De mkb-accountant en Cloud Computing

NBA

November 2014

De tekst van deze brochure is tot stand gekomen met medewerking van NEMACC, het mkb kenniscentrum waarin NBA en de Erasmus Universiteit Rotterdam hun expertise bundelen, en met medewerking van NOREA.

Inhoudsopgave

Voorwoord

Voor de mkb-ondernemer vervult u als accountant een belangrijke rol. U komt regelmatig bij hem over de vloer en kent zijn bedrijf in financieel opzicht van binnen en van buiten. Uw brede kennis en ervaring maakt dat de mkb-ondernemer u ziet als een belangrijke adviseur, en dat niet alleen op financieel gebied. Ook op veel andere terreinen bent u voor hem het eerste aanspreekpunt.

Cloud Computing zou zo'n ander terrein kunnen zijn. Wordt u door uw klant over dit onderwerp geraadpleegd, of treft u bij uw klant een of meerdere Cloud-toepassingen aan, dan is het belangrijk dat u over voldoende deskundigheid beschikt. En dat u weet waar uw beperkingen liggen, zodat u op dat gebied naar anderen kunt doorverwijzen. Deze NBA brochure biedt u een kader waarmee u vragen omtrent Cloud Computing tegemoet kunt treden. De ontwikkelingen op dit gebied gaan snel. Het is daarom van belang uw kennis op dit gebied op peil te (blijven) houden. Deze brochure is daar een goed startpunt voor.

Risico's

Cloud Computing is niet nieuw en het is ook geen rocket science. Het is wel een onderwerp dat op dit moment veel aandacht krijgt. Als mkb-accountant heeft u hier mogelijk ook al vragen over gekregen van uw klanten. Daarnaast maakt u wellicht ook zelf al in meerdere of mindere mate gebruik van Cloud Computing om uw eigen bedrijfsprocessen te ondersteunen. Of wellicht biedt u via uw kantoor vormen van Cloud Computing aan uw klanten aan.

Eén ding is zeker: ook Cloud Computing kent, naast de voordelen die het kan opleveren voor u en uw klanten, ook risico's. En ongeacht het feit of u een advies-, samenstellings-, beoordelings- of controleopdracht uitvoert, is het verstandig dat u enig begrip heeft van de belangrijkste risico's van Cloud Computing. Daarbij is het handig dat u de risico's voor uzelf of voor uw klant ook in enige mate kunt wegen.

Cloud Computing geen doel

Cloud computing is nooit doel op zich. Cloud computing helpt u of uw klanten hun bedrijfsdoelen te behalen. De risico's die Cloud Computing met zich brengt, kunnen er dus toe leiden dat de bedrijfsdoelen niet worden bereikt. De met Cloud Computing verbonden bedrijfsrisico's vragen dan ook om beheersingsmaatregelen om de risico's te beperken of weg te nemen. Die risico's zijn onder meer afhankelijk van de soort Clouddienst, de vorm waarin deze wordt aangeboden en de kwaliteit van de betreffende Clouddienst.

Bring Your Own Device (BYOD)

Het internet maakt het mogelijk dat gebruikers met eigen laptops, smartphones en tablets en vanaf elke locatie in de Cloud kunnen werken. Dit levert ook risico's op. Denk bijvoorbeeld aan gezinsleden die gebruikmaken van diezelfde laptop, smartphone of tablet en daardoor misschien onbedoeld ook toegang hebben tot de bedrijfsapplicaties. Om veilig te kunnen werken in de Cloud, is het noodzakelijk dat er bijvoorbeeld gebruik wordt gemaakt van wachtwoorden en dat er heldere en concrete afspraken worden gemaakt (en vastgelegd) om te voorkomen dat anderen kunnen beschikken over deze wachtwoorden.

Beheersing van risico's door de aanbieder van Clouddiensten

Wanneer gebruik gemaakt wordt van de Cloud zal de beheersing van bedrijfsrisico's deels geschieden door de organisatie die gebruikmaakt van de diensten. Maar ook de aanbieder van de Clouddiensten zal hier voor een deel aan kunnen bijdragen. Middels een zogenaamd assurance-rapport kunnen aanbieders zekerheid geven met betrekking tot de opzet van hun beheersingsmaatregelen. Een andere mogelijkheid is dat zij de resultaten van een onderzoek naar de opzet, het bestaan en de werking van hun interne beheersing in een assurance-rapport laten weergeven. Tevens worden ISO-certificeringen gehanteerd en is het keurmerk 'Zeker-Online' in de markt gezet.

Opdracht heeft invloed op benodigde kennis

De kennis die u nodig heeft van Cloud Computing is mede afhankelijk van de opdracht die u heeft gekregen van uw klant. Wanneer u bijvoorbeeld controlewerkzaamheden uitvoert voor uw klant, zult u (in het kader van uw kennis van de huishouding) inzicht moeten hebben in de manier waarop Cloud Computing onderdeel uitmaakt van de business van uw klant. Schiet uw expertise bij een opdracht tekort, dan kunt u een IT-auditor of andere expert inschakelen voor bijstand. Voert u een samenstellingsopdracht uit en doet uw klant relatief weinig in de Cloud, dan kunt u doorgaans volstaan met een meer algemene kennis van Cloud Computing. Welke opdracht u ook uitvoert, houdt u in gedachten dat Cloud Computing in de kern een vorm van uitbestede automatisering is en (ten opzichte de andere vormen van automatisering) niet veel nieuwe bedrijfsrisico's met zich brengt.

Kernvragen

Het niveau van de geautomatiseerde informatieverwerking bij uw klanten neemt toe. Daar zult u uw werkzaamheden en adviezen op moeten afstemmen. Om u behulpzaam te zijn bij uw werkzaamheden als mkb-accountant heeft de NBA deze brochure '*De mkb-accountant en Cloud Computing*' voor u geschreven. Hierin krijgt u antwoord op drie kernvragen:

- Wat is Cloud Computing? (zie hoofdstuk 1)
- Waarom is Cloud Computing belangrijk voor mkb-accountants én hun klanten? (zie hoofdstuk 2)
- Welke mogelijke gevolgen heeft Cloud Computing voor mijn beroepspraktijk? (zie de hoofdstukken 3, 4 en 5)

Leeswijzer

Bij het beantwoorden van de drie kernvragen is het bijna onvermijdelijk dat ook een stukje van de techniek aan de orde komt die met Cloud Computing samenhangt. In deze brochure is getracht de nadruk te leggen op de beheersingsorganisatie en de gevolgen voor (de werkzaamheden van) de accountant. De techniek wordt daarbij zo veel mogelijk op de achtergrond geplaatst. De (vak)technische verhandelingen vindt u derhalve met name in de bijlagen. Wilt u helemaal niets van die techniek weten, of beschikt u al over enige kennis met betrekking tot Cloud Computing, start dan met het lezen bij hoofdstuk 2.

Deze brochure verschaft u extra inzicht in Cloud Computing. Gezien de dynamiek op het terrein van Cloud Computing adviseren wij u de actuele ontwikkelingen op dit terrein te blijven volgen en u niet uitsluitend te baseren op de informatie uit deze brochure.

01 | Wat is Cloud Computing?

Cloud Computing is niets anders dan een aanduiding voor het op aanvraag via internet beschikbaar stellen van hardware, software en data aan gebruikers. Waar bedrijven vroeger software en hardware in eigen beheer ontwikkelden en aanschaften, maakt Cloud Computing het mogelijk dat de gebruiker naar behoefte functionaliteit en capaciteit kan afnemen, zonder dat hij daar zelf voor hoeft te investeren of deze hoeft te onderhouden. Door de combinatie van al bestaande technieken en toepassingen zijn er nieuwe dienstconcepten en toepassingsmodellen ontwikkeld. De belangrijkste technology drivers hiervoor zijn internet en de toegang tot applicaties via apps en mobiele apparatuur, zoals laptops, tablets en smartphones. De toegenomen opslag-, verwerkings- en transportcapaciteit heeft dit extra gestimuleerd. Deze technology drivers maakten het mogelijk nieuwe businessmodellen te ontwikkelen.

Kenmerken Cloud Computing

De kenmerken van Cloud Computing zijn als volgt worden weer te geven:

- toegang tot applicatie en data kan alleen met een internetverbinding;
- gebruikers delen bronnen (bijvoorbeeld opslagruimte, rekencapaciteit, servers) met elkaar;
- de omgeving is naar rato van de gebruikersbehoefte flexibel op te schalen of in te krimpen;
- er is sprake van een hoge mate van zelfbediening in het beheer;
- de dienstverlening vindt plaats onder strikt gemonitorde en beveiligde condities;
- afrekenmodellen gaan uit van betaling naar gebruik en verbruik in plaats van betaling voor eigendom.

1.1 Dienstconcepten Cloud Computing

Er worden verschillende dienstconcepten of servicemodellen aangeboden door dienstverleners, waarvan wij er hier vier beschrijven.

In het eenvoudigste model kan de gebruiker beschikken over servers, data-opslag etc. die eigendom zijn van een serviceprovider. De gebruiker betaalt alleen voor hetgeen daadwerkelijk gebruikt wordt. Dit model wordt aangeduid met de naam ‘Infrastructure as a service’ (IaaS). De gebruiker moet de infrastructuur vervolgens zelf voorzien van bijvoorbeeld een operating systeem, een databasemanagementsysteem en eigen applicaties.

Het tweede dienstconcept draagt de naam ‘Platform as a service’ (PaaS). Hierbij heeft de dienstverlener al een deel van de inrichting verzorgd, bijvoorbeeld door te kiezen voor het operating systeem en voor het datamanagementsysteem en de ontwikkeltools. De gebruiker kan echter zijn eigen applicaties installeren of ontwikkelen.

Het derde dienstconcept is 'Software as a service' (SaaS). Hierbij krijgt de gebruiker een door de dienstverlener onderhouden softwaretoepassing tot zijn beschikking. De gebruiker kan hier zijn bedrijfsactiviteiten in verwerken.

Het laatste dienstconcept dat wij hier beschrijven is Business Process as a Service (BPaaS). Bij dit dienstconcept wordt (een deel van) een bedrijfsproces aangeboden.

De genoemde dienstconcepten worden nader uitgewerkt in bijlage 1.

1.2 Toepassingsmodellen Cloud Computing

De hiervoor besproken dienstconcepten kunnen op verschillende manieren worden toegepast. Hiervoor staan vier toepassingsmodellen ter beschikking: de Public Cloud (voor iedereen toegankelijk), een Private Cloud (voor één gebruiker), een Hybride Cloud (een combinatie tussen de eerste twee) of een Community Cloud (voor een specifieke groep gebruikers). Een korte toelichting op deze toepassingsmodellen staat in bijlage 2.

1.3 Samenwerkende aanbieders Clouddiensten

De diverse aanbieders van Clouddiensten werken veel samen. Zo maken veel aanbieders van SaaS- en PaaS-diensten voor hun verwerking en opslag gebruik van IaaS-aanbieders. Exact Online, Reeleezee en Open Text Cordys maken voor hun opslag en verwerking onder meer gebruik van de diensten van de IaaS-aanbieders Rackspace en Amazon. IaaS-aanbieders werken op hun beurt voor de opslag en verwerking van data dikwijls samen met elkaar. Dit doen zij vooral om tijdelijke pieken in het gebruik van verwerking en/of opslag van data te kunnen opvangen.

