevens, doorgeven van gegevens aan derde partijen en achterhouden van gegevens.
 - b. niet toegestane handelingen van derden. Deze betreffen de onderwerpen van a. plus het onbevoegd voordeel halen uit slechte beveiliging van de opslag van gegevens of van gegevens in transport naar een andere plaats.
 - c. het omgaan met het feit dat de cloud vaak zijn gegevens op diverse geografische plaatsen heeft opgeslagen.
Welke bepalingen zijn op dit terrein opgenomen?
3. Compliance met publiekrechtelijke wetgeving, bv. wetgeving als de Patriot Act, Sarbanes Oxley: Zijn er afspraken vastgelegd als gevolg van deze wetgeving en welke eisen stellen aan de beschikbaarheid van bv. leveren van gegevens, rapportages, audits etc. Welke zijn dit?

bv. met sectorale wetgeving:

Zijn er afspraken gemaakt als gevolg van wetgeving in:

 - de gezondheidssector. Zo ja, welke?
 - in de bank of verzekeringssector. Zo ja, welke?
 - in de justitiesector, zo ja, welke?
 - in de energiesector, zo ja, welke?
 - in de telecommunicatiesector. Zo ja, welke?
 - zijn er andere? Zo ja, welke?

Ga hier bijvoorbeeld na:

 - toegang tot de gegevens voor wie?
 - eisen aan plaats van opslag?
 - bewaartermijn, zo ja welke, waarvoor?
 - garanties voor verwijderen van de gegevens?
 - audit van de dienst of de cloud? Welke aspecten? Hoe vaak?
 - afspraken over monitoren om inbreuken te ontdekken? Welke? Rapportage aan wie? En hoe vaak?

B2. PUBLIEKRECHTELIJKE ASPECTEN AAN CLOUDCOMPUTING.

Op het terrein van publiekrechtelijke wetgeving heeft uw organisatie te maken met generieke en specifieke wetgeving. Onder generieke wetgeving vallen wetgevingen als de wetgeving ter bescherming van de persoonlijke levenssfeer, de Patriot act in de USA, milieuwetgeving, etc. Onder specifieke wetgeving vallen wetgeving in onderwijs, zorg, financiële sector, etc.

1. Voor wat wetgeving betreft zijn hierboven generieke wetten aangegeven. Wetten leiden tot een toestemming of een verbod. Bij toestemming kan er sprake zijn van toestemming zonder meer, toestemming voor bepaalde groepen, toestemming met rapportage plichten. De toestemming zelf kan uit de wet of uit een vergunning volgen.
 - a. Kunt u aangeven met welke generieke wetgeving uw organisatie als klant van clouds of clouddiensten vooral te maken heeft? Geldt dit voor uw private én publieke clouds?

- b. Kunt u aangeven, wat de gevolgen van deze wetgeving zijn, als uw organisatie gebruik maakt van clouddiensten of van een cloud, welke:
 - b.1. zich in Nederland bevindt;
 - b.2. zich in het buitenland bevindt?
 - c. Wie controleert of de aangegeven maatregelen ook worden nageleefd? En wat houdt die controle in? Wat zijn de boetes bij niet naleving?
2. Voor wat wetgeving betreft zijn hierboven specifieke wetten aangegeven. Deze leiden tot een toestemming of een verbod. Bij toestemming kan er sprake zijn van toestemming zonder meer, toestemming voor bepaalde groepen, toestemming met rapportage plichten. De toestemming zelf kan uit de wet of uit een vergunning volgen.
- a. Kunt u aangeven met welke specifieke wetgeving klanten van clouds of clouddiensten van uw organisatie vooral te maken heeft? Geldt dit voor private én publiek clouds of...
 - b. Kunt u aangeven, wat de gevolgen van deze wetgeving zijn, als uw organisatie gebruik maakt van diensten of van een cloud, welke:
 - b.1. zich in Nederland bevindt;
 - b.2. zich in het buitenland bevindt?
 - c. Wie controleert of de aangegeven maatregelen ook worden nageleefd? En wat houdt die controle in? Wat zijn de boetes bij niet naleving?
3. Hoe gaat uw organisatie om met de voor haar geldende wetgeving op het terrein van services en clouds? Waar heeft uw organisatie hiervoor adviesdiensten van derden ingeschakeld en wat betekende dat?
4. Welke maatregelen nemen uw leveranciers om te voldoen aan de generieke en specifieke wetgeving, bijvoorbeeld de Patriot act, de HIPAA (USA gezondheidswetgeving)? En wat zijn daar de effecten van voor hen zelf en hun klanten?
5. Is het u bekend, welke wetgeving op dit terrein komende is? Welke wetgeving verwacht u? Ook op politiek niveau wordt er gekeken naar cloudcomputing. Zijn er aanwijzingen dat bepaalde landen erg of bepaalde landen minder geschikt voor uw organisatie zijn voor cloud rekencentra? Welke zijn dat? En wordt daar politiek op gevoerd en door wie in uw organisatie?