De gebruiker weet vaak niet welke organisatie zijn data verwerkt c.q. opslaat en wat de mogelijke consequenties daarvan zijn. In de Verenigde Staten bijvoorbeeld maakt de Patriot Act het mogelijk dat de Amerikaanse overheid inzage heeft in verwerkte en/of opgeslagen data van gebruikers. In andere jurisdicties geldt mogelijk vergelijkbare wetgeving of is wetgeving niet duidelijk.

Maakt uw klant gebruik van Clouddiensten of wil hij dat op korte termijn gaan doen? In dat geval is het goed dat uw klant zich bewust is van het voorgaande zodat hij kan bepalen hoe hij met deze risico's wil omgaan (zie hoofdstuk 2).

1.4 Architectuurmodellen Cloud Computing

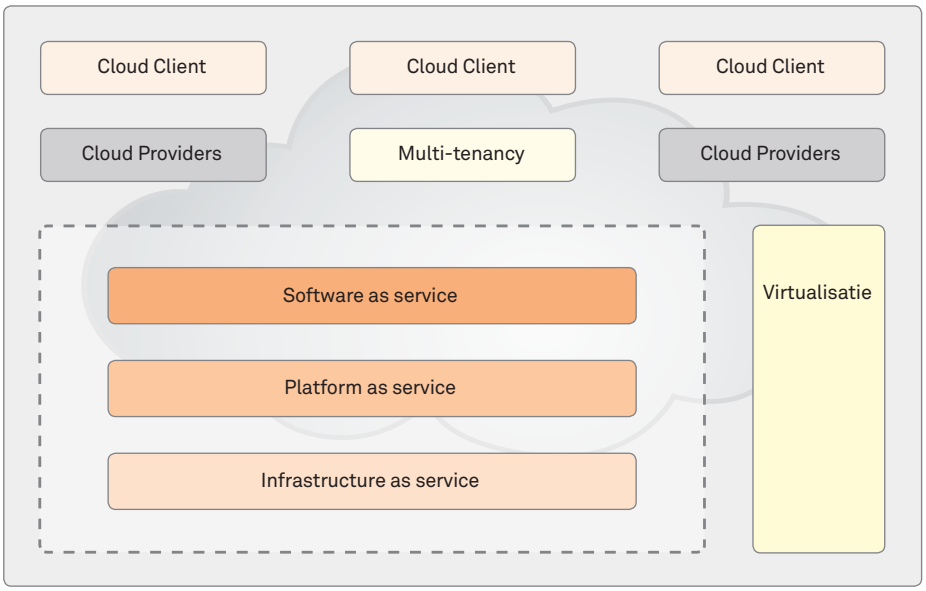
Een veelheid aan Clouddiensten is voortgekomen vanuit het basismodel voor geautomatiseerde informatieverwerking. Elke geautomatiseerde informatieverwerkingseenheid bestaat uit een computer (ook wel server) waarop gegevens worden bewerkt en opgeslagen met behulp van een programma. De Clouddiensten maken gebruik van een onderliggende infrastructuur, die complex kan worden door toepassingen te combineren. In bijlage 3 wordt hier nader aandacht aan besteed.

Gevolgen Cloudarchitectuurmodellen

De typen Clouddiensten die Clouddienstaanbieders leveren, in combinatie met het (al dan niet) gebruikmaken van multi-tenancy[1], virtualisatie[2] en verschillende locaties, vormen samen een Cloud Computing Architectuur. Een basismodel van Cloud Computing Architectuur ziet er als volgt uit (zie figuur 1).

1 Multi-tenancy: meerdere gebruikers die gebruikmaken van dezelfde omgeving en applicaties.
2 Virtualisatie: het softwarematig simuleren van meerdere omgevingen op één computer.

Figuur 1: Basismodel Cloud Computing Architectuur



Dankzij virtualisatie en multi-tenancy kunnen cloudgebruikers dezelfde toepassingssoftware gebruiken, dezelfde databases en dezelfde hardware. Dit brengt risico's met zich mee. Om die reden zijn interne beheersingsmaatregelen nodig die datavermenging van individuele gebruikers tegengaan en integere verwerking en dataopslag waarborgen.

In bijlage 3 wordt meer in detail ingegaan op bepaalde aspecten van de architectuur.

02 | Risico's bij Cloud Computing

Cloud Computing brengt op zich niet veel nieuwe bedrijfsrisico's met zich mee. Veel bedrijfsrisico's bestaan op dit moment ook al bij het gebruik van automatisering in eigen huis of bij uitbesteding aan een derde partij. Belangrijk kenmerk van Clouddiensten is dat een derde partij deze aanbiedt en dat de gebruiker zelf directe invloed heeft op de inhoud en de kwaliteit van de dienst(verlening) inclusief de interne beheersing. Die invloed kan de gebruiker uitoefenen door te kiezen voor een bepaald dienstconcept (IaaS, PaaS, SaaS of BPaas) en een bepaald toepassingsmodel (Public, Private, Hybride of Community Cloud).

2.1 Soorten bedrijfsrisico's

Mkb-ondernemers realiseren zich in de praktijk vaak niet voldoende welke bedrijfsrisico's zij lopen als gevolg van de automatisering in het algemeen en Cloud Computing in het bijzonder. Deze organisaties zijn vaak ook niet groot genoeg om een gespecialiseerde afdeling te hebben die de automatisering kan regelen en onderhouden en die zich kan verdiepen in de bedrijfsrisico's.

Bij bedrijfsrisico's moet u denken aan een inbreuk op de beschikbaarheid en continuïteit, de integriteit en vertrouwelijkheid van data en processen en aan compliance. Maar ook aan aansprakelijkheidsrisico's op basis van de wet computercriminaliteit en de privacywetgeving. Omdat de Cloud zich doorgaans ook tot buiten de eigen landsgrenzen uitstrekt, kan de wet- en regelgeving van andere landen van toepassing worden. Gaat het mis, dan kan er politieke, financiële, juridische, operationele of imagoschade ontstaan. Een risicoanalyse moet daarom inzicht geven in de bedreigingen, de kansen op schade en de mogelijke omvang daarvan alsmede in de risk appetite[3].

Bijlage 4 geeft voorbeelden van bedrijfsrisico's die kunnen ontstaan als gevolg van Cloud Computing.

2.2 Interne beheersing

Een stelsel van interne controlemaatregelen en procedures bij de Clouddienstaanbieder en bij de gebruiker is noodzakelijk om de inherente bedrijfsrisico's, verbonden aan het gebruik van Cloud Computing, terug te brengen tot een aanvaardbaar niveau voor de gebruiker.

Bij een Public Cloud geldt dat hoe uitgebreider het dienstniveau van de Clouddienstaanbieder is, hoe beperkter de mogelijkheden van de gebruiker zijn om de Clouddienst intern te beheersen.

3 Risk appetite: de bereidheid van een onderneming om een risico van een bepaalde (afgebakende) omvang zelf te lopen.

Een Private of Community Cloud biedt aanbieders en gebruikers de mogelijkheid om concrete afspraken te maken over de invulling van de Clouddienst, waaronder de interne beheersing en de verantwoording daarover. Bijvoorbeeld over de manier waarop de dienst feitelijk wordt ingevuld, waar verwerking en opslag plaatsvindt, hoe de toegangsbeveiliging geregeld is en wie daarvoor verantwoordelijk is. Ook kunnen afspraken worden gemaakt over de mogelijkheid om specifieke wet- en regelgeving na te leven, zoals privacy- en fiscale regelgeving. Afspraken over de interne beheersing en verantwoording daarover, inclusief vormen van externe toetsing door een onafhankelijke deskundige of de auditor van de gebruiker(s), horen daar ook bij. De afspraken worden vastgelegd in een contract en een SLA (Service Level Agreement), waarin de operationele afspraken staan beschreven.

Clouddienstaanbieders besteden vaak veel aandacht aan hun interne beheersing. Zij hebben veelal een 'Control Framework' (beheersingskader) ingericht, waarin staat hoe zij de kwaliteit van hun dienstverlening borgen en de interne beheersing daarvan. Sommige aanbieders laten de kwaliteit van hun dienstverlening en interne beheersing periodiek beoordelen door externe onafhankelijke auditors en verstrekken gebruikers een certificaat of een assurance-rapport. Ook is het mogelijk dat zij de auditors van gebruikers toestaan om zelf de kwaliteit van dienstverlening en interne beheersing te onderzoeken ('Right to audit').

2.3 Bring Your Own Device

Snelle technologische ontwikkelingen, Cloud Computing en lagere prijzen voor mobiele apparaten hebben het gebruik en bezit van laptops, smartphones en tablets flink gestimuleerd. Medewerkers nemen daardoor steeds vaker hun eigen apparatuur mee naar hun werkomgeving om deze daar te gebruiken. Deze trend - Bring Your Own Device (BYOD) - maakt het mogelijk dat werknemers via hun eigen mobiele apparatuur verbinding kunnen maken met het bedrijfsnetwerk. Hierdoor kunnen zij ook rechtstreeks toegang krijgen tot bepaalde bedrijfsapplicaties, -gegevens en -resources, zoals e mail, fileservers, databases en intranet. BYOD brengt ook bedrijfsrisico's met zich mee.

Mobiele apparaten bieden gebruikers via apps toegang tot een veelheid aan diensten. Maar welke activiteiten een app op een mobiel apparaat uitvoert, en met welke data, is niet altijd duidelijk. Apps kunnen dus gewoon toegang hebben tot data die op een mobiel apparaat zijn opgeslagen (contactpersonen, e-mails, databestanden, foto's, etc.). Daarnaast slaan gebruikers van mobiele apparaten vaak automatisch de op hun mobiele apparaat opgeslagen data als back-up op in de Cloud (de iCloud van Apple, SkyDrive van Microsoft of Google Drive van Google).

Maatregelen gewenst

Bedrijfsgegevens kunnen via mobiele apparaten buiten de beveiliging en beheersing van de organisatie komen. Dit kan de vertrouwelijkheid en integriteit van de data aantasten. Het is bijvoorbeeld mogelijk dat derden (of apps!) zakelijke e-mail kunnen lezen die via een mobiel apparaat kan worden benaderd of daarop zelfs is opgeslagen. Hiermee kunnen de belangen van het bedrijf ernstig worden geschaad. Om nog maar niet te spreken over de eventuele gevolgen van het verlies of de diefstal van een mobiel apparaat, dat toegang geeft tot het bedrijfsnetwerk of zakelijke Cloudtoepassingen en/of waarop ook zakelijke data zijn opgeslagen. Organisaties moeten daarom maatregelen nemen om BYOD veilig te laten plaatsvinden. Idealiter wordt een BYOD-regeling opgesteld waarin concreet vermeld wordt:

- welke mobiele apparaten zijn toegestaan;
- of werknemers alle apps mogen gebruiken of slechts een select aantal;
- welke toepassingen en websites niet gebruikt mogen worden (bijvoorbeeld Dropbox voor tijdelijk opslaan van data en uitwisseling van data met derden).

Aanmelding bij - en registratie door - de werkgever van privéapparaten die ook zakelijk mogen worden gebruikt, in combinatie met een Mobile Device Managementsysteem (MDM), is een oplossing. Hierdoor kunnen de zakelijke en privé-omgevingen worden gescheiden en kan er zakelijk alleen worden gewerkt met de apps die de werkgever toestaat of mogelijk zelf verstrekt. Een aantal accountantskantoren gebruikt deze mogelijkheid om onder meer de vertrouwelijkheid van klantgegevens te kunnen waarborgen.

03 | Gevolgen voor samenstellings-, beoordelings- en controleopdrachten

In hoofdstuk 1 en 2 is toegelicht wat Cloud Computing is en welke dienstconcepten en toepassingsmodellen er worden gebruikt. Daarbij zijn ook de mogelijke bedrijfsrisico's betrokken. In dit hoofdstuk leggen we de link naar uw dagelijkse praktijk. Wat zijn de mogelijke gevolgen van Cloud Computing als u een samenstellings-, beoordelings- of controle-opdracht uitvoert?

Welke opdracht u als accountant ook uitvoert, u bent niet verantwoordelijk voor de betrouwbare gegevensverwerking van uw klant. Het management van de onderneming is hiervoor verantwoordelijk. Afhankelijk van uw opdracht zult u wel in meer of mindere mate aandacht besteden aan de manier waarop de ondernemer gebruikmaakt van Cloud Computing. Ook kunt u, vanuit uw natuurlijke adviesfunctie en op basis van tijdens de opdracht verkregen kennis, voor uw klant een signalerende functie hebben als het gaat om bedrijfsrisico's als gevolg van Cloud Computing.

Bij samenstellingsopdrachten verricht u geen onderzoek naar het stelsel van interne beheersingsmaatregelen. Bij beoordelings- en controleopdrachten is dit onderzoek qua omvang en diepgang doorgaans beperkt. Dit houdt in dat u zich over de getroffen beheersingsmaatregelen (ook ten aanzien van de automatisering) doorgaans niet zult uitspreken, of slechts met een beperkte mate van zekerheid.

3.1 Gevolgen voor een samenstellingsopdracht

Een samenstellingsopdracht op basis van NV COS Standaard 4410 is de opdracht waarbij de ondernemer zijn accountant vraagt hem te ondersteunen bij het opstellen en presenteren van historische financiële informatie (bijvoorbeeld een jaarrekening of een SBR-krediet rapportage).

Als accountant hoeft u de nauwkeurigheid en volledigheid van de door het management verstrekte informatie niet te verifiëren. Slechts als u tijdens de opdracht constateert dat de informatie niet compleet, niet nauwkeurig of anderszins niet bevredigend is, zult u moeten vragen om aanvullende informatie. Uit dit oogpunt is het dus niet per definitie nodig om aandacht aan Cloud Computing te besteden.

In het kader van de samenstellingsopdracht wordt van u wel verwacht dat u voldoende inzicht in het administratief systeem en de administratieve vastleggingen heeft om de opdracht te kunnen uitvoeren. In dit kader zult u mogelijk enige aandacht aan de Cloud Computing van uw klant moeten besteden.

Er is echter nog een belangrijke reden waarom u inzicht zou willen hebben in de kwaliteit van de ICT. Dat is de mogelijkheid om uw klant, in het kader van de adviesfunctie, te wijzen op potentiële risico's bij het gebruik van ICT. Als uw klant er prijs op stelt, kunt u hem desgevraagd ondersteunen c.q. adviseren bij het adequaat inrichten van de ICT in zijn bedrijfsvoering.

3.2 Gevolgen voor een beoordelingsopdracht

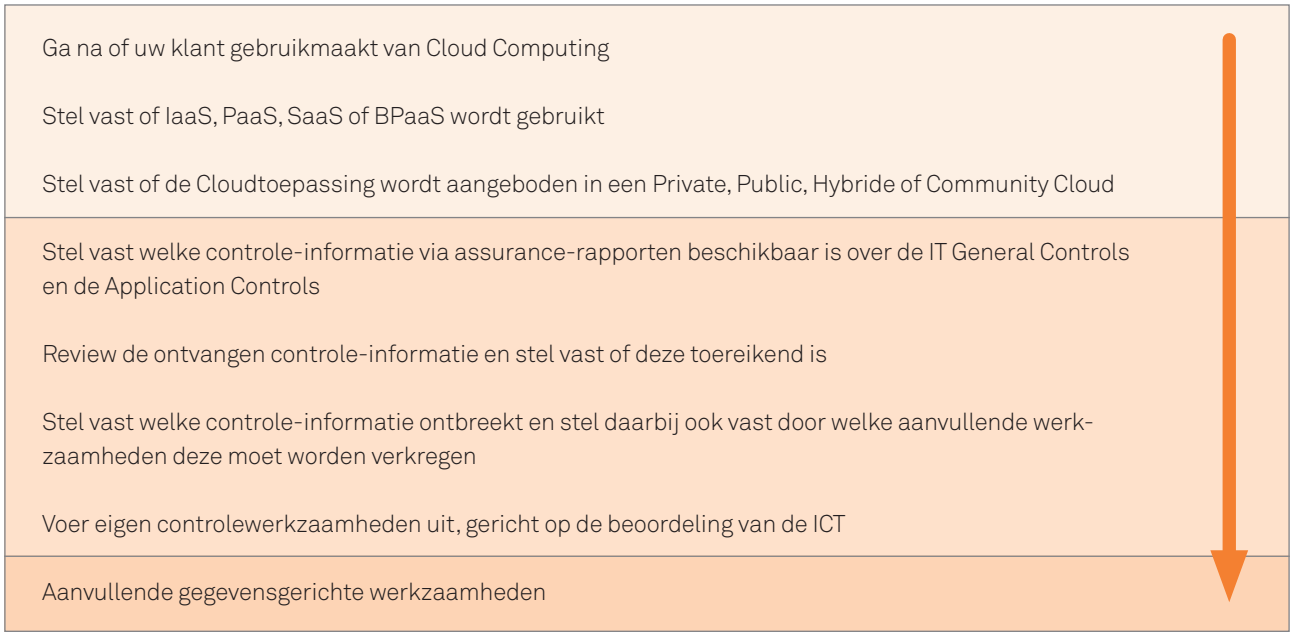
Een beoordelingsopdracht op basis van Standaard 2400 uit de NV COS is een opdracht die een ondernemer geeft aan zijn accountant om - op basis van zijn administratie en de door hem verstrekte gegevens - tot een bepaalde conclusie te komen. Die conclusie behelst voor de accountant te concluderen dat op basis van de uitgevoerde werkzaamheden niets is gebleken op grond waarvan hij zou moeten concluderen dat het financiële overzicht niet is opgesteld in overeenstemming met de van toepassing zijnde grondslagen voor financiële verslaggeving. Om een beoordelingsverklaring te kunnen afgeven, zult u zich conform Standaard 2400 vooral baseren op ingewonnen inlichtingen en uitgevoerde cijferanalyses. De Standaard geeft tevens aan dat u als accountant inzicht dient te hebben in de administratieve systemen en de administratie van uw klant. De standaard gaat daarbij echter niet zo ver dat hij van u verlangt dat u zich verdiept in de ICT en de daarmee verbonden maatregelen voor interne beheersing. Dus ook niet in de wijze waarop uw klant gebruik maakt van Cloud Computing. Tenzij u zich op grond van uw waarnemingen en analyses bewust wordt van de mogelijkheid dat het beoordeelde financiële overzicht een afwijking van materieel belang bevat waarvan de oorzaak (mede) ligt in het gebruik van de Cloud. Op dat moment wordt het wél van belang om kennis te verzamelen omtrent de opzet van de Cloud Computing bij uw klant en de maatregelen voor interne beheersing die daaromtrent zijn getroffen. Om hier inzicht in te krijgen, kunt u gebruikmaken van het beschrevene voor een controleopdracht (zie paragraaf 3.3).

In specifieke branches komt het voor dat u als accountant bij het uitvoeren van een beoordelingsopdracht wordt gevraagd om expliciet aandacht te schenken aan de naleving van wet- en regelgeving die in die branche van belang is. U zult daar dan over moeten rapporteren in uw beoordelingsverklaring. De kwaliteit van de ICT en de daarin opgenomen maatregelen voor interne beheersing kunnen daarbij een onderwerp van beoordeling zijn. Dit bovenstaande heeft niet alleen betrekking op het gebruik van Cloud Computing, maar geldt in algemene zin voor het gebruik van ICT.

3.3 Gevolgen voor een controleopdracht

De bedrijfsrisico's bij Cloud Computing zijn niet anders dan de bedrijfsrisico's bij de huidige, andere vormen van automatisering. Wél maakt Cloud Computing per definitie gebruik van de dienstverlening van een derde partij en van het internet. Verwerking en/of opslag van data kan daardoor plaatsvinden in een omgeving die met andere gebruikers wordt gedeeld. Dat Clouddiensten vaak ingevuld worden door meerdere partijen is daarbij een mogelijk complicerende factor. De aanbieder en gebruiker zijn - afhankelijk van het dienstconcept en toepassingsmodel - verantwoordelijk voor de invulling van de activiteiten, taken en verantwoordelijkheden. Én voor de hierbij behorende interne beheersingsmaatregelen. Onderstaand wordt een mogelijke aanpak geschetst voor de controle van Cloud Computing (zie figuur 2).

Figuur 2: Controleaanpak bij Cloud Computing



De eerste stap die u hier als accountant moet zetten, is nagaan of uw klant gebruikmaakt van Cloud Computing voor geautomatiseerde processen die gerelateerd zijn aan significante posten in de jaarrekening. Als dat zo is, dan zult u in het kader van uw controle zicht moeten krijgen op de manier waarop uw klant die Clouddiensten feitelijk invult. Kijk daarbij zeker ook naar de verdeling van activiteiten, taken en verantwoordelijkheden en de hierbij behorende interne beheersing. U kunt daarbij mogelijk gebruikmaken van contracten, SLA's of - en dat is met name bij publieke Clouddienstaanbieders het geval - algemene leveringsvoorwaarden.

Aandachtsgebieden bij Cloud Computing

Zoals eerder aangegeven, verschillen de aandachtsgebieden bij Cloud Computing weinig van die bij de huidige vormen van ICT:

- functioneel en technisch beheer en onderhoud van de ICT-infrastructuur;
- changemanagement;
- het systeem van logische en fysieke toegangsbeveiliging, inclusief identificatie en authenticatie van gebruikers;
- het proces van back-up en recovery, met specifieke aandacht voor wat er plaatsgevonden heeft tijdens de controle-periode;
- probleem- en incidentmanagement.

Aanvullende aandacht is echter nodig voor:

- interne beheersingsmaatregelen die gericht zijn op vertrouwelijke en integere informatie-uitwisseling via het internet;
- de manier waarop - en de locatie waar - dataopslag en -bewaring plaatsvinden, inclusief de daarbij behorende waarborgen voor de integriteit van deze data;
- de wijze waarop de integriteit en vertrouwelijkheid van de verwerking en opslag van data gewaarborgd zijn bij gedeeld gebruik (virtualisatie en muti-tenancy).

Nadruk zal dus liggen op het kennisnemen van de dienstverlening bij derden en het beoordelen van de kwaliteit daarvan.

Inschatting controlerisico

Een controle van de jaarrekening wordt uitgevoerd in overeenstemming met de NV COS. Als accountant van uw controleklant zult u moeten kunnen inschatten of er voor u een aanvaardbaar controlerisiconiveau ontstaat. De interne beheersingsmaatregelen bij de Clouddienstaanbieder en bij uw controleklant moeten u daarvoor voldoende aanknopingspunten geven. Wanneer aanvullende gegevensgerichte werkzaamheden nodig zijn, zult u al in een vroeg stadium zeker moeten stellen dat u over de benodigde gegevens (waaronder de transactiedata) kunt beschikken. Hierbij moet u wel vaststellen dat:

- deze gegevens volledig zijn; én
- dat ze voldoende betrouwbaar zijn om uw gegevensgerichte controlewerkzaamheden hierop uit te kunnen voeren.