B3 NORMEN.

Op het terrein van cloud computing en service kan gebruik worden gemaakt van diverse normen. Deze normen betreffen bijvoorbeeld:

- a. De NIST 800-53 R3. Deze gaat over het auditen van clouds en clouddiensten. Dan worden er vragen gesteld als beneden aangegeven (www.cloudaudit.org). Maakt uw organisatie gebruik van de mogelijkheden van een dergelijke standaard om uw cloud of clouddienst te auditen? En zo ja hoe?
- b. Op de wiki : http://cloud-standards.org/wiki/index.php?title=Main_Page staan voorts de andere standaards op dit terrein genoemd. Het betreft onder andere:
 - b.1. het [Open Virtualization Format \(OVF\)](#) : DSP0243 Open Virtualization Format (OVF) V1.1.0 This specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.
 - b.2. het [Interoperable Clouds White Paper](#): DSP-IS0101 Cloud Interoperability White Paper V1.0.0 This white paper describes a snapshot of the work being done in the DMTF Open Cloud Standards Incubator, including use cases and reference architecture as they relate to the interfaces between a cloud service provider and a cloud service consumer.
 - b.3. de komende standaards van de ETSI ([The European Telecommunications Standards Institute \(ETSI\)](#))
 - b.4. de komende standaards van het [Open Grid Forum \(OGF\)](#) en haar werkgroep [Open Cloud Computing Interface \(OCCI\) Working Group](#) The purpose of this group is the creation of a practical solution to interface with Cloud infrastructures exposed as a service (IaaS). We will focus on a solution which covers the provisioning, monitoring and definition of Cloud Infrastructure services. The group should create this API in an agile way as we can have advantages over other groups if we deliver fast.

1. Is/wordt door uw organisatie meegewerkt aan het maken van deze standaards? En wat is uw ervaring daarbij?
2. Heeft u bij het maken van contracten gekeken naar een of meerdere van deze standaards? Wat waren uw ervaringen daarbij?
3. Zijn er naar uw mening andere niet genoemde belangrijke standaards op dit terrein? Welke zijn dit?
4. Gebruikt uw organisatie in uw contracten standaards? Welke? Waarvoor? Wat zijn uw ervaringen hiermee?

C. DE BUSINESS CASE.

De vragen over de business case zijn onderverdeeld in twee categorieën:

- C1 Uw positie en de omgeving.
- C2 De business case zelf

C1 UW POSITIE.

1. Vanaf welke datum bent u met welk gebruik van cloud diensten begonnen en wat is de omvang van dit gebruik?
3. Mc Kinsey maakt bij het beslissen over het gebruik maken van de cloudservices en andere mogelijkheden van de cloud onderscheid tussen vier typen van besluiten. Deze zijn:
 1. Financiële: Men stelt dat de huidige cloud computing niet kosten doelmatig is vergeleken met de kosten van de data centers van de grote ondernemingen.
 2. Technische: Qua beveiliging en betrouwbaarheid moeten bezwaren worden weggenomen en toepassingen opnieuw vormgegeven worden.
 3. Operationele: De visie, dat gebruik van clouds een zekere mate van flexibiliteit geeft en sneller mogelijkheden operationeel krijgen moet in de juiste context worden gezien.
 4. Organisatorische: De IT vraag- en aanbodorganisatie moeten worden aangepast op het werken in een wereld, waarin cloud computing mogelijk is.
 - a. Kunt u aangeven in welke mate bovengenoemde overwegingen in uw organisatie bij elk gebruik van de cloud aan de orde kwam? En wat daar de gevolgen van waren?
 - b. Kunt u aangeven in hoeverre deze overwegingen ook een rol hebben gespeeld in de gemaakte business case?
4. Mc Kinsey rekent voor, dat voor grotere organisaties cloud computing services in het algemeen niet aantrekkelijk zijn wat betreft kosten en Amhurst c.s (Communications of the ACM, 2010) stellen, dat gezien het feit, dat licenties vaak aan computers gebonden zijn veelal open source software gebruikt wordt. (zie additioneel materiaal site www.fontys.nl/lectoren/ictgoveranance). Voorts stelt men dat de kosten van clouds met meer dan 60% omlaag moeten, wil het voor klanten aantrekkelijk worden hun hele rekencentrum in de cloud te hangen.