Wilt u bij de beoordeling van de bedrijfsrisico's en interne beheersingsmaatregelen gebruikmaken van extra guidance voor Cloud Computing? Er zijn meerdere organisaties die deze guidance hebben ontwikkeld, maar belangrijke organisaties die u hiervoor als bron kunt benaderen zijn het Nationaal Cyber Security Centrum (NCSC) en de Information Systems Audit and Control Association (ISACA).

04 | De accountant als gebruiker/aanbieder van Cloud Computing

Voor uw eigen bedrijfsvoering of voor de dienstverlening aan uw klanten kunt u prima gebruikmaken van Cloud Computing. Zo kunt u Clouddiensten inkopen om financiële en personele administraties te ondersteunen, rapportages en aangiftes samen te stellen, om dossiers bij te houden of u kunt een portaal gebruiken om met uw klanten te communiceren.

U zult of uw kantoor zal zorg moeten dragen voor de continuïteit van de bedrijfsvoering. Ook zal voldaan moeten worden aan de verplichtingen die de beroepsuitoefening met zich brengt, zoals het waarborgen van de vertrouwelijkheid van de gegevens van klanten. Integer bewaren van klantgegevens en -dossiers hoort daar ook bij. Treden er problemen op, dan kunt u zich als accountant niet verschuilen achter de Clouddienstaanbieder. U blijft eindverantwoordelijk voor de kwaliteit van de dienstverlening die u, met ondersteuning van een Clouddienst, verricht. U zult dus maatregelen moeten hebben getroffen om deze verantwoordelijkheid te kunnen dragen.

Geeft u uw klanten de gelegenheid om via uw kantoor gebruik te maken van een Clouddienst (bijvoorbeeld voor hun personele en/of financiële administratie)? Ga in dat geval na of deze faciliteit voldoende waarborgen bevat voor een integere en continue gegevensverwerking en gegevensopslag/bewaring.

Let op: Als u als accountant optreedt als aanbieder van Cloud Computing bent u mogelijk, afhankelijk van de afspraken die u maakt met uw klant, aansprakelijk voor schade die ontstaat ten gevolge van fouten in de dienstverlening door de Clouddienstaanbieder. Het is verstandig om de afspraken die u hierover wilt maken met uw klant (en de Clouddienstaanbieder) te laten beoordelen door een deskundige. Besef ook dat problemen in de dienstverlening van de Clouddienstaanbieder uw reputatie kunnen aantasten!

Cloud Computing heeft ook invloed op de personele bezetting binnen uw organisatie. Medewerkers die nu functioneren als server-, systeem en/of netwerkbeheerder zullen in de nieuwe constellatie een aangepaste rol krijgen. Onderhoudswerkzaamheden zullen verminderen, maar ander ICT-werk blijft bestaan. Denk daarbij aan de verwerking van indienst- en uitdiensttredingen, onderhoud en uitgifte van lokale systemen en infrastructuur en aansluitingen van printers en telefoons. Dat betekent dat u als mkb-accountant ook opnieuw over taakverdelingen zult moeten nadenken. Wie doet welke vorm van beheer en waar liggen de functiescheidingen? Ook daar zult u het met elkaar over eens moeten worden.

05 | Hoe kiest uw klant de juiste Clouddienst?

Uw klant kan in voorkomende situaties bij u aankloppen met de vraag of u wilt meedenken over de vraag of hij gebruik zal (gaan) maken van Clouddiensten. Daarbij verlangt hij van u een analyse van de bedrijfsmatige risico's en/of advies.

Stel nu dat u deze vraag concreet krijgt, vindt u zichzelf dan voldoende deskundig om een dergelijke opdracht te aanvaarden? Oordelen over de kwaliteit van aangeboden Clouddiensten kan technische, juridische en/of fiscale deskundigheid vereisen waarover lang niet iedere mkb-accountant beschikt. Met kwaliteit wordt hierbij overigens niet alleen gedoeld op functionaliteit vanuit het oogpunt van bedrijfsvoering, maar ook op de beoordeling van de functionele, technische, en juridische invulling van de Clouddienst. Inclusief de mogelijkheid om te kunnen voldoen aan wet- en regelgeving die relevant is voor de gebruiker.

Strategie eerst

De beslissing om (delen van) de huidige bedrijfsvoering door Cloud Computing te laten ondersteunen, kent strategische, tactische en operationele aspecten. Louter focussen op directe kostenvoordelen is onverstandig, omdat daarbij voorbijgegaan kan worden aan belangrijke strategische vraagstukken. Denk bijvoorbeeld aan de mogelijke gevolgen van:

- (te) grote afhankelijkheid van een of meer Clouddienstaanbieders;
- tegenvallende prestaties van de Clouddienstaanbieder;
- tegenvallende mogelijkheden om door te groeien en de functionaliteit uit te breiden;
- tegenvallende mogelijkheden om bestaande applicaties te koppelen en te integreren,
- het risico van vendor lock-in;
- het opslaan van de data op een onbekende locatie (privacy, bedrijfsspionage);
- geringe betrokkenheid van - en acceptatie door - de eigen medewerkers, verlies aan expertise binnen het eigen bedrijf, etc.

Kortom, eerst hoort een beslissing op strategisch niveau te worden genomen, pas daarna horen de tactische en operationele vraagstukken aan bod te komen. U kunt hierbij als mkb-accountant zeker een toegevoegde waarde hebben, zelfs als uw bijdrage zich zou beperken tot het louter stellen van de juiste vragen.

Verbetering van de bedrijfsvoering, doorgroeimogelijkheden, lagere kosten en meer flexibiliteit door realisatie van schaalvoordelen zijn overwegingen om de bedrijfsvoering (gedeeltelijk) te laten ondersteunen door Cloud Computing. Dit moet worden afgezet tegen de mogelijkheden, maar ook tegen de eventuele bedreigingen, van het gebruik van Cloud Computing. Afgewogen moet worden in hoeverre deze bedreigingen voor de onderneming reëel zijn en welke schade deze kunnen opleveren. De ondernemer moet hiervoor zicht hebben op de eisen die vanuit de eigen bedrijfsvoering gesteld moeten

worden aan Clouddienstverlening. Vervolgens kan via een leveranciersselectie worden bekeken welk dienstconcept en welk toepassingsmodel aan deze eisen tegemoet kunnen komen en welke Cloudaanbieder de desbetreffende Cloud-dienst zou kunnen leveren. Informatie in de vorm van algemene voorwaarden of assurance-rapporten (zie bijlage 5) kan daarbij behulpzaam zijn. Na besluitvorming zullen de afspraken moeten worden vastgelegd in een contract en een SLA.

Een aantal aandachtspunten met betrekking tot de interne beheersing bij Cloud Computing staan uitgewerkt in bijlage 6.

Tip

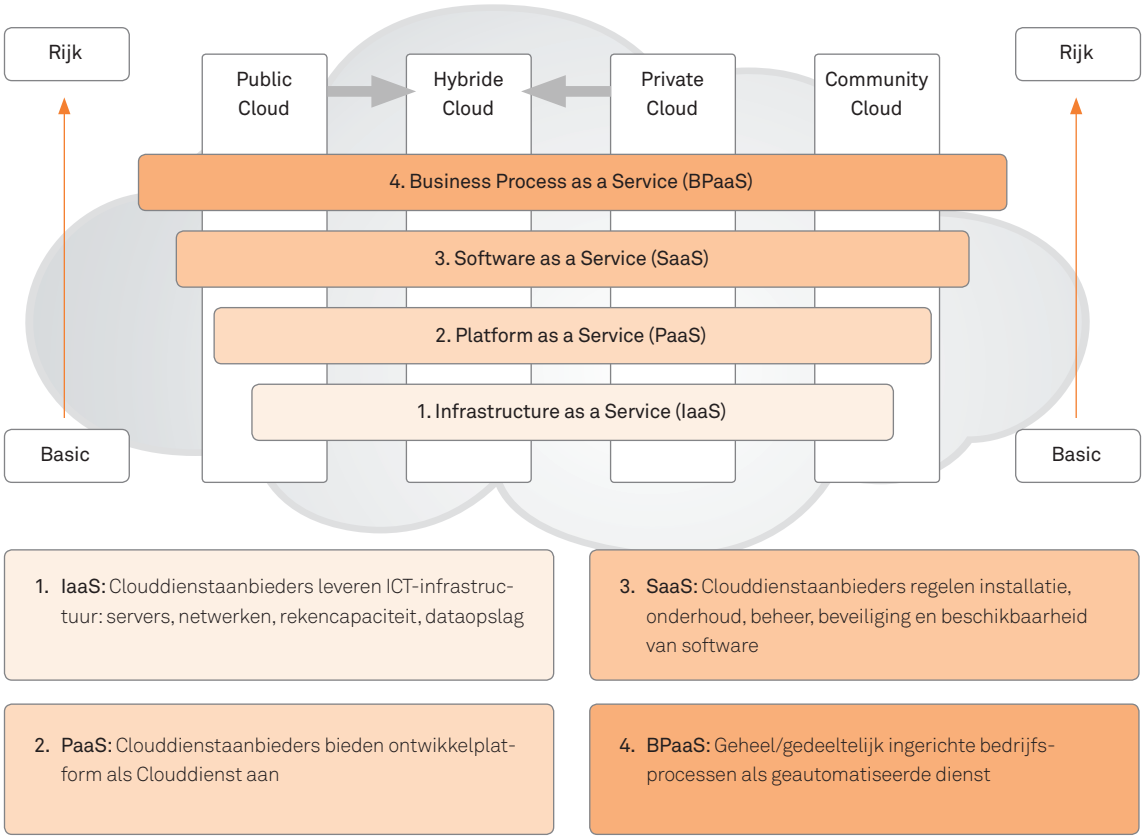
De medio 2013 gelanceerde website **www.cloudbewust.nl** is gericht op het mkb en biedt een overzichtelijk aantal stappen om te kiezen voor een bepaalde Clouddienst. De website is opgezet door ECP en MKB-Nederland met ondersteuning van het Ministerie van Economische Zaken.

Bijlage 1 | Dienstconcepten

Er zijn vier verschillende dienstconcepten (ook wel 'services'):

- Infrastructure as a Service (IaaS);
- Platform as a Service (PaaS);
- Software as a Service (SaaS);
- Business Process as a Service (BPaaS).

Figuur 3: Dienstconcepten en toepassingsmodellen



Infrastructure as a Service (IaaS)

IaaS is de meest kale, basic vorm van Cloud Computing. De Clouddienstaanbieder biedt ICT infrastructuurcomponenten aan in de vorm van servers, netwerken, rekencapaciteit en dataopslag. De afnemer van deze Clouddienst:

- is volledig vrij om eigen systemen en diensten te ontwikkelen en kan ook zelf zijn besturingssysteem kiezen;
- kan de systemen voor zijn eigen organisatie gebruiken of deze ter beschikking stellen aan derden in de vorm van een Clouddienst;
- is zelf verantwoordelijk voor de functionaliteit, de verwerking en de opslag van data.