Vragen:

 - a. speelt het gebruik van Linux systemen in uw organisatie? En heeft dit een relatie met de mogelijkheden van cloudcomputing?
 - b. heeft u overwogen uw hele rekencentrum in de cloud te zetten en speelden hierbij financiële overwegingen een rol? Wat was de uitkomst hiervan en waarom?
 - c. kijkend naar mogelijke besparingen om een heel rekencentrum in de cloud te zetten, komt McKinsey tot een besparing van 10-15% aan menskracht. Zijn er bij u ook dit soort berekeningen gemaakt? En wat was de uitkomst?
 - d. de cloud mogelijkheden leiden ertoe eens scherp naar eigen centra te kijken. Men

- private laas public laas.

Lute (2009) geeft aan, dat bij een onderzoek de volgende voordelen van cloudservices werden genoemd:

Redenen om cloud computing te overwegen	
On-demand schaalbaarheid en flexibiliteit voor de business	50%
Reductie hardwarekosten	38%
Reductie aantal ict-medewerkers en administratiekosten	35%
Toegang tot mogelijkheden die 'in huis' niet ontwikkeld worden	28%
Wij gebruiken cloud computing niet en overwegen dat ook niet	19%
Capaciteit van het datacenter	16%
Capaciteit van de storage	11%
Frequente software-updates	10%
Anders	5%

- kunt u per cloud service aangeven, welke aspecten bij elke service een rol speelden en hoe dat tot uiting kwam in de business case?
- welk aspect was per cloud service in uw geval het belangrijkste en waarom?
- kunt de voordelen in geld uitdrukken? Zo ja, zou u dit uit kunnen leggen?

- IBM (Mayo, R. c.s, november 2009) stelt dat bij het overgaan van een traditionele infrastructuur naar een public cloud infrastructuur de financiële voordelen beperkt zijn. Wel worden belangrijke financiële voordelen geboekt als men overgaat naar een private cloud. Is dit ook uw ervaring? Zo ja, waarom wel, zo nee, waarom niet. Kunt u dit met een voorbeeld ondersteunen?
- IBM (Mayo, R. c.s, november 2009) gaat na op basis van ROI, waar de voor/nadelen van de diverse types cloudservices liggen. Loop achtereenvolgens de voordelen en de nadelen door en ga daarbij erop in, hoe dit per cloud service bij uw organisatie speelt.
 - Zijn in de business cases voor uw cloudtoepassingen de besparingen op het terrein van apparatuur meegenomen? Het betreft afschrijving en lopende kosten voor huisvesting en energie?
 - Zijn in de business cases voor uw cloudtoepassingen de kosten en besparingen op het terrein van programmatuur meegenomen?

Het betreft hier:

 - virtualisatie programmatuur;
 - beheerprogrammatuur;
 Besparingen betreffen de mindere licentiekosten voor operating systemen, netwerk, verwerking, opslag| etc.
 - Zijn in de business cases voor uw cloudtoepassingen de kosten en besparingen op het terrein van het leveren van ICT opgenomen? Dat betekent het automatisch leveren van bijvoorbeeld testomgevingen, het automatisch kunnen testen van toepassingen; het hebben en in productie zijn van een beleid voor patches, upgrades enz.
 - Zijn in de business cases voor uw cloudtoepassingen de kosten en besparingen door de verhoogde productiviteit opgenomen? Deze kan zijn ontstaan door het nu geautomatiseerd doen van taken, het hebben van standards service in een service catalog, het sneller ter beschikking hebben van ICT etc.
 - Zijn in de business cases voor uw cloudtoepassingen de kosten en besparingen door de beter systeembeheer opgenomen als betere geautomatiseerde monitoring, rapportages, beter overzicht door minder apparatuur etc.
- IBM (2009) heeft de organisatiekosten, communicatiekosten etc. om met bepaalde clouds te werken niet in zijn voordelen/nadelen opgenomen. Dat houdt in dat men een organisatie moet hebben om met in elk geval de externe cloud leverancier om te gaan. Wat is deze organisatie voor u en wat zijn de hiermee gepaard gaande kosten?
- Heeft u een standaard formaat voor het maken van business cases? Hoe ziet dat eruit? Heeft u dit formaat aangepast voor het maken van business cases voor cloudtoepassingen? Wat houdt deze aanpassing in? Staan hier naast op financiële voordelen te herleiden opbrengsten ook andere in? En welke zijn dat? Wat is de relatieve grootte daarvan?
- Heeft u een hybride cloud? Wat betekent dat voor de business case? Als u eerder dezelfde service in eigen huis deed, dan moeten bij het overgaan naar een hybride situatie er voordelen optreden. Welke zijn dat?