De Clouddienstaanbieder is dus alleen verantwoordelijk voor de onderliggende infrastructuur, zoals servers en systemen voor dataopslag. Afhankelijk van de gemaakte afspraken tussen de Clouddienstaanbieder en de afnemer is één van beiden verantwoordelijk voor de toegang, back-up en recovery van de opgeslagen data. De Clouddienstaanbieder biedt vaak een basisvoorziening aan, maar de afnemer zal zelf moeten bepalen of deze voor hem toereikend is. Voorbeelden van (internationale) aanbieders: Microsoft (Azure), Rackspace en Amazon. Enkele lokale spelers bieden dergelijke services ook aan.

Platform as a Service (PaaS)

Er zijn ook aanbieders van Clouddiensten die een ontwikkelplatform aanbieden met een verzameling standaarddiensten (besturings- en datamanagementsysteem, ontwikkeltools). Op basis daarvan kan de gebruiker snel eigen toepassingen ontwikkelen. De afnemer is zelf verantwoordelijk voor de uiteindelijke applicatie. Het onderliggende platform (services, verwerkings- en opslagcapaciteit) is de verantwoordelijkheid van de aanbieder van de Clouddienst. Voorbeelden van aanbieders van PaaS: Microsoft, Amazon, Google, Open Text Cordys, Mendix en WordPress.

Software as a Service (SaaS)

Als de aanbieder van een Clouddienst zorgt voor installatie, onderhoud en beheer, beveiliging en beschikbaarheid van de software, gaat het om Software as a Service (SaaS). De SaaS-aanbieder is daarbij verantwoordelijk voor de toepassingsmogelijkheden en alle onderliggende hard- en software. De afnemer gebruikt de standaardfunctionaliteit die de aanbieder van de SaaS-dienst hem aanbiedt en kan daar doorgaans niets aan wijzigen. Soms biedt de aanbieder de gebruiker de mogelijkheid om de aangeboden standaardfunctionaliteit - binnen de mogelijkheden van de dienst - naar eigen wens vorm te geven en te koppelen met toepassingen die in de eigen omgeving van de gebruiker draaien.

Bekende voorbeelden van SaaS-toepassingen: Microsoft Office 365, de online boekhoudpakketten van Exact, Reeleezee, Twinfield, UNIT4, PM Software, Cash, Davilex, Muis, Yob, AccountView, maar ook LinkedIn, Facebook, Gmail van Google en Hotmail van Microsoft. Andere bekende voorbeelden zijn de opslagdiensten Dropbox, Google Drive, Microsoft Skydrive of Apple iCloud, waarmee de gebruiker data kan opslaan in de vorm van tekst, foto's, films, muziek, etc. Deze toepassingen zijn vaak te gebruiken via apps.

Business Process as a Service (BPaaS)

Bij Business Process as a Service worden geheel of gedeeltelijk ingerichte bedrijfsprocessen aangeboden als een geautomatiseerde dienst. BPaaS is een recente ontwikkeling, waarbij de processen door de diensten van meerdere Clouddienstaanbieders worden vormgegeven. Voorbeelden van BPaaS zijn: salaris- en factuurverwerkingsprocessen (inclusief betaalbaarstelling en betaling), human resources management, maar ook ons elektronisch betaalsysteem, vormgegeven door de betaalfunctie in boekhoudsoftware gecombineerd met het elektronische betaalsysteem van de banken. Een ander bekend voorbeeld is iDEAL, waarmee klanten van een webwinkel in hun aankoopproces via hun eigen bank(rekening) de betaling van een product afhandelen. Bij een BPaaS-dienst zijn dus meerdere partijen verantwoordelijk voor de functionaliteit, het beheer, het onderhoud, de beveiliging en de continuïteit van de keten. Wanneer een van de schakels in de keten niet naar behoren functioneert, levert dit een risico op voor de gehele keten. Concreet voorbeeld daarvan is een grote storing bij iDEAL, waardoor webwinkels de betalingen van hun klanten niet konden verwerken. Dit werkte onmiddellijk negatief door in hun omzetten.

Bijlage 2 | Beschrijving toepassingsmodellen Cloud Computing

Public Cloud

De Public Cloud is de meest vergaande vorm van Cloud Computing. Public Clouddiensten zijn voor iedereen toegankelijk en worden vaak aangeboden door grote internationaal opererende bedrijven. Maar ook kleine nationaal opererende bedrijven kunnen dergelijke diensten aanbieden. Voor de afnemer is de aangeboden infrastructuur onzichtbaar. Deze bevindt zich - ergens ter wereld - op een locatie van de aanbieder of een onderaannemer en wordt ook gedeeld met andere gebruikers. De gebruiker heeft feitelijk geen invloed op de functionaliteit of de kwaliteit van de aangeboden dienst. Voorbeelden van aanbieders: Microsoft (IaaS, PaaS, SaaS), Google (IaaS, SaaS), Apple (SaaS), Open Text Cordys (PaaS), Amazon (IaaS), Salesforce voor CRM (PaaS, SaaS), WordPress voor de ontwikkeling en het onderhoud van websites (PaaS), maar ook Rackspace (IaaS).

Private Cloud

Bij een Private Cloud werkt de gebruiker op een infrastructuur en met toepassingen die specifiek zijn ingericht voor zíjn organisatie. De functionaliteit en infrastructuur worden niet gedeeld met andere organisaties. Bij dit toepassingsmodel heeft de gebruiker meer zeggenschap en controle over de data, de beveiliging en de kwaliteit van de dienst. Het onderhoud van de Private Cloud ligt - afhankelijk van het gekozen dienstconcept - bij de aanbieder en/of de gebruiker.

Hybride Cloud

Voor sommige Clouddiensten wordt gekozen voor de combinatie van de Public Cloud met een Private Cloud. Zo kunnen bijvoorbeeld toepassingen binnen de Public Cloud een Private Cloud ondersteunen wanneer er sprake is van een piekbelasting.

Community Cloud

Binnen een Community Cloud worden Clouddiensten aangeboden voor een groep organisaties met een gemeenschappelijk belang. De Community Cloud is aangepast aan de specifieke eisen die de deelnemende organisaties aan de Clouddienst stellen, zoals datalocatie, beveiliging en architectuurkeuzes. De hardware staat bij één of meer van de deelnemende organisaties of een derde partij, wat het risico van inbreuk op de beschikbare data beperkt. Voorbeelden van organisaties met een gemeenschappelijk belang die in een Community Cloud werken, zijn onderwijsorganisaties, overheidsinstellingen en zorginstellingen. Een Clouddienst (bijvoorbeeld een administratieve toepassing) die zich richt op een

specifieke groep gebruikers in een bepaald gebied is ook te beschouwen als dienstconcept binnen een Community Cloud. Voorbeelden in die context, van op Nederland gerichte Clouddiensten op het terrein van de financiële administratie, zijn: Twinfield, Reeleezee, UNIT4, Exact Online en Pro Management.

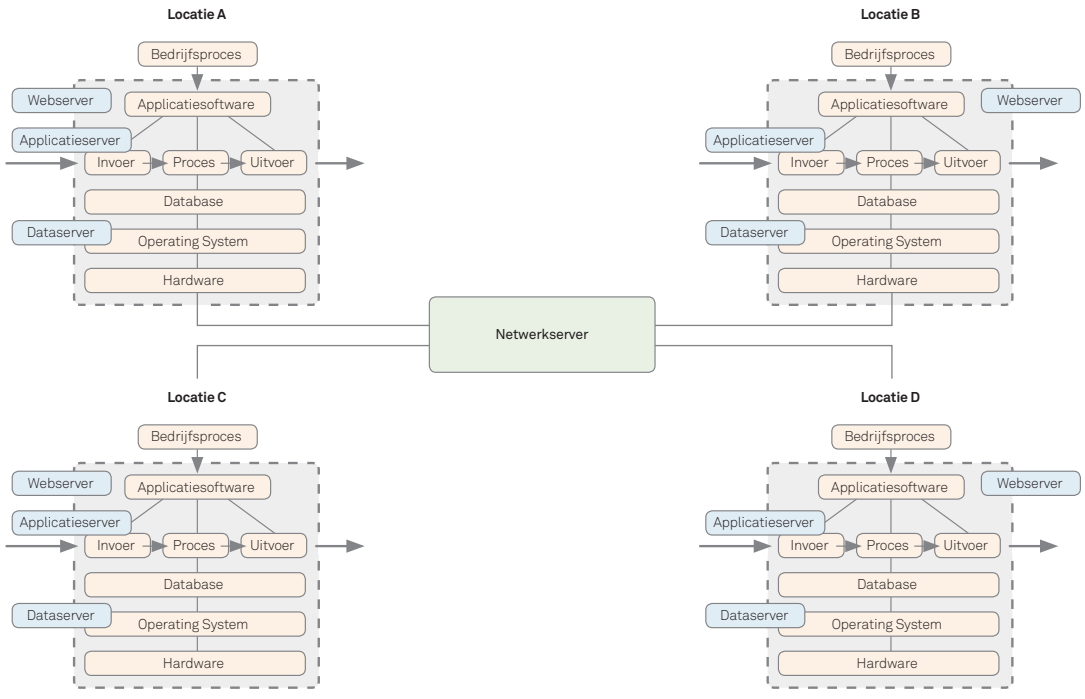
Bijlage 3 | Architectuur

Hieronder wordt een nadere toelichting gegeven op verschillende aspecten van de architectuur.

Servers

Een server kan een speciale functie hebben; zo bestaan er applicatieservers om applicaties toe te passen, dataservers voor opslag en bewerking van data, netwerkservers om dataverkeer tussen verschillende computers te faciliteren, web-servers, etc. Zo kan een ICT-infrastructuur ontstaan waarin meerdere applicaties, meerdere databases en meerdere computers/servers met elkaar in een netwerk samenwerken om de bedrijfsvoering te faciliteren. In onderstaand schema wordt een voorbeeld van een dergelijke structuur weergegeven (zie figuur 4).

Figuur 4: Infrastructuur geautomatiseerde informatieverwerking Cloud Service Location



Virtualisatie

Virtualisatie maakt het mogelijk om op één fysieke computer meerdere besturingssystemen en toepassingen te installeren. Elk in hun eigen afgeschermde omgeving, gebruikmakend van een deel van de hardware als 'eigen' resource en onafhankelijk van elkaar. Voorheen was het gebruikelijk dat op een fysieke computer één besturingssysteem was geïnstalleerd en dat deze computer ook maar voor één toepassing werd gebruikt. Praktisch erg inefficiënt, omdat voor die toepassing capaciteit beschikbaar is die mogelijk zelden volledig wordt gebruikt.