Spelen de echte financiële voordelen nog? Zo nee, waarom niet?

15. Wat is uw conclusie over de voor- en nadelen van cloud toepassingen anno 2011?
 - welke toepassingen zijn gewoon geschikt voor de cloud? En voor de private of de publieke?
 - is er verschil qua geschiktheid wat betreft het continu doen van een beroep op cloud diensten ten opzichte van het gebruik bij het omgaan met piekloads, wisselende capaciteitseisen, voorkomen van tijdelijke investeringen etc.? Welke zijn die verschillen?
 - wat ziet u voor uw organisatie als echte belemmeringen om van clouds gebruik te maken en waarom?
16. Zijn bij de business case voor elke cloud of dienstleverancier de volgende onderwerpen meegenomen en hoe zijn deze per case gewaardeerd? Als zij niet zijn meegenomen, waarom niet?
 - a. de wijze van inrichting van de cloud leverancier en de wijze van rapporteren over het wel of niet halen van de eisen van de contracten of SLA's;
 - b. hoe de leverancier omgaat met toegangscontrole en welke faciliteiten zij biedt om deze controle bij haar klant te houden?
 - c. hoe zij omgaat met netwerk- en applicatiebeveiliging en hoe zij de door hen op dat terrein genomen maatregelen kunnen justificeren?
 - d. welke modellen de leverancier biedt op het terrein van recovery, elasticiteit van de diensten?
 - e. de mate waarin de eigen diensten eenvoudig naar de cloud kunnen worden overgezet en mogelijk eenvoudig van de ene naar de andere cloudleverancier kunnen worden verplaatst?
 - f. of men voorziet in wijzen van werken om eenvoudig virtuele omgevingen van de eigen rekencentra over te zetten naar de cloud en ze te optimaliseren?
 - g. hoe men omgaat met de communicatie over het beheer van de dienstverlening tussen de klant en de cloudleverancier?
 - h. welke mogelijkheden er voor de klant en welke er voor de applicatie aanwezig zijn om te komen tot doordachte besluiten over het beheer van het verkeer met de cloud?
 - i. hoe de mogelijke koppeling van informatie van de cloud applicatie met eigen beheerde applicatie is te realiseren is en wie de verantwoordelijkheid van deze interface heeft
 - j. of wat de cloudleverancier levert verschillend of minder is dan de diensten, die het eigen rekencentrum al levert?

D. DE IMPLEMENTATIE.

Lute c.s. (2009) geven aan , dat bij het realiseren van een cloud oplossing een organisatie in het algemeen drie stadia doorloopt. Dit zijn de stadia van het ontwikkelen van een interne cloud, een pilot met een externe cloud en het opstellen van een roadmap voor de langere termijn.

1. Heeft uw organisatie deze stadia ook doorlopen? Lute (2009) geven ook aan dat bij het denken over cloud sourcing waarbij eerst de ICT voorzieningen in eigen huis werden geëxploiteerd, de organisatie een traject doorloopt met:
 - a. in fase 1:
 - a.1. virtualiseren, optimaliseren en centraliseren van ICT omgevingen;
 - a.2. volledig uitnutten van de mogelijkheden van virtualisatie met aandacht voor beschikbaarheid, flexibiliteit en kosten reductie;
 - a.3. tenslotte het zorgen voor monitoring en beheer.
 - b. in fase 2: nu er overzicht is van infrastructuur en applicaties en duidelijk is wat conform de SLA verwacht wordt, gaat men over tot het doen van een pilot. Dat betekent:
 - b.1. het kiezen van het juiste projectteam;
 - b.2. het kiezen van de externe cloud;
 - b.3. het bepalen van de voor de pilot geschikte applicatie en dat plaatsen op de cloud;
 - b.4. het kiezen van doelen en de evaluatie criteria.