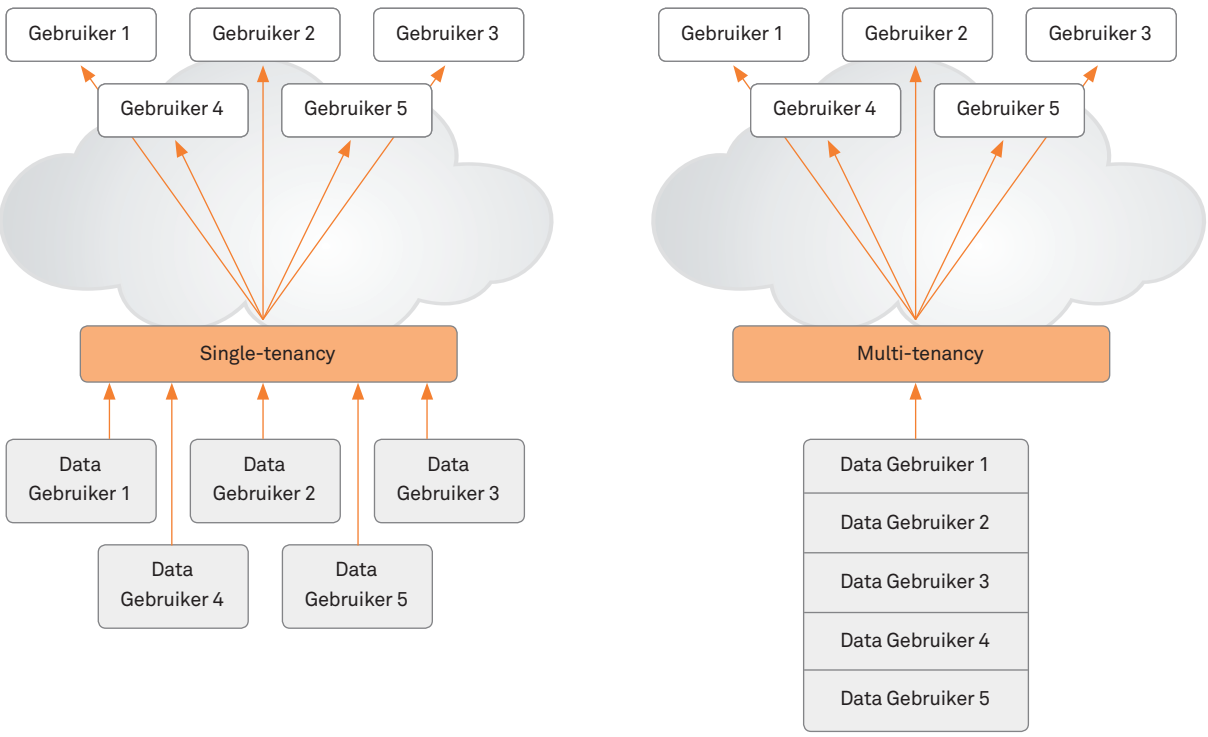
Virtualisatie is toe te passen op alle componenten van een ICT-infrastructuur: server-virtualisatie, operating system-virtualisatie, database-virtualisatie en applicatie-virtualisatie. Clouddienstaanbieders passen vaak virtualisatie toe van applicaties, databases en servers. Motief daarvoor is dat virtualisatie het mogelijk maakt om processen zo efficiënt mogelijk in te richten en aan te bieden. Het gemeenschappelijk en gedeeld gebruik van ICT-middelen is hier ook niet bezwaarlijk, mits:

- de verschillende processen gescheiden zijn;
- er geen vermenging en/of bewerking van data kan optreden;
- er specifieke beveiligingsmaatregelen zijn genomen tegen aanvallen in de beheer-/virtuele laag.

Multi-tenancy

Clouddienstaanbieders passen vormen van single-tenancy (één gebruiker) en multi-tenancy (meerdere gebruikers) toe (zie figuur 5). Bij multi-tenancy benutten meerdere gebruikers dezelfde toepassing en database, waarbij de dataverwerking en -opslag plaatsvinden in één (virtuele) omgeving. De data van elke gebruiker krijgen daarbij een eigen, onderscheidend kenmerk mee.

Figuur 5: Single-tenancy versus multi-tenancy



Bij multi-tenancy mogen de data van de ene gebruiker niet beschikbaar komen voor de andere gebruiker. Dat vereiste een goede identificatie en autorisatie/authenticatie, alsmede een adequate changemanagementprocedure, die moet waarborgen dat een wijziging door gebruiker 1 geen invloed heeft op de toegang tot, of het gebruik van, de data van de andere gebruikers in dezelfde omgeving. Gedeeld gebruik van resources maakt gebruikers wel afhankelijk van andere gebruikers. Een hard- en/of softwarestoring treft alle gebruikers die van deze virtuele omgeving en/of toepassing gebruikmaken. Ook een eventuele inbeslagname door Justitie kan meerdere gebruikers treffen.

Bijlage 4 | Voorbeelden van bedrijfsrisico's gerelateerd aan Cloud Computing

In onderstaand schema ziet u een aantal voorbeelden van mogelijke bedreigingen voor de beschikbaarheid en continuïteit van data en processen, voor de integriteit en vertrouwelijkheid van data en voor het naleven van wet- en regelgeving.

Situaties die een bedreiging kunnen doen ontstaan (niet limitatief)	Mogelijk bedreigend voor:		
	Beschikbaarheid en continuïteit van data en processen	Integriteit en vertrouwelijkheid van de data	Naleven wet- en regelgeving (compliance)
Strategische informatie opgeslagen in de Cloud		•	
Ontoereikende logische en fysieke beveiliging van data en processen bij de Clouddienstaanbieder (verder: CDA)	•	•	•
Onvoldoende back-up en recovery voor herstel van services bij storingen bij de CDA, inclusief disaster recovery en uitwijk	•	•	•
Ontoereikende beveiliging van dataverkeer over het internet		•	
Ontoereikend intern beheer en interne beheersing bij CDA *(bijvoorbeeld bij toepassen virtualisatie en multi-tenancy)*	•	•	
Ontoereikend changemanagement van applicaties en infrastructuur bij de CDA	•	•	
Ontoereikend incidentenbeheer CDA	•	•	
Ontbreken van voldoende toepassingsgerichte interne beheersingsmaatregelen (application controls) op invoer, verwerking, uitvoer en opslag)		•	

Situaties die een bedreiging kunnen doen ontstaan (niet limitatief)	Mogelijk bedreigend voor:		
	Beschikbaarheid en continuïteit van data en processen	Integriteit en vertrouwelijkheid van de data	Naleven wet- en regelgeving (compliance)
Onvoldoende mogelijkheid om via een audit trail de goede werking van processen en opslag, inclusief incidentmanagement, vast te stellen		•	•
Onvoldoende technische capaciteit en bezetting van de organisatie van de CDA	•	•	
Faillissement of overname van de CDA door een andere partij	•		
Vendor lock-in; de gebruiker kan in technische zin zijn data en/of programma's/processen niet overbrengen naar een andere CDA	•		
Onvoldoende doorgroeimogelijkheden naar nieuwe of aangepaste functionaliteit	•		
Onduidelijkheid over juridisch eigenaarschap data	•		•
Onduidelijkheid over fysieke locatie/omstandigheden waaronder data worden opgeslagen en bewaard	•	•	•
Onvoldoende duidelijkheid over wet- en regelgeving waaronder de Clouddienst wordt aangeboden en de CDA functioneert			•
Onduidelijkheid over de aansprakelijkheid voor beschikbaarheid dienstverlening, performance, etc.			•
Onduidelijkheid over de mogelijkheid om te kunnen voldoen aan wet- en regelgeving, waaronder privacyregelgeving, maar ook fiscale regelgeving			•
Onvoldoende duidelijkheid over juridische voorwaarden waaronder de dienstverlening van de CDA plaatsvindt			•
Ontbrekende of ontoereikende exit-strategie, waardoor de gebruiker niet weet hoe hij kan overstappen naar een andere CDA (data opgeslagen in een open formaat of fysiek op te halen?) en onder welke voorwaarden	•		•

Bijlage 5 | Assurance-rapport, certificering en keurmerk

Assurance-rapport

U bent de term in de tekst al eerder tegengekomen: assurance-rapport. Een auditor stelt dit rapport op in opdracht van een Clouddienstaanbieder, of op verzoek van een klant of zijn accountant. De meeste assurance-rapporten komen dus niet eerder in beeld dan dat u bezig bent met een controleopdracht bij een klant waarbij IT - en dus ook Cloud Computing - een belangrijke rol speelt. Een kort overzicht van de meest gangbare assurance-rapporten (zie ook bijlage 9):

- **Een assurance-rapport gebaseerd op de International Standard on Assurance Engagements (ISAE) 3402 (Standaard 3402) of de Amerikaanse variant SSAE 16**. Dit rapport is primair bedoeld voor de controlerend accountant van de gebruiker van de dienstverlening van de Clouddienstaanbieder. De rapportage kent twee varianten: een rapportage gericht op de opzet van de interne beheersingsmaatregelen van de Clouddienstaanbieder op een bepaald moment (type 1) en een rapportage die naast de opzet ook het bestaan en de werking van de beheersingsmaatregelen gedurende een bepaalde periode omvat (type 2).
- **Een assurance-rapport gebaseerd op Standaard 3000.** Deze rapportage is vaak bedoeld voor een ruimere doelgroep. De rapportage richt zich niet alleen op zaken die van belang zijn voor de controle van de financiële verantwoording, maar er wordt ook gekeken of de dienstverlening en de interne beheersingsmaatregelen van de Clouddienstaanbieder voldoen aan een algemeen aanvaard kwaliteitsniveau.
- **SOC 1, SOC 2 en SOC 3** (SOC staat voor Service Organization Controls reports). SOC 1 staat voor een rapportage naar aanleiding van een opdracht die is uitgevoerd onder de Amerikaanse assurance standaard SSAE 16. Deze is te vergelijken met een assurance-rapport in het kader van ISAE 3402 (Standaard 3402). Veel kleinere datacenters en hostingpartijen laten hun belangrijke beheerprocessen al auditen volgens SOC 1 of standaard 3402. SOC 2 en SOC 3 worden afgegeven voor een breder publiek en komen tot stand onder de Amerikaanse assurance standaard AT 101. Deze beide rapportages richten zich in brede zin op de beheersing van de kwaliteitscriteria beveiliging, beschikbaarheid/continuïteit en vertrouwelijkheid. SOC 2 en SOC 3 zijn vergelijkbaar met assurance opdrachten onder ISAE 3000 (Standaard 3000).

Certificering (ISO 27001 en ISO 27002)

Naast de hiervoor omschreven assurance-rapporten, is er nog een ander fenomeen: de ISO 27001- en de ISO 27002-certificering. De standaarden ISO 27001 en 27002 hebben beide betrekking op de invulling van informatiebeveiliging. Zij zijn de opvolgers van ISO 17799 (voorheen de Code voor Informatiebeveiliging).

ISO 27001 is normatief van opzet en bevat harde eisen waaraan de organisatie moet voldoen om gecertificeerd te worden. Deze eisen worden beschreven op het niveau van maatregelen die de organisatie moet treffen. ISO 27002 is niet-normatief van opzet en bevat 'best practices' voor de implementatie van informatiebeveiliging. Beide standaarden richten zich

primair op de beheersing van informatiebeveiliging. Dit kan weliswaar raakvlakken hebben met de beheersing van de integriteit van de data en het waarborgen van de vertrouwelijkheid, maar dat is niet de primaire focus. Om die reden leveren certificaten die gebaseerd zijn op ISO 27001 of ISO 27002 onvoldoende controlebewijs voor een accountant. Een accountant die wil weten in welke mate bepaalde risico's zijn afgedekt, dient de 'verklaring van toepasselijkheid' ('statement of applicability') in te zien.

Nadere informatie over de ISO-standaarden 27001 en 27002 is beschikbaar bij het NEN in Delft, in het white paper NCSC '*Cloudcomputing & security*', januari 2012 (als bron opgenomen in bijlage 7) en het artikel van Koorn en Stoof: '*IT-assurance versus IT-certificering*', gepubliceerd in Compact 2013-2.

Keurmerk Zeker-Online

Medio 2013 is het keurmerk 'Zeker-Online' actief geworden. Dit is een onafhankelijk en transparant keurmerk voor online administratieve diensten, ofwel Clouddiensten. Het keurmerk staat daarmee voor betrouwbaarheid, veiligheid en continuiteit, kwaliteit in functionaliteit en juridische zekerheid van de Cloud.

De Belastingdienst, het Electronic Commerce Platform Nederland (ECP) en aanbieders van Clouddiensten hebben samen bijgedragen aan de ontwikkeling van 'Zeker-Online'. Hun missie is daarbij: een kwaliteitsgarantie kunnen bieden aan gebruikers van Clouddiensten. De kwaliteitseisen voor het keurmerk zijn gedefinieerd en vastgelegd in het 'Normenkader Zeker-Online'. Hierbij werkten de hiervoor genoemde partijen nauw met elkaar samen, daarbij ondersteund door een groep auditors. Binnen het normenkader is met een kwaliteitsbril gekeken naar de technische infrastructuur, de administratieve structuur en verwerkingswijze (generieke en specifieke maatregelen in de applicatie), en naar de juridische infrastructuur. De Stichting Zeker-Online verleent het (nieuwe) keurmerk, dat zichtbaar maakt welke Clouddienstaanbieders diensten leveren die voldoen aan belangrijke online securityvereisten. Daarin hebben de beveiligingsrichtlijnen van het National Cyber Security Center een belangrijke rol gespeeld.

Wil een Clouddienstaanbieder in aanmerking komen voor het keurmerk? In dat geval zal hij, en zijn eventuele onderaannemers, moeten voldoen aan hoge kwaliteitseisen die een betrouwbare, continue verwerking van transacties waarborgen. Dat geldt niet alleen voor de applicatie die de administratieve gegevens verwerkt en waaruit financiële informatie voortkomt. Voor het totaalpakket van de dienstverlening door de aanbieder die het keurmerk voor zijn oplossing heeft verworven, geldt dit óók. Is het keurmerk toegekend, dan mag de klant erop vertrouwen dat:

- hij eigenaar is van zijn gegevens;
- hij voortdurend zelfstandig hierover kan beschikken; en
- de administratieve dienstverlening voldoet aan de relevante wet- en regelgeving.

Meer informatie over het keurmerk leest u op **www.zeker-online.nl**

Bijlage 6 | Interne beheersing bij Cloud Computing

Als uw klant Cloud Computing wil gebruiken, dan moet er over diverse zaken goed worden nagedacht. In het overzicht dat hierna volgt, ziet u een groot aantal voorbeelden van vragen die in het kader van de interne beheersing van belang kunnen zijn. Of deze vragen bij u uw klant aan de orde zijn, hangt mede af van de risico's die uw klant in zijn specifieke situatie loopt (zie bijlage 4 voor een aantal voorbeelden van dergelijke risico's).

Voorbeelden van vragen gericht op de interne beheersing bij Cloud Computing	
A	**Integriteit, vertrouwelijkheid, beschikbaarheid en continuïteit**
A-1	Is de bescherming van data gewaarborgd (logische en fysieke toegangsbeveiliging)?
A-2	Zijn het intern beheer en de interne beheersing toereikend geregeld?
A-3	Is het changemanagement toereikend geregeld?
A-4	Is het probleem- en incidentenmanagement toereikend geregeld?
A-5	Zijn er voldoende toepassingsgerichte interne beheersingsmaatregelen in de toepassingen opgenomen (Application Controls)?
A-6	Zijn er voldoende mogelijkheden om via een audittrail de goede werking van processen en opslag vast te kunnen stellen?
A-7	Zijn er toereikende back-up- en recovery-maatregelen getroffen?
A-8	Is het dataverkeer via internet goed beveiligd?
A-9	Is de (technische) capaciteit en bezetting van de organisatie op voldoende niveau?
A-10	Is duidelijk waar de data (fysiek) staan opgeslagen (ook de back-up) en onder welke omstandigheden?
A-11	Is zekergesteld dat verwijderde data ook echt (uit de Cloud) verwijderd zijn?
A-12	Is de data-integriteit bij het gebruik van een gedeelde infrastructuur gewaarborgd?

A-13	Is het identiteits- en toegangsbeheer adequaat?
A-14	Geeft de aanbieder in voldoende mate inzicht in de getroffen beheer- en beveiligingsmaatregelen (inclusief opgetreden incidenten)?
B	**Compliance/Privacy**
B-1	Kan de afnemer invulling geven aan de hem opgelegde (wettelijke) privacy-eisen?
B-2	Zijn er verschillen in wet- en regelgeving tussen de landen (ook binnen de EU) die van belang zijn voor de aanbieder/afnemer?
B-3	Is bekend (in het geval er persoonsgegevens worden opgeslagen) in welk land deze gegevens worden opgeslagen? Worden, als het gaat om een Amerikaanse leverancier van Cloud Computing, bij die opslag de Veilige Haven Beginselen in acht genomen?
B-4	Is de telecommunicatiewet van toepassing op de aanbieder van Clouddiensten?
B-5	Zijn er wettelijke bepalingen die de afnemer verplichten dat (overheids)data binnen Nederlandse grenzen moeten blijven?
B-6	Zijn er 'wettelijke' verplichtingen die de afnemer mogelijk belemmeren/beperken in het gebruik van Clouddiensten?
B-7	Is duidelijk welk recht op de Clouddienst van toepassing is?
B-8	Is duidelijk wie aansprakelijk gesteld kan worden voor de beschikbaarheid, performance, beveiliging of opslag van een (grensoverschrijdende) Clouddienst?
B-9	Vallen data die buiten de landsgrenzen door private partijen worden verwerkt/opgeslagen onder buitenlandse wetgeving?
B-10	Kan de aanbieder /afnemer voldoen aan de aankomende wetgeving met betrekking tot de meldplicht?
B-11	Kan de afnemer voldoen aan artikel 33 WBP/ Art. 10 Europese Dataprotectierichtlijn?
B-12	Beschikt de afnemer over het 'right-to-audit'?
B-13	Verstrekt de aanbieder een assurance-rapport en/of een vorm van certificering?
B-14	Wie is (juridisch) aansprakelijk bij inbreuk op de data-confidentialiteit?
B-15	Kunnen overheden van andere (niet EU-) landen de data inzien?
B-16	Is duidelijk wie de (juridische) eigenaar is van de in de Cloud(dienst) opgeslagen data?
B-17	Kan worden voldaan aan de verplichtingen die voortvloeien uit de fiscale wet- en regelgeving?
C	**Businesscontinuïteit**
C-1	Beschikt de afnemer over garanties met betrekking tot het voortbestaan van de dienst (bijvoorbeeld bij exit/insolventie)?
C-2	Is er een exit-strategie als de Clouddienstaanbieder toch failliet gaat of wordt overgenomen?
C-3	Zijn de gegevens van de afnemer te allen tijde toegankelijk?
C-4	Kunnen de opgeslagen data snel, en in een standaard/bruikbaar formaat, worden weggehaald?

C-5	Beschikt de afnemer over garanties met betrekking tot de beschikbaarheid (up-time)?
C-6	Zijn er twijfels over de financiële positie van de aanbieder?
C-7	Zijn er voldoende waarborgen met betrekking tot het onderhoud en de ontwikkeling van applicaties in de Cloud?
C-8	Zijn er voldoende mogelijkheden om specifieke (op de individuele afnemer gerichte) functionaliteit en/of wijzigingen door te voeren?
D	**Integratie en standaarden**
D-1	Zijn er voldoende mogelijkheden tot 'reversibility' of 'portability'?
D-2	Biedt de Clouddienstaanbieder voldoende standaarden voor interoperabiliteit?
D-3	Bestaat er een gevaar voor 'Vendor lock-in'?
E	**Contract**
E-1	Weet het bedrijf van de afnemer in voldoende mate waar zij bij het gebruik van een Clouddienst op moet letten?
E-2	Is de afnemer in staat c.q. in de gelegenheid om de beloftes/toezeggingen van de aanbieder te controleren?
E-3	Zijn de overeengekomen diensten/prestaties - zoals beschikbaarheid, responstijden, etc. - in voldoende mate vastgelegd in een SLA in de vorm van heldere prestatie-indicatoren en garanties op die indicatoren?
E-4	Is de aanbieder voldoende transparant met betrekking tot de geleverde prestaties?
E-5	Is het bij incidenten (onderbreking van service) altijd duidelijk waar het probleem ligt en welke partij hierop moet worden aangesproken?
E-6	Zijn de rechten, plichten en verantwoordelijkheden tussen aanbieder en afnemer duidelijk?
E-7	Zijn de standaardvoorwaarden van de Clouddienst-aanbieder (volstrekt) eenzijdig en/of te complex?
F	**Business Case**
F-1	Remmen bestaande licenties de overgang naar de Cloud?
F-2	Bestaat er onzekerheid ten aanzien van de prijsontwikkeling in de toekomst?
F-3	Beschikt de organisatie van de afnemer over een goed beeld wat de Cloud voor de organisatie zou kunnen beteken?
F-4	Maken eerder gedane investeringen in IT-systemen de overstap naar Clouddiensten rendabel?
F-5	Is er sprake van een hoge mate van complexiteit, bij integratie met verschillende aanbieders en eigen systemen (legacy)?

Bijlage 7 | Literatuur

AFM (2013). Themaonderzoek niet OOB-accountantsorganisaties, Deel 1: NBA-kantoren.
www.afm.nl

College Bescherming Persoonsgegevens (2012), Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier
www.cbpweb.nl/downloads/

ENISA (2009). Cloud Computing, Benefits, Risks and recommendations for information security.
www.enisa.europa.eu/publications

Koninklijk NIVRA. Leidraad 14 Opdrachten in de mkb-praktijk
www.nba.nl/Documents/Wet/

NBA (2014). Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak
www.nba.nl/Documents/

NCSC (2012). Cloudcomputing & security
www.ncsc.nl/binaries/

NIST. The NIST Definition of Cloud Computing. Special Publication 800-145.
http://csrc.nist.gov/publications/

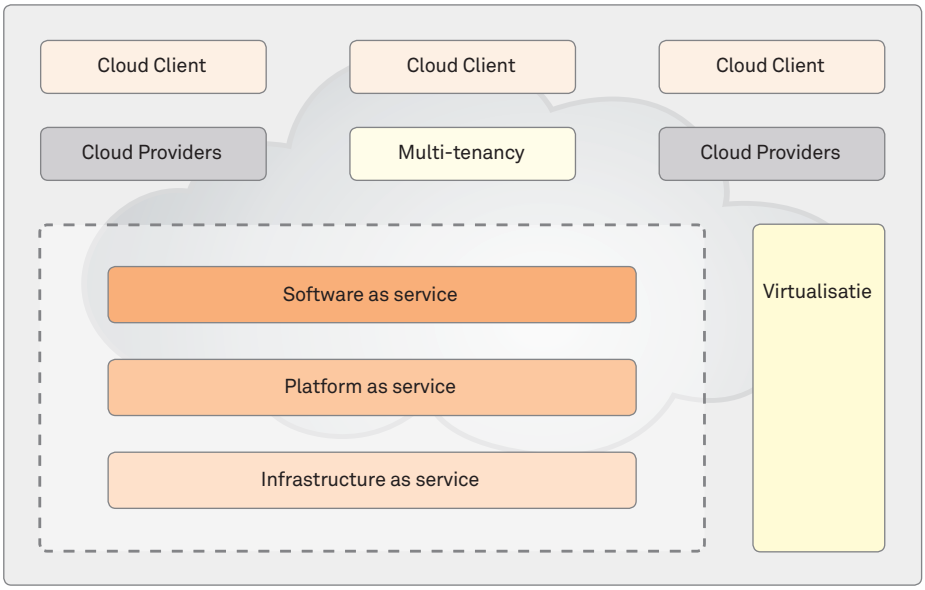
Verdonck, Kloosters & Associates B.V. (2012). CLOUD COMPUTING, FUNDAMENT OP ORDE. Rapport in opdracht van het ministerie van EL&I
www.rijksoverheid.nl/bestanden/