Nu wordt ook duidelijk welke hulp men nodig heeft om de gewenste cloud met de juiste eigenschappen van de service qua beschikbaarheid, security en authenticatie te realiseren.

- c. in fase 3: er wordt een road map voor gebruik van cloud computing gegeven voor de organisatie.
2. a. Kunt u aangeven in hoeverre het traject, dat Lute c.s. beschrijven herkenbaar is voor uw organisatie?
 - b. Als u fase 1 doorlopen hebt, was er toen bij u transparantie wat betreft ICT omgevingen en had u duidelijk uw monitoring en beheer op orde, zodat de eisen te stellen aan een cloud leverancier helder | waren?

- c. Bent u voor een aantal faciliteiten overgegaan naar fase 2? Welke criteria golden voor u bij de keuze van het projectteam voor cloud computing?
 - d. Welke criteria hebt u gehanteerd bij de keuze voor de cloud?
 - e. Op welke criteria is bij u de eerste applicatie gekozen om van de cloud gebruik te maken?
 - f. Heeft u uw eerste ervaringen met cloud computing geëvalueerd? Zo ja, wat was uw conclusie?
 - g. Was er zicht op de extra interne en externe deskundigheid nodig om te komen tot cloudcomputing? Zoja, waar had uw organisatie extra deskundigheid nodig en was die beschikbaar op de markt? Waar?
3. Heeft u een cloud computing roadmap? Wat staat in deze roadmap?
- bv. - de wijze van implementatie van cloud services, zoals de te leveren business case; de implementatie plannen; de integratie van de cloud applicatie met eigen applicaties, de nodige administratieve organisatie, waaronder de rapportages en monitoring; de in te richten eigen organisatie en haar skills etc.
 - mogelijke diensten welke van een cloud kunnen worden afgenomen;
 - mogelijke diensten welke niet van een cloud kunnen worden afgenomen etc.
 - een tijdsframe voor verdere roll-out van cloud services.

E. HET WERKEN MET OUTSOURCING.

De vragen over werken met cloud computing zijn onderverdeeld in de vijf onderdelen

- E.1. Organisatie (van beheer rondom cloud computing),
- E.2. Sturing (van de kwaliteit van diensten bij de leverancier),
- E.3. Informatie (over de performance van de cloud vanuit de leverancier van de diensten),
- E.4. Maatregelen (genomen door leverancier en inzicht hierin)
- E.5. Auditen (bij klant en leverancier)

E.1. ORGANISATIE.

Afhankelijk van de soort service (SaaS, PaaS en/of IaaS), die men uit de cloud afneemt, zouden bij de cloud leverancier de standaard operationele beheer processen (en bijbehorende activiteiten) aanwezig kunnen/moeten zijn. Denk hierbij aan een Service Desk, continuïteitsbeheer, incidentbeheer, monitoring etc. Daarnaast zou men in de eigen organisatie kunnen denken aan processen op strategisch en tactisch niveau:

- a. op strategisch niveau:
 - bijhouden van de **portfolio** aan cloud services en de technologie;
 - kijken hoe men met de organisatie van de informatievoorziening intern omgaat en welke **eisen** dat stelt aan de leverancier van cloud services;
- b. op tactisch niveau als:
 - bijhouden van de **kosten** van cloudsourcing en de **planning** van de diensten;
 - **monitoren van de kwaliteit** en bijhouden/sluiten van **contracten** en **SLA's**;

VRAGEN:

1. We onderscheiden private/public SaaS, PaaS en IaaS diensten. Dit leidt tot zes mogelijke cloud diensten. Bij elke mogelijkheid moet men processen inrichten.
 - a. Kunt u aangeven welke operationele processen, zoals boven aangegeven, relevant zijn voor elke soort cloud service waar uw bedrijf mee te maken heeft?
 - b. Kunt u aangeven welke tactische en strategische processen, zoals boven aangegeven, relevant zijn voor elke soort cloud service waar uw bedrijf mee te maken heeft?
2. Als u clouddiensten vergelijkt met niet cloudgebaseerde diensten, stelt u dan dezelfde eisen voor het beheer van de dienst(en) aan zowel interne als externe leverancier(s)? Wat zijn eventuele verschillen? Denk hierbij aan eisen over bijvoorbeeld beschikbaarheid van diensten, vertrouwelijkheid van gegevens, incidentresponse en -afhandeling. Denk ook aan bijhouden portfolio, kwaliteit en contracten.
3. U beseft dat de cloud leverancier tenminste een aantal processen moet hebben ingericht.
 - a. welke van die processen heeft uw leverancier van private clouddiensten ingericht?

- b. welke van die processen heeft uw leverancier van public cloud diensten ingericht?
- c. is het inrichten van deze processen om cloud diensten te leveren naar uw mening voldoende? Zo nee:
 - welke processen zou de private cloud leverancier nog meer moeten inrichten?
 - welke processen zou de public cloud leverancier nog meer moeten inrichten?

E.2. STURING.

- 6. Hoe is de sturing van de interne cloud leverancier ingericht?
 - Is er sprake van een IT governance board, waar alle ICT zaken aan de orde komen? Wie zit in deze board?
 - Is er sprake van accountmanagers met klanten?
 - Zijn er vaste overleggen tussen klant en cloudleverancier? Wat is hun agenda, wie zitten hierin en hoe vaak komen zijn bijeen?
- 7. Hoe is de sturing van de externe cloud leverancier ingericht?
 - Is er sprake van een klantenraad, waar alle ICT zaken aan de orde komen? Wie zit in deze raad?
 - Is er sprake van accountmanagers met klanten?
 - Zijn er vaste overleggen tussen klant en cloudleverancier? Wat is hun agenda, wie zitten hierin en hoe vaak komen zijn bijeen?

E.3. INFORMATIE.

- 8. Hoe rapporteert de cloud leverancier over zijn dienstverlening?
 - is er transparantie over operationele zaken als beschikbaarheid, incidenten tav. de vertrouwelijkheid en integriteit?
 - zijn de financiële zaken transparant? Is er inzicht in kostenopbouw van de dienstverlening?
 - wat is de frequentie van rapportages?
 - heeft u de mening dat u op tijd inzicht heeft in problemen tav. beschikbaarheid, incidenten tav. de vertrouwelijkheid en integriteit?
- 9. Heeft u de mogelijkheid om inzage te krijgen in eventuele auditrapportages op het functioneren van de cloud? Zo ja, wordt u actief geïnformeerd, dat deze er zijn? Indien beschikbaar, wat is hun kwaliteit? Komt deze overeen met de eisen, die u vanuit uw eigen organisatie eraan moet stellen?
- 10. Heeft u inzicht in het beleid van de cloudleverancier tav.:
 - de beschikbaarheid van ICT voorzieningen en het wegnemen van bottlenecks hierin?
 - de bescherming van de vertrouwelijkheid van gegevens en het wegnemen van bottlenecks hierin, voorzover door hen mogelijk?
 - de bescherming van de integriteit van de gegevens en het wegnemen van bottlenecks hierin, voorzover door hen mogelijk?
 Hoe heeft u dit inzicht verkregen en wordt dit inzicht actief geupdated?
- 11. Kunt u on line / real time monitoren:
 - het verkeer van gegevens van, op en naar de cloud;
 - de gegevens op de cloud;
 - het verwerken van gegevens in de cloud;
 - het bewerken van gegevens op de cloud.
 - performance van de cloud (response tijden, throughput, resterende opslagcapaciteit)
 Zijn hier tools voor aanwezig? Welke tools zijn dat? Hoe ziet hun rapportage eruit? Wie levert deze?

E.4. MAATREGELEN.

- 12. Heeft u inzicht in de maatregelen, die de leverancier van cloud diensten genomen heeft om de beschikbaarheid, vertrouwelijkheid en integriteit van uw gegevens te garanderen? Of heeft u zelf

maatregelen genomen om eventuele calamiteiten van een cloudleverancier te voorkomen? (via andere cloudaanbieders of eigen uitwijkmogelijkheden)

13. Worden de in de vorige vraag genoemde maatregelen in samenspraak met u als klant getest, gemonitord en verbeterd?

E.5. AUDIT

In zijn aandachtspunten bij een eventuele audit van clouds aangegeven (vanuit SAS-70, AICPA/CICA Trust Services Principles and Criteria, en de ISO27001). We zullen deze in het volgende doorlopen.

Vragen:

14. Elke audit gaat in op diverse soorten audits.
- welke eisen stelt u aan een audit van uw cloud en/of clouddiensten? Eist u een SAS-70 verklaring? Eist u een trust verklaring? Eist u een ISO 27000 certificatie? Wat is de achtergrond hiervan?
 - welke eisen stelt u aan de focus van een audit? Systemen en beheersmaatregelen, alleen beheersmaatregelen of de zekerheid dat er een 27001 organisatie is?
 - Wat is de frequentie van de audit?
 - Sommige audits gaan niet in op continuïteitsbeheer (= door kunnen gaan bij uitval). Stelt u dus aanvullende eisen op een SAS-70 verklaring? En welke zijn dit?
15. Er bestaat voor auditing van clouds en clouddiensten een specifieke norm. Dit is de NIST 800-53 R3. Dan worden er vragen gesteld als in figuur 7. aangegeven (www.cloudaudit.org). Maakt uw organisatie gebruik van de mogelijkheden van een dergelijke standaard (die toegespitst is op clouddiensten) om uw cloud of clouddienst te auditen? En zo ja hoe? Zo nee, gebruikt u een alternatieve manier?

F. HET BEEINDIGEN VAN EEN CLOUDDIENST.

De vragen in dit onderdeel gaan over mogelijkheden voor het verplaatsen, veranderen of beëindigen van clouddiensten bij een leverancier. De vragen zijn onderverdeeld naar twee onderdelen: F.1. Contractuele aspecten en F.2. Technische aspecten

F.1. CONTRACTUELE ASPECTEN.

- Uw cloud diensten worden afgenomen met als basis:
 - voor private clouds een SLA;
 - voor public clouds en cloudservices: een contract met een SLA.
 Is deze situatie juist? Zo nee, hoe is deze anders?
- Kijkende naar beëindiging van de afname van de cloud of clouddiensten: zijn hier in de SLA of het contract bepalingen over opgenomen/verschillende deze bepalingen wat betreft:
 - private of public clouds?
 - Saas, Paas of Iaas diensten?
 - wat zijn deze verschillen? En wat houden ze in?
 - betreffen deze de duur van de overeenkomst?
 - betreffen deze de verplichtingen van de cloudleverancier om programma's en/of gegevens terug te geven of te verwijderen?
 - betreffen deze de verplichtingen van de cloudleverancier om de documentatie over programma's en/of gegevens te geven?
 - betreffen deze de verplichtingen van de cloudleverancier om aan de beëindiging en eventuele overdracht van programma's en gegevens aan een derde mee te werken?
 - betreffen deze een check, eventueel door een derde, of alle programma's en/of gegevens verwijderd zijn?

F.2. TECHNISCHE ASPECTEN.

3. Kunt u technisch gezien uw van de cloud afgenomen diensten eenvoudig verplaatsen? Zo ja, waarom? Zo nee, waarom niet?
4. Welke standaards gebruikt uw cloud leverancier, welke verplaatsen eenvoudiger mogelijk maakt? Bv. qua operating systeem, qua documentatie etc.
5. Moet u uw gegevens converteren, als u de cloud leverancier verlaat? Hoe zeker bent u ervan dat deze conversie correct verloopt? Of dat u alle gegevens, die u nu heeft, gaat converteren of hebt geconverteerd? Waarom?
6. Als u uw gegevens verwijdert, hoe zeker bent u dan alle gegevens verwijderd zijn? Waarom? Welke acties moet u extra uitvoeren om hier wat zeker van te zijn?

G. IMPACT VAN CLOUD COMPUTING.

Fingar (2009) geeft aan dat organisaties door het implementeren van cloud technologie kunnen veranderen. Hij spreekt van een overgang van een 1.0 organisatie naar een Organisatie 2.0. In feite spreekt hij over de mogelijkheden van cloud computing in het algemeen op een organisatie. Daarnaast komt de mogelijke organisatieverandering door:

- het afstoten van (delen van) de oude rekencentrum organisatie;
- het opbouwen van een organisatie nodig om de leverancier(s) van de cloud | services aan te sturen/te monitoren.

Organisatie 1.0	Organisatie 2.0
Kent hiërarchie	Is platter
Kent fricties in afstemming	Gestroomlijnde processen
IT-gedreven technologie inzet	Gebruikers gedreven inzet
Teams op één plaats aanwezig	Teams wereldwijd & 24*7
Informatiesystemen zijn voor gestructureerde informatie	Ook sociale platformen.
Proprietary standaarden	Meer open standaarden
Gepland	On demand werken
Lange time to market	Korte time to market
Informatie op need to know basis	Uitgangspunt transparante informatievoorziening.

De vragen zijn:

1. Is er een positieve impact aan te geven op de organisatie door het gebruik van cloud services:
 - a. Wat is de impact geweest van het invoeren van SaaS op de organisatie? Men denke hierbij bijvoorbeeld aan:
 - het gebruiken van mailservices extern kan leiden tot minder spam, betere beschikbaarheid van het netwerk wereldwijd en zo tot een organisatie, die meer van ICT gebruik maakt;
 - het gebruiken van standaardpakketten eist het invoeren van standaard werkwijzen over de hele organisatie heen. Hierdoor is het mogelijk geworden eerder informatie centraal te consolideren, beter centraal te sturen. Men denke hierbij bijvoorbeeld aan het invoeren van SAP wereldwijd door Accenture.
 - het gebruiken van Salesforce belooft een kortere time to market van CRM toepassingen, waardoor eerder en beter op klanteninformatie kan worden gestuurd.
 - standaards in het bedrijf wereldwijd maakt het werken met teams en hun ondersteunende platforms 7*24 uur mogelijk. Men denke aan het gebruik van sociale platforms door de MSD;
 - b. Wat is de impact geweest van het invoeren van PaaS op de organisatie? Men denke hierbij aan:
 - het gebruiken van platformapplicaties, welke men kan parametriseren, leidt ertoe, dat men zelf geen exploitatiediensten heeft, en ook geen maatwerkdienst. Men kan standaardfaciliteiten inrichten door gebruikersorganisaties, welke daarvoor een centraal coördinatiepunt hebben ingericht;

- het hebben van Microsoft Azure maakt het gebruik van MS applicaties mogelijk zonder te hoeven denken aan installatie en bijhouden van updates. Voorts is steeds managementinformatie over het gebruik van het platform aanwezig. Het maakt de ICT-organisatie transparanter.
 - men wil videoconferencing en gebruikt het platform van Surf, waarbij men een gegeven faciliteit parametrizeert en van de participanten de gegevens invoert en in staat is on line te overleggen.
- c. Wat is de impact geweest van het invoeren van laas op de organisatie? Men denke hierbij bijvoorbeeld aan:
- men heeft piekcapaciteit nodig om een archief te converteren en gebruikt hiervoor de mogelijkheden van Amazon E2. New York times deed dit met zijn oude archief van de 1920's. Snel waren de computerfaciliteiten aanwezig, snel het programma geschreven en binnen 24 uur was de conversie gedaan. Men werkte gewoon on demand.
2. De eigen ICT organisatie kan veranderen door het afnemen van cloud diensten. Hierbij onderscheiden we meerdere situaties:
- eigen exploitatiediensten worden in de cloud gezet;
 - een deel van de eigen exploitatiediensten worden in de cloud gezet;
 - nieuwe diensten worden via de cloud afgenomen.
- a. Kunt u aangeven, of en welke situaties bij uw organisatie optreden?
- b. Kunt u per onderdeel aangeven of dit positieve danwel negatieve affecten heeft gehad op de kwaliteit van de exploitatiediensten. Denk hierbij in ieder geval aan exploitatiekosten, dagelijkse ondersteuning, performance, mogelijkheden, benodigde skills, operationele taken van de eigen ICT organisatie, gebruik van testomgeving/teststraat, kwaliteitszorg, ontwikkelproces ICT veranderingen, data intelligence mogelijkheden.
- c. Kunt u aangeven, welke cloudservice (SaaS, PaaS, IaaS) het grootste effect had en waarom? Kunt u dit effect ook in baten/kosten aangeven?

BRONNEN.

1. Donkers, M. : *De verandering in de ICT organisatie van kleine en middelgrote organisaties door het gebruik van Cloudcomputing*, scriptie, Open Universiteit, Heerlen, 2011.
2. Fingar, P.: *dot.cloud, the 21^{ste} century business platform*, Meghan-Kiffer press, Tampa, 2009.
3. Greer, M. B. (2009). *Software as a Service inflection point : using Cloud computing to achieve business agility*. New York; Bloomington, IN: iUniverse, Inc.
4. Greer jr., Melvin B.: *Software as a service inflection point*, iUniverse, Bloomington, 2009
5. Lute, E. (Eindredactie): *Over cloud computing, waarom een taxi kopen, als je alleen vervoer nodig hebt?*, TIEM, Baarn, 2009.
6. Mell, P., & Grance, T. (2009a). The NIST Definition of Cloud Computing. Retrieved 29 November 2010, from <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
7. Mell, P., & Grance, T. (2009b). Effectively and Securely Using the Cloud Computing Paradigm. Retrieved 12 December 2010, from <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt>