SRA (2010). SRA Controleaanpak en Automatisering: SRA Praktijkhandreiking

Bijlage 8 | Voorbeelden van Cloud Architectuur-modellen en Clouddiensten

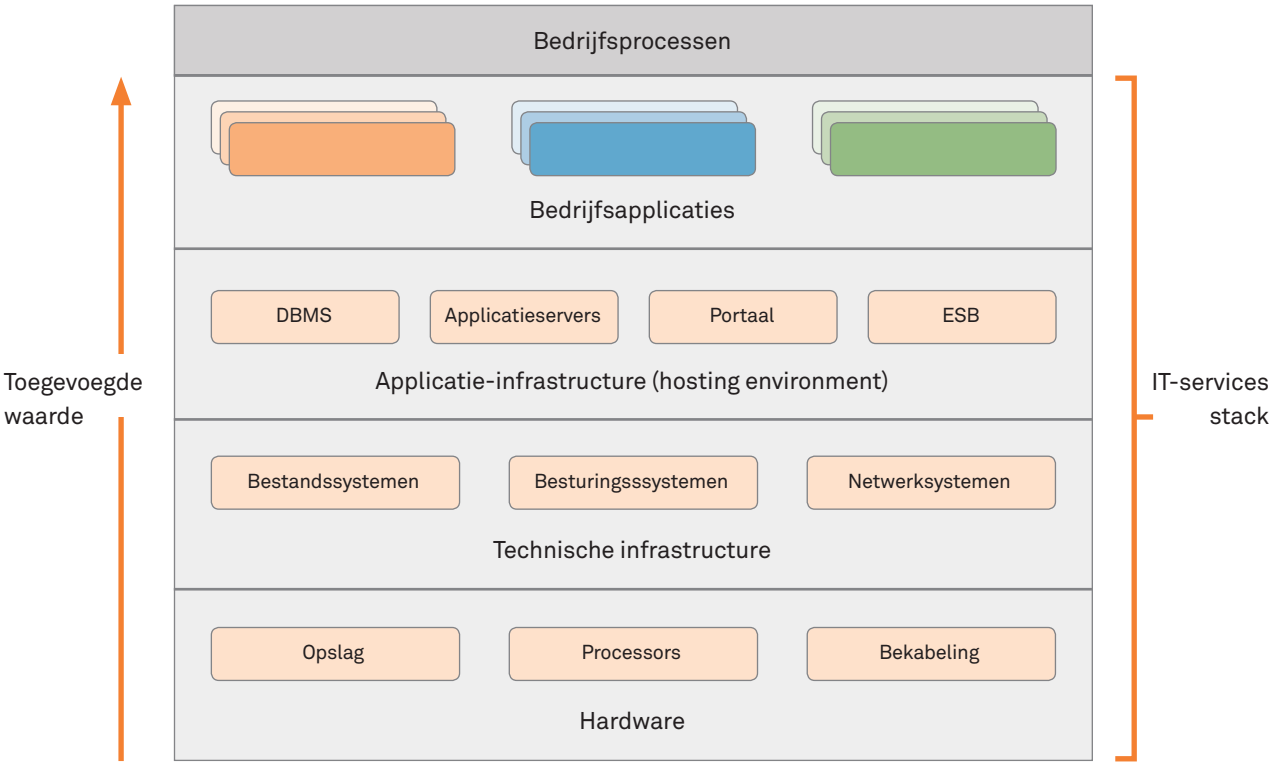
In paragraaf 1.4 is ingegaan op de architectuur van Cloud Computing, waarbij met name aandacht is besteed aan locatie, multi-tenancy en virtualisatie. Dit is schematisch weergegeven in figuur 1, die hier voor de duidelijkheid nog even wordt herhaald.

Figuur 1: Basismodel Cloud Computing Architectuur



Alle Clouddiensten hebben tot doel dat zij bedrijfsprocessen ondersteunen. Hierdoor ontstaat er een gelaagdheid aan 'informatieverwerkingsinfrastructuren'. Laat u zich echter door de dynamiek rond de continue ontwikkeling van nieuwe Clouddiensten vooral niet afleiden van de essentie: een zo effectief en efficiënt mogelijke ondersteuning van de bedrijfsvoering. De samenhang tussen bedrijfsprocessen en de lagen in de (onderliggende) informatieverwerkingsprocessen ziet er daarbij als volgt uit:

Figuur 6: IT-services stack (overgenomen uit Hasan: A Glance to Cloud Computing, Saturday, November 1, 2008)



De ICT-diensten die de markt biedt, concentreren zich op elk van deze lagen. Als u en uw klant dit gelaagde beeld van ICT goed voor ogen hebben, is het gemakkelijker om te doorzien hoe Cloud Computing zich hiermee verhoudt. Natuurlijk is de werkelijkheid complexer dan dit gestileerde basismodel. Wilt u meer weten over Cloud Computing en Cloud Computing Architectuurmodellen, dan adviseren wij u om de websites van verschillende Clouddienstaanbieders nader te bekijken. In deze NBA-brochure is er bewust voor gekozen om op deze plek geen voorbeelden op te nemen, omdat anders al gauw sprake zou zijn van niet meer up-to-date materiaal.

Bijlage 9 | Overzicht relevante verschillen tussen assurance-rapporten

Toepassing	Inhoud	Inhoud van het rapport
	Standaard 3402	
Communicatiemiddel tussen accountants in het kader van de controle van de jaarrekening over de interne beheersing bij een serviceorganisatie aan wie de controleklant diensten heeft uitbesteed.	Het rapport geeft aan in hoeverre het door de service-organisatie gedefinieerd stelsel van interne beheersings-maatregelen in opzet/bestaan op enig moment in de tijd aanwezig is en functioneert over een aangegeven periode (werking). Het is aan de accountant van de uitbestedende organisatie om na te gaan welk stelsel van interne beheersing in het onderzoek is betrokken (scope) en of het niveau van interne beheersing van het beoordeelde stelsel van maatregelen/procedures voor hem van voldoende niveau is om daarop in zijn controle te kunnen steunen. In dat kader zal hij moeten vaststellen of: • alle voor zijn controle van belang zijnde maatregelen in de beoordeling van het stelsel zijn meegenomen; • de uitgevoerde controlewerkzaamheden voldoende bewijs hebben om de conclusie (oordeel van de onafhankelijke auditor) te onderbouwen. Dit rapport is van belang voor de controlerende accountant van de gebruiker van de dienstverlening van de serviceorganisatie.	Twee typen rapportages zijn mogelijk: • **Type I rapport:** Dit rapport heeft betrekking op de opzet/het bestaan op enig moment in de tijd • **Type 2 rapport:** Dit rapport heeft naast opzet/bestaan ook betrekking op het functioneren gedurende de aangegeven periode.
Standaard 3000	**Standaard 3000**	
Assurance-rapport ten behoeve van een ruime doelgroep. ISO 27001/2	Het rapport geeft aan in hoeverre een organisatie voldoet aan de in de standaard aangegeven eisen. Het rapport biedt de serviceorganisatie de mogelijkheid om publiekelijk aan te geven dat de door de serviceorganisatie te definiëren dienstverlening, inclusief interne beheersing, aan algemeen aanvaarde kwaliteitsnormen voldoet. Ook hier is het aan de lezer om na te gaan of het beoordeelde	Twee typen rapportages zijn mogelijk: • Een assurance-rapport dat betrekking heeft op de opzet/het bestaan op enig moment in de tijd. • Een assurance-rapport dat ook

Toepassing	Inhoud	Inhoud van het rapport
	stelsel en de gehanteerde normen voor hem van voldoende niveau zijn en of alle voor hem van belang zijnde maatregelen in de beoordeling van het stelsel zijn meegenomen. Dit rapport is van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	betrekking heeft op het functioneren van het beoordeelde stelsel gedurende de aangegeven periode.
ISO 27001/2		
Basis voor het afgeven van een certificaat. Richt zich met name op informatiebeveiliging.	Het certificaat geeft aan in hoeverre het managementsysteem van de beoordeelde organisatie voldoet aan de in de standaard aangegeven eisen. Uit dit certificaat kan worden afgeleid dat de organisatie over een systeem beschikt om toepasselijke beheersmaatregelen op te zetten en naar behoren te laten functioneren. Hierbij moet worden aangetekend dat de in de standaard opgenomen eisen ruimte laten voor interpretatie door de uitvoerend auditor en afhankelijk zijn van de beleidsdoelstellingen van de organisatie. Daarom is het van belang inzicht te krijgen in de onderdelen/processen van de organisatie die gecertificeerd zijn en de maatregelen die zijn genomen. Dit blijkt uit de "verklaring van toepasselijkheid" ("statement of applicability").	Certificaat waarin is aangeven in hoeverre het managementsysteem van een organisatie voldoet aan de in de standaard opgenomen eisen.
SOC 1 (Amerikaanse regelgeving)		
Richt zich op interne beheersingsmaatregelen, die van belang zijn in het kader van controle van de jaarrekening	Problematiek is vergelijkbaar met Standaard 3402. Het rapport is van belang voor de controlerende accountant van de gebruiker van de dienstverlening van de serviceorganisatie.	Problematiek vergelijkbaar met Standaard 3402.
SOC 2 (Amerikaanse regelgeving)		
Assurance-rapport ten behoeve van een ruime doelgroep.	De problematiek is vergelijkbaar met Standaard 3000. Als normenkader voor de beoordeling wordt vaak gebruikgemaakt van de 'Trust Services Principles' die zich richten op beveiliging (inclusief betrouwbaarheid), beschikbaarheid (inclusief continuïteit), verwerkingsintegriteit, vertrouwelijkheid en privacy. Het rapport is van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	Problematiek vergelijkbaar met Standaard 3000.
SOC 3 (Amerikaanse regelgeving)		
Assurance-rapport ten behoeve van publiekelijk gebruik, veelal in de vorm van een extern gericht keurmerk.	De problematiek is vergelijkbaar met Standaard 3000. Als normenkader voor de beoordeling wordt vaak gebruikgemaakt van de 'Trust Services Principles' die zich richten op beveiliging (inclusief betrouwbaarheid), beschikbaarheid	Publiekelijk gericht keurmerk dat verwijst naar het achterliggend assurance-rapport.

Toepassing	Inhoud	Inhoud van het rapport
	(inclusief continuïteit), bewerkingsintegriteit, vertrouwelijkheid en privacy. Dit rapport is van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	
Zeker-Online		
Keurmerk inzake de kwaliteit van online administratieve diensten	De beoordeling is gebaseerd op een uitgebreid normenstelsel. Dit normenstelsel is te downloaden van de website van Zeker-Online (**www.zeker-online.nl**). Het keurmerk is van belang voor gebruikers van de dienstverlening van Clouddienstaanbieders.	Publiekelijk gericht keurmerk dat verwijst naar achterliggend assurance-rapport (Standaard 3402).

Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl