Risico's door de cloud

organisatorische en juridische aandachtspunten & maatregelen

Auteur: Yvonne van Boxmeer
Studentnr.: 850483309
Datum: 17 april 2012

Risks by the Cloud

Organizational and Legal Issues & Measures

Yvonne van Boxmeer (850483309)
17 april 2012
Business Process Management and IT
Open Universiteit, faculteit Informatica

1e Begeleider: Dr. ir. H.P.E. Vranken
2e Begeleider & examinator: Prof. dr. M.C.J.D. van Eekelen

Inhoudsopgave

Samenvatting

De hoofdvraag van dit onderzoek is: *"Wat zien organisaties als de belangrijkste organisatorische en juridische risico's bij het gebruik van cloud computing en hoe gaan zij met deze risico's om?"*

Bij cloud computing worden IT-middelen via internet beschikbaar gesteld als diensten uit onuitputtelijke bronnen door veelal commerciële leveranciers. Deze nieuwe ontwikkeling brengt, net als alle andere nieuwe ontwikkelingen, risico's met zich mee. Voor organisaties is het dan ook van groot belang om deze risico's inzichtelijk te hebben bij het maken van de keuze om wel of niet (gedeeltelijk) de overstap te maken naar een cloud omgeving.

Dit onderzoek heeft als doel de belangrijkste organisatorische en juridische risico's inzichtelijk te maken die gelden voor alle organisaties die van plan zijn de overstap te maken naar een cloud omgeving of al hebben gemaakt. Per risico wordt aandacht besteed aan risicomijdende of risicobeperkende maatregelen.

Om antwoord te geven op de hoofdvraag van dit onderzoek, zijn de volgende onderzoeksvragen opgesteld en vervolgens beantwoord:

1. Welke organisatorische risico's worden door organisaties als meest risicovol aangeduid?
2. Wat zijn voor organisaties de belangrijkste juridische risico's?
3. Op basis van welke methode en afspraken zijn deze risico's geïdentificeerd en geclassificeerd?
4. Hoe classificeren de organisaties de benoemde risico's? Worden ze vermeden, geaccepteerd, verzekerd of beperkt?
5. Welke maatregelen worden ingezet om risico's te beperken of te vermijden?

Het onderzoek bestaat uit een literatuurstudie waaruit een theoretisch kader is afgeleid. Dit theoretisch kader is vervolgens empirisch getoetst en aangevuld tot een compleet overzicht van risico's en maatregelen.

Uit de literatuur is het mogelijk geweest 6 organisatorische en 5 juridische risico's te destilleren en 5 maatregelen om deze risico's te beperken of te vermijden. Dit heeft geresulteerd in een matrix die de koppeling tussen de 11 risico's en de 5 maatregelen beschrijft. Deze matrix diende als hypothese voor het praktijkonderzoek.

Het empirisch onderzoek bestond uit een schriftelijke enquête onder medewerkers van verschillende organisaties en branches. Deze medewerkers zijn benaderd vanuit zakelijk overkoepelende interesses op het gebied van cloud computing en beveiliging.

Concreet betrof het de LinkedIn-groepen Platform voor InformatieBeveiliging, Cloud Security Alliance – Nederland en Cloud Computing Nederland. Met deze doelgroepen was het mogelijk om een onderzoeksdoelgroep te creëren van ruim 1300 personen. Ondanks een beperkte respons (63 personen) is de foutmarge beperkt tot 12% bij een betrouwbaarheidspercentage van 95%. De 63 respondenten vertegenwoordigen 11 branches, waardoor de resultaten als algemeen geldend kunnen worden beschouwd voor alle organisaties die gebruik (gaan) maken van een cloud omgeving.

De resultaten uit het literatuuronderzoek dienden als input voor het empirisch onderzoek. Uit de resultaten werd duidelijk dat de risico's uit de literatuur werden bevestigd. Daarnaast zijn zowel de organisatorische als de juridische risico's uitgebreid met een extra risico dat in het empirisch onderzoek veelvuldig werd benoemd. Dit heeft geresulteerd in zeven organisatorische en zes juridische risico's, die kunnen worden aangeduid als belangrijk in relatie tot het gebruik van cloud computing.

Organisatorisch risico 1: Leveranciers lock-in
Het ontbreken van de mogelijkheid om van leverancier te kunnen veranderen wordt door 52% van de respondenten als risico benoemd. Het merendeel van de respondenten geeft aan dit risico te accepteren. Daarnaast worden maatregelen als standaardisatie, het gebruik van meerdere leveranciers, contractafspraken en exit-strategieën ingezet om het risico te vermijden of te beperken.

Organisatorisch risico 2: Data lock-in
In tegenstelling tot de leveranciers lock-in heeft "slechts" 37% van alle respondenten dit risico benoemd. Geconstateerd is dat zowel de literatuur als de LinkedIn-groepen dit risico hoger schatten (52%). De impact van data die is opgeslagen in een leverancierspecifiek formaat en dus niet kan worden gemigreerd, zien zij als een groot risico. Maatregelen hiervoor zijn voornamelijk standaardisatie, exit-strategieën en zorgvuldige leveranciers- en productselecties.

Organisatorisch risico 3: Imagoschade door toedoen van andere bedrijven
De kans op imagoschade door een andere organisatie door het delen van een cloud omgeving wordt door 49% van de respondenten als risico geïdentificeerd. De verhouding tussen de risicoclassificaties vermijden en verminderen lag dicht bij elkaar, maar de maatregelen zijn wel verschillend. Ter vermijding worden maatregelen als standaardisatie, leveranciersselectie en encryptie genoemd. Ter vermindering ligt de nadruk op eigen beheer en het aanpassen van processen en procedures.

Organisatorisch risico 4: Governance is niet goed geregeld
Het risico op gebrek aan controle en toezicht op beleid, procedures en standaarden is door 44% van de respondenten benoemd, waarbij meer dan de helft van de respondenten aangaf de kans op dit risico te verminderen. Maatregelen die hiervoor genoemd worden zijn het maken van goede contract en/of Service level agreement-afspraken, leveranciersmanagement en kwaliteitsbewaking middels audits.

Organisatorisch risico 5: Cloud leverancier stopt met leveren van diensten
De redenen waarom een cloud leverancier stopt met het leveren van diensten kunnen divers zijn, maar de gevolgen hiervan kunnen grote impact hebben. Dit risico is door 41% van de respondenten geïdentificeerd. Maatregelen ter vermijding en vermindering van het risico zijn het gebruik van meerdere leveranciers, goede contractafspraken en lokale opslag.

Organisatorisch risico 6: Onbekendheid met nieuwe IT-omgeving
Het gebrek aan kennis over de nieuwe omgeving en dus de afhankelijkheid van de kennis van de leverancier wordt als risico door 37% van de respondenten benoemd. Opvallend bij dit risico ten opzichte van de andere organisatorische risico's is dat hier de meest genoemde classificaties accepteren en verminderen zijn. Maatregelen hebben betrekking op het verminderen van de afhankelijkheid van de leverancier door bijvoorbeeld een private cloud te gebruiken.

Organisatorisch risico 7: Databeschikbaarheid en beveiliging
Dit risico op het gebied van algemene databescherming en beschikbaarheid was in het literatuuronderzoek niet zichtbaar geworden. Van de respondenten noemden 16% risico's die hierop betrekking hebben. De maatregelen hiervoor zijn met name risicomijdend: lokale opslag, encryptie en private cloud.

Juridisch risico 1: Privacy van data niet voldoende geborgd
Het risico dat privacygevoelige data beschikbaar is voor onbevoegden is met 80% het meest genoemde risico. Tevens is men zeer duidelijk door met een overgrote meerderheid het risico te classificeren als vermijden. Maatregelen hebben betrekking op onder andere zorgvuldige selectie van producten en leveranciers, toepassen van encryptie en beveiliging, kwaliteitsbewaking en private clouds. Waar de beveiliging van organisatorisch risico 7 betrekking heeft op algemene databescherming gaat dit risico expliciet over het borgen van privacygevoelige data zoals persoonsgegevens.

Juridisch risico 2: Onvoldoende inzicht in naleving van de regels
Ieder land heeft een eigen wetgeving omtrent data en verplichtingen en bevoegdheden van organisaties. Door cloud computing wordt de kans dat wetgeving uit andere landen van invloed is groter. 44% van de respondenten benoemt dit risico, waarbij er geen classificatie speciaal opvalt. Wel zijn er meer maatregelen genoemd voor het vermijden van het risico, waaronder contract- en SLA-afspraken, private cloud en compliance teams, dan voor het verminderen van het risico, waar extern advies en audits worden genoemd.

Juridisch risico 3: Beperkingen door wet- & regelgeving
Landen stellen door onder andere privacywetgeving eisen aan de opslag van data in en de transport van data door landen. Door 41% van de respondenten is dit risico benoemd samen met maatregelen met betrekking tot opslag binnen landsgrenzen, inrichten van compliance teams, private cloud of eigen beheer.

Juridisch risico 4: Documentatie niet (tijdig) beschikbaar voor onderzoek
Indien organisaties documentatie dienen op te leveren in het kader van audits of rechtszaken, ontstaat het risico dat de documentatie niet tijdig beschikbaar is, wat negatieve gevolgen voor het onderzoek kan hebben. In 39% van de reacties is dit risico geïdentificeerd. De classificaties verzekeren, verminderen en vermijden worden hier in oplopende percentages genoemd, met maatregelen als lokale opslag, private cloud en contractafspraken.

Juridisch risico 5: Inbeslagname van data
Doordat meerdere organisaties gebruik maken van één omgeving, ontstaat het risico dat data in beslag wordt genomen op het moment dat één van de organisaties in aanraking komt met justitie. Voor 30% van de respondenten is dit een belangrijk risico. Hierbij kiest het merendeel van de respondenten voor het vermijden van dit risico door goede afspraken in contracten en SLA's met de leverancier en encryptie van data.

Juridisch risico 6: Data ter beschikking van derde partij i.v.m. wet-/regelgeving
Dit risico ligt in het verlengde van risico 1 "privacy van data niet voldoende geborgd", maar is door veel respondenten (24%) afzonderlijk genoemd en was niet afkomstig uit het literatuuronderzoek. Het belang van dit risico wordt duidelijk in het feit dat alle respondenten die dit risico noemen aangeven dit risico te vermijden door de overstap naar een cloud omgeving niet te maken of hooguit de stap naar een private cloud te zetten. Het gaat hierbij niet specifiek om privacygevoelige data, maar ook om andere organisatiedata die men niet openbaar wil geven.

Maatregelen
Door de respondenten zijn diverse maatregelen genoemd. Deze kunnen worden opgedeeld in drie hoofdcategorieën, namelijk techniek, afspraken en organisatie-inrichting.

De technische maatregelen beperken de afhankelijkheid van andere partijen door middel van standaardisatie, exit-strategieën en het gebruik van meerdere leveranciers. Maar ook encryptie en het gebruik van lokale opslag of een private cloud biedt een technische oplossing voor de geconstateerde risico's.
Afspraken met leveranciers in contracten en SLA's zorgen voor een goede relatie tussen afnemer en leverancier(s), waarbij afspraken en verantwoordelijkheden duidelijk onderling zijn afgestemd en vastgelegd.

De laatste categorie betreft de organisatie-inrichting. Door het inrichten van compliance teams, leveranciersmanagement en/of auditteams zorgen afnemers ervoor dat zij minder afhankelijk zijn van externe adviseurs of leveranciers.

Waar de juridische risico's met name worden afgehecht met maatregelen op het gebied van afspraken, zijn er voor de organisatorische risico's meer mogelijkheden. Uit het onderzoek blijkt dat er zes maatregelen zijn die enkel voor de organisatorische risico's gelden en slechts één specifiek juridische maatregel. Maatregelen voor organisatorische risico's kunnen vanuit organisatorisch oogpunt (organisatie-inrichting en afspraken) worden genomen, maar ook kan vanuit de techniek worden gehandeld. Dit zal veelal de eerste stap zijn, omdat hiermee ook eventuele technische risico's worden afgehecht. Daarnaast heeft een organisatie meestal niet de behoefte om de organisatie te wijzigingen bij de implementatie van nieuwe technologieën.

Algemene conclusie
Zowel op organisatorisch als juridisch gebied is slechts één extra risico genoemd ten opzichte van de literatuur. Hierdoor mag als algemene conclusie worden geconstateerd dat de risico's uit de literatuur nog steeds van toepassing zijn voor alle organisaties binnen alle branches die de overstap naar een cloud omgeving willen maken of hebben gemaakt. Door deze risico's te onderkennen en te classificeren kunnen grote gevaren voorkomen worden. Tevens zorgt de risico-inventarisatie en classificatie voor een betere onderbouwing bij de besluitvorming om wel of niet gebruik te gaan maken van een cloud omgeving. Daarnaast bespreekt de literatuur slechts een beperkt aantal mitigerende maatregelen. Het betreffen zowel hoog als laag gewaardeerde maatregelen. Waar de literatuur met name spreekt over techniek gerelateerde maatregelen, geven de respondenten aan ook maatregelen te nemen op het gebied van organisatie-inrichting en contracten. Tevens is in het onderzoek gevraagd naar de risicomethodiek die wordt gehanteerd. Hieruit komt geen eenduidig antwoord, waardoor hier geen conclusies uit getrokken kunnen worden.

1 Inleiding

Dit onderzoek kijkt naar de risico's op organisatorisch en juridisch gebied, waarmee een organisatie rekening dient te houden bij het gebruik van een cloud omgeving. Het onderzoek is uitgevoerd als afstudeeropdracht in het kader van de masteropleiding Business Process Management and IT.

1.1 Achtergrond

De laatste jaren wordt er veel gesproken over cloud computing, waarbij er verschillende definities worden gehanteerd. Het is dan ook veelal een "parapluterm voor verschillende trends in de turbulente IT-wereld" waarbij het uitgangspunt is dat cloud computing betrekking heeft op het direct op aanvraag beschikbaar zijn van onuitputtelijke IT-middelen middels internet (Hilley, 2009).

Vaak wordt de uitgebreide NIST-definitie uit 2009 gehanteerd om duidelijk te maken wat wordt verstaan onder cloud computing (Mell & Grance, 2009):

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort of service provider interaction.

Deze onderdelen worden aangeboden middels drie servicemodellen: Infrastructure-, Platform- en Software-as-a-Service. Bij Infrastructuur-as-a-Service (IaaS) wordt enkel de infrastructuur ter beschikking gesteld en verzorgt de afnemer zelf alle (ontwikkel-)applicaties. Naast de infrastructuur worden bij Platform-as-a-Service (PaaS) ook de programmeertools ter beschikking gesteld. Bij Software-as-a-Service (SaaS) verzorgt de leverancier naast de services infrastructuur en het ontwikkelplatform ook standaardapplicaties. De onderliggende infrastructuur en ontwikkelplatforms zijn hierbij buiten het zicht van de afnemer. Daarnaast zijn er vier deploymentmodellen op basis waarvan een cloud omgeving kan worden gebruikt. De private cloud is een volledig afgeschermd datacenter voor één organisatie. De community cloud is ook nog volledig afgeschermd, maar wordt gebruikt door meerdere organisaties met een gemeenschappelijk doel. Een public cloud wordt aan verschillende bedrijven beschikbaar gesteld. Verschillende bedrijven gebruiken een deel van deze cloud voor hun eigen organisatie. Het vierde model betreft een hybrid cloud waarbij een combinatie van de drie bovenstaande modellen wordt gebruikt. Deze combinatie van karakteristieken, servicemodellen en deploymentmodellen biedt organisaties steeds meer flexibiliteit en mogelijkheden.

Steeds meer bedrijven zijn de afgelopen jaren gebruik gaan maken van een vorm van cloud computing. Hier liggen verschillende redenen aan ten grondslag. De ene organisatie kiest voor een cloud omgeving uit kostenbesparend oogpunt. Een andere organisatie besluit terug te gaan naar zijn core business en (bereidt zich voor om) alle andere werkzaamheden uit te besteden. En weer een andere organisatie kiest voor snellere schaalbaarheid van zijn IT omgeving zonder een nieuw pand aan te kopen of wil simpelweg gebruik maken van de nieuwste moderne technologieën zonder dat er grote investeringen nodig zijn.

Daarnaast zijn er veel organisaties die bewust besluiten om niet over te stappen naar een cloud omgeving. Redenen hiervoor zijn veelal de onbekendheid met de snel veranderende nieuwe markt en onvoldoende inzicht in de risico's en de mogelijke maatregelen hiervoor.

Iedere nieuwe ontwikkeling brengt risico's met zich mee. Voor organisaties is het dan ook van groot belang dat inzichtelijk is welke risico's op kunnen treden en hoe met eventuele nadelige gevolgen wordt omgegaan.

Het onderkennen van risico's is dan ook een belangrijk onderdeel in de besluitvorming om wel of niet de overstap te maken naar een cloud omgeving voor (een deel van) de IT-voorzieningen. Gedeeltelijk zullen deze risico's overeenkomen met de risico's die wellicht reeds onderkend waren vanuit het bestaande datacenter. Chen, Paxson & Katz (2010) geven aan dat problemen zoals phishing en zwakke wachtwoorden ook problematisch waren voor de traditionele webapplicaties en datahosting. Maar door het gebruik van een cloud omgeving ontstaan ook nieuwe risico's door bijvoorbeeld gedeelde fysieke middelen. Of zoals Kim (2009) aangeeft, blijven de zorgen wellicht hetzelfde als in de traditionele omgeving, maar worden de bedrijven zich er meer bewust van doordat de directe invloed op de omgeving, data en resources uit handen is gegeven.

In dit onderzoek worden de risico's met betrekking tot het gebruik van cloud computing nader belicht. Enisa maakte in 2009 een onderverdeling in technische, organisatorische en juridische risico's (Enisa, 2009). Deze drie typen vormen het uitgangspunt in dit onderzoek dat bestaat uit twee onderdelen. Allereerst is een literatuurstudie uitgevoerd. Hierin is op basis van bestaande literatuur van 2008 tot en met 2011 gekeken naar de risico's die zijn onderkend in relatie tot cloud computing. Daarna zijn de resultaten uit deze studie getoetst aan en aangevuld door respondenten uit de praktijk middels een empirisch onderzoek.

In de literatuurstudie is een duidelijk wetenschappelijk beeld geschetst van cloud computing en risicomanagement. Daarna is overeenkomstig de drie bovengenoemde typen inzicht gegeven in de risico's en welke maatregelen hiertegen in de literatuur worden benoemd. Op basis hiervan is een matrix opgesteld met het type risico, de onderkende risico's en de maatregelen om deze risico's tegen te gaan. Dit overzicht is middels een enquête getoetst in de praktijk. Hierbij is gekeken naar welke risico's worden onderkend in organisaties en op welke wijze de organisaties besloten met deze risico's om te gaan. Op basis hiervan is gevraagd naar de maatregelen die worden genomen om het risico te vermijden of verminderen.

Dit alles met als doel inzicht te geven in de meest voorkomende risico's op organisatorisch en juridisch gebied waarmee bedrijven te maken kunnen krijgen bij het gebruik van een cloud omgeving. Tevens worden de belangrijkste maatregelen in relatie tot deze risico's inzichtelijk gemaakt. In de literatuurstudie is uitgegaan van een SaaS-omgeving, om het onderzoek zo breed mogelijk op te zetten. In een SaaS-omgeving worden alle diensten, van infrastructuur tot software, van een derde partij afgenomen, waardoor de risico's toenemen. Problemen die in eigen beheer niet spelen, worden wel inzichtelijk bij de afname van een soortgelijke omgeving bij derden. Daarnaast is uitgegaan van een public cloud aangezien ook hier meer risico's op kunnen treden, welke niet of in beperkte mate spelen bij een private cloud. In het empirisch onderzoek is verder geen onderscheid meer gemaakt in service- en deploymentmodellen. Uit de reacties blijkt dat de stap naar een public cloud voor verschillende organisaties een te grote stap is en dat de private cloud als haalbare tussenstap wordt gezien.

In dit hoofdstuk wordt verder de probleemstelling behandeld samen met de onderzoeksvragen (paragraaf 1.2). Hoofdstuk 2 bevat de literatuurstudie, waarna in hoofdstuk 3 de onderzoeksmethode verder wordt besproken. De resultaten van het onderzoek worden gepresenteerd in hoofdstuk 4. Hoofdstuk 5 bevat de conclusies en antwoorden op de onderzoeksvragen. Tevens worden hier aanbevelingen gegeven voor vervolgonderzoeken. Tot slot wordt in hoofdstuk 6 teruggekeken naar de betekenis en beperkingen van het onderzoek evenals naar het onderzoeksproces.

1.2 Probleemstelling

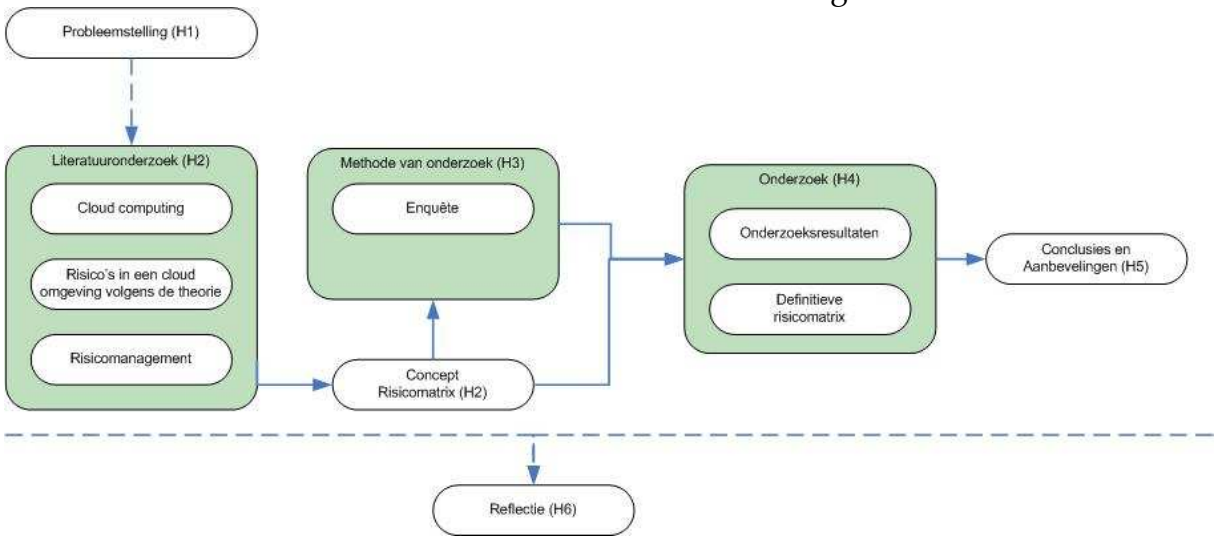
De hoofdvraag van dit onderzoek is: "*Wat zien organisaties als de belangrijkste organisatorische en juridische risico's bij het gebruik van cloud computing en hoe gaan zij met deze risico's om?*"

Het antwoord op deze vraag zal worden gegeven middels een matrix waarin voor alle risico's, uitgesplitst in organisatorische en juridische risico's, aangegeven wordt welke maatregelen kunnen worden gehanteerd ter vermijding en vermindering van het risico. Deze risico's gelden voor iedere organisatie die besluit gebruik te maken van een cloud omgeving voor (een deel van) de IT voorzieningen. Een organisatie dient dan ook te bepalen op welke wijze het risico dient te worden geclassificeerd en welke maatregelen eventueel genomen kunnen worden. De maatregelen uit dit onderzoek kunnen hiervoor worden gebruikt.
Ter beantwoording van de hoofdvraag zijn de volgende onderzoeksvragen geformuleerd:

1. Welke organisatorische risico's worden door organisaties als meest risicovol aangeduid?
2. Wat zijn voor organisaties de belangrijkste juridische risico's?
3. Op basis van welke methode en afspraken zijn deze risico's geïdentificeerd en geclassificeerd?
4. Hoe classificeren de organisaties de benoemde risico's? Worden ze vermeden, geaccepteerd, verzekerd of beperkt?
5. Welke maatregelen worden ingezet om risico's te beperken of te vermijden?

1.3 Aanpak van het onderzoek

De structuur van het onderzoek wordt zichtbaar in het volgende model:



Figuur 1: Het onderzoeksmodel

Op basis van de probleemstelling en de onderzoeksvragen is er een literatuurstudie uitgevoerd. In deze literatuurstudie is stil gestaan bij de definities van cloud computing en risicomanagement en is een wetenschappelijk antwoord geformuleerd op de onderzoeksvragen 1, 2 en 5. Op basis van deze informatie is een risicomatrix gecreëerd. Deze dient als hypothese voor het praktijkonderzoek.
In het praktijkonderzoek zijn zowel de onderzoeksvragen 1, 2 en 5 als de onderzoeksvragen 3 en 4 middels enquêtes voorgelegd aan een grote en diverse onderzoeksgroep. Hierbij is gekeken of de gegevens in de matrix werden bevestigd, aangevuld of volledig gewijzigd.

1.4 Relevantie

Bij het bestuderen van een grote hoeveelheid bestaande literatuur werd duidelijk dat het merendeel van de literatuur ingaat op de techniek achter cloud computing. Hierbij werd veelvuldig gebruik gemaakt van leveranciersvoorbeelden. Voor applicaties werd verwezen naar o.a. Salesforce, Gmail en Google Docs, voor infrastructuur en platforms zijn dit Amazon's EC2, Google Code en Microsoft Azure (Clarke, 2010). Het afnemersperspectief, met de mogelijkheden en risico's die organisaties moet onderkennen bij het gebruik van een cloud omgeving, wordt vaak slechts beperkt besproken in de wetenschappelijke literatuur.

Dit onderzoek heeft voornamelijk betrekking op het afnemersperspectief, doordat is gekozen om de scope te beperken tot de organisatorische en juridische risico's. De technische risico's zijn in de literatuurstudie nog wel meegenomen om het overzicht compleet te maken, maar worden verder in het onderzoek niet meer behandeld. Hiervoor is bewust gekozen omdat de aandacht meestal uit gaat naar de technische risico's en dat aan de organisatorische en juridische risico's relatief minder aandacht wordt besteed. Tevens komen de technische risico's in de literatuur veelvuldig aan bod vanuit het leverancierssperspectief.

2 Literatuurstudie

Dit hoofdstuk bespreekt de theorie en definities van cloud computing en risicomanagement. Tevens wordt een eerste antwoord gegeven op de onderzoeksvragen 1, 2 en 5.

Voor het uitvoeren van het literatuuronderzoek is gebruik gemaakt van de volgende bronnen:
- Koninklijke bibliotheek in Den Haag
- Digital Library van de Open Universiteit
- www.cloudsecurityalliance.org
- www.nist.gov/itl/cloud/

De belangrijkste zoekcriteria betroffen cloud computing, business/technical/legal riks en cloud computing risk mitigation. Daarna heeft verdere verdieping op deze onderwerpen plaats gevonden op basis van de literatuurlijsten in de reeds gevonden literatuur. Hierbij was het uitgangspunt dat, door de snelle ontwikkelingen van de afgelopen jaren, artikelen niet ouder mochten zijn dan 2010. Uitzonderingen zijn gemaakt voor artikelen waar veelvuldig naar werd terugverwezen in de recentere artikelen.

2.1 Cloud computing

Er doen veel verschillende termen over cloud computing de ronde. Cloud computing is veelal een "parapluterm voor verschillende trends in de turbulente IT-wereld" waarbij het uitgangspunt is dat cloud computing betrekking heeft op het op aanvraag beschikbaar zijn van onuitputtelijke IT-middelen middels internet (Hilley, 2009).

Waar veel definities (o.a. Armbrust et al., 2009 en Hilley, 2009) zich vooral richten op de wijze van beschikbaar stellen (Infrastructuur, Platform of Applicaties as a Service), wordt er in andere literatuur juist gekeken naar de basisprincipes die ten grondslag liggen aan deze diensten.

Vanuit de techniek geredeneerd ontstaat de volgende cloud definitie:

> a cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009).

Het National Institute of Standards and Technology (Mell & Grance, 2009) combineert het volledige concept van techniek en gebruik in één definitie:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort of service provider interaction.

Uit deze definitie zijn de volgende vijf karakteristieken te benoemen:

1. On-demand self-service: De cloud afnemer kan, zonder inmenging van de cloud leverancier, IT-faciliteiten (zoals opslagcapaciteit) uitbreiden of toevoegen.
2. Broad network access: Computerfaciliteiten zijn toegankelijk via het netwerk en toegang wordt mogelijk gemaakt door standaard mechanismes.
3. Resource pooling: De leverancier biedt een set generieke IT-faciliteiten aan, met verschillende fysieke en virtuele middelen, welke dynamisch beschikbaar worden gesteld wanneer de afnemer hierom vraagt. De afnemer heeft over het algemeen geen inzicht in de exacte fysieke locatie van de middelen.
4. Rapid elasticity: Capaciteiten kunnen snel, flexibel en soms automatisch worden uitgebreid of beperkt. Voor de afnemer lijkt het alsof er onbeperkte capaciteit op ieder gewenst moment beschikbaar is.
5. Measured Service: Automatische controle en optimalisatie van de middelen vindt plaats door metingen op verschillende, dienstafhankelijke, abstractieniveaus.

Een van de kenmerken van cloud computing, “pay-per-use”, wordt mogelijk gemaakt door de combinatie van resource pooling, waarbij niet meer middelen worden ingezet dan nodig zijn, en measured services, waarbij metingen plaatsvinden op verschillende niveaus.

Daarnaast gaat cloud computing uit van verschillende afnemersvormen. De twee uiterste zijn private en public clouds. De private cloud wordt gebruikt voor organisaties die een cloud bouwen specifiek voor eigen gebruik; een intern datacenter al dan niet gehost door een andere partij. De public cloud is beschikbaar voor iedereen op basis van “pay-as-you-go” (Armbrust et al., 2009).

De NIST-definitie (Mell & Grance, 2011) spreekt over vier deploymentmodellen:

1. Private cloud: Gebruikt door één organisatie, middels een eigen infrastructuur in een eigen, afgescheiden datacenter. Beheer kan plaats vinden door de eigen organisatie of door een derde partij.
2. Community cloud: Gebruikt door meerdere organisaties met een gemeenschappelijk doel, middels een eigen infrastructuur in een gemeenschappelijk datacenter. Het beheer wordt verzorgd door de organisaties of door een derde partij. Een voorbeeld hiervan is een rijksbreed datacenter, waarbij meerdere overheidsorganisaties gebruik maken van gemeenschappelijke locatie, middelen en technische ondersteuning, Hierdoor worden kosten gedeeld en middelen flexibel ingezet naar behoefte.

3. Public cloud: Publiek beschikbaar, ontwikkelaar georiënteerd, gezamenlijke cloud infrastructuur die wordt beheerd door een organisatie die de cloud dienst levert.
4. Hybrid cloud: Een combinatie van de bovenstaande cloud modellen die hun afzonderlijke eigenschappen behouden maar onderling gekoppeld zijn. Bijvoorbeeld een organisatie met vestigingen in meerdere landen, waarbij ieder land gebruik maakt van een eigen private cloud. Deze private clouds worden gekoppeld aan een community cloud voor de hele internationale organisatie.

In de cloud zijn drie servicemodellen mogelijk aldus het NIST. Deze zijn gericht op software, platform en infrastructuur.

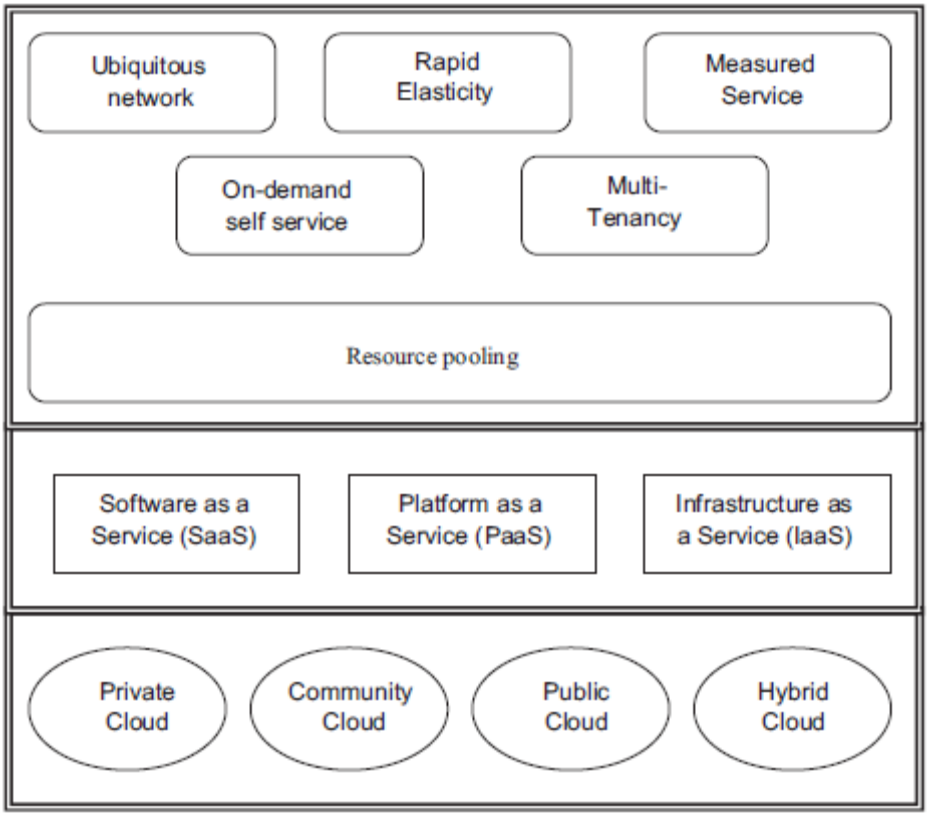
1. Software-as-a-Service (SaaS): Vanuit de cloud worden standaard applicaties aangeboden aan de afnemer. Deze kan de afnemer bereiken via een veelal webgebaseerde interface. Het beheer van de onderliggende infrastructuur (netwerk, servers, besturingssystemen, opslag etc.) wordt door de cloud leverancier uitgevoerd. Uitzonderingen hierop kunnen specifieke afnemersconfiguraties zijn, die alsnog door de afnemer worden beheerd.
2. Platform-as-a-Services (PaaS): De leverancier levert het ontwikkelplatform met de programmeertools. De afnemer kan hierop zelf zijn applicaties ontwikkelen met behulp van deze tools. De leverancier verzorgt tevens het beheer van de onderliggende infrastructuur, maar de afnemer behoudt de controle over de applicaties en bijbehorende configuraties.
3. Infrastructure-as-a-services (IaaS): De leverancier stelt de infrastructuur ter beschikking waarop de afnemer de vrije keus heeft in het gebruik van software (waaronder besturingssystemen en applicaties). Het beheer van de infrastructuur blijft bij de leverancier, maar de afnemer heeft vergaande zeggenschap over de gebruikte netwerkonderdelen.

In figuur 2 wordt de samenhang tussen de karakteristieken, de deployment- en de servicemodellen getoond.

De reden waarom een organisatie de overstap maakt van een fysiek beperkend datacenter naar een cloud omgeving is dat door het aanbieden van Software- en Platform-as-a-Service en middelen op aanvraag:

- de service georiënteerde architectuur kan bijdragen aan het reduceren van IT-overhead voor de eindgebruiker,
- grotere flexibiliteit kan worden gecreëerd,
- de total cost of ownershop (TCO) wordt gereduceerd.

Daarnaast worden mogelijkheden als geavanceerde data-acquisitie, dataopslag, data management, data-integratie en andere serviceprocessen via internet genoemd als voordelen van de overstap naar een cloud omgeving (Mirzaei, 2008).



Figuur 2. Relaties tussen de 5 karakteristieken, de 4 deploymentmodellen en de 3 servicemodellen. (Subashini & Kavitha, 2010)

2.2 Risicomanagement

Een risico start met een bedreiging. Bedreigingen zijn gebeurtenissen die een potentieel verstorende invloed hebben op de betrouwbaarheid van een object (Overbeek, Lindgreen & Spruit, 2005). Niet iedere bedreiging zal leiden tot problemen, doordat niet iedere bedreiging werkelijkheid wordt. Daarom wordt voor iedere bedreiging gekeken naar de kans dat en de gevolgen als de bedreiging werkelijkheid wordt. Op deze manier wordt een bedreiging tot risico gekwantificeerd.

Onder een risico wordt verstaan de kans dat de bedreiging daadwerkelijk zorgt voor een verstoring en wat de negatieve gevolgen hiervan zijn voor de organisatie. Vaak wordt dit aangegeven als Risico = Kans x Impact. Indien een organisatie op basis van de benoemde risico's maatregelen neemt wordt er gesproken over risicomanagement. Risicomanagement betreft dan ook het nemen van beslissingen die gericht zijn op het voorkomen of minimaliseren van de nadelige effecten die het optreden van risico's met zich mee kunnen brengen. Hierdoor is het een stuurinstrument voor de organisatie. Goed risicomanagement zorgt voor een kostenreductie doordat er adequate maatregelen kunnen worden genomen.

Bedreigingen zijn voor iedere organisatie die gebruik maakt van een specifiek object hetzelfde. Het risico is echter afhankelijk van de organisatie. De wijze waarop een organisatie omgaat met de onderkende risico's en welke maatregelen er worden genomen zijn afhankelijk van organisatorische keuzes. Naast de kansen die een risico met zich meebrengt voor een organisatie is ook de risicobereidheid van de organisatie zeer bepalend.

Een organisatie heeft vier opties in de maatregelen die genomen kunnen worden bij de risico's: Accepteren, verzekeren, verminderen en vermijden. Niet alle risico's zijn te verzekeren, denk hierbij aan risico's op het gebied van imagoschade. Voor sommige risico's geldt dat de impact zeer laag is óf de kosten om het risico te voorkomen onevenredig hoog zijn, waardoor gekozen zal worden om het risico te accepteren indien het zich voor gaat doen. Om risico's te vermijden worden preventieve maatregelen ingezet, zodat de kans van optreden wordt voorkomen. Een andere optie om de risico te verkleinen is door in plaats van de kans te beperken, de impact te beperken. Hierdoor wordt het risico niet vermeden, maar wel verminderd.

Risicomanagement is dan ook de combinatie van het identificeren en classificeren van risico's en het benoemen van maatregelen hiervoor. Er zijn veel modellen en procedures voor het inrichten van risicomanagement binnen een organisatie.
In de literatuur worden een paar procedures expliciet in relatie gebracht met cloud computing:

- Risicomanagement op basis van Business Level Objectives met als subproces semi-kwantitatieve BLO-gedreven cloud risico-assessment (Oriol Fitó & Guitart, 2010)
- Risico Breakdown Structure (Tanimoto, Hiramoto, Iwashita, Sato & Kanai, 2011)
- Beveiligingsframework voor cloud computing omgeving (Tabaki, Joshi & Ahn, 2010a)
- Informatiebeveiliging risicomanagement framework (Zhang, Wuwong, Li & Zhang, 2010)

Leidend in alle procedures is de behoefte om de belangrijkste risico's te inventariseren en te beschrijven, waarna de kans en impact worden bepaald. Op basis hiervan kunnen de maatregelen worden vastgesteld om de risico's te beheersen dan wel winstgevend te maken.

De verschillen in de procedures zitten voornamelijk in details en de wijze van weergeven. Oriol Fitó & Guitart (2010) (Figuur 7 in bijlage 2) maken gebruik van *Business Level Objectives (BLO's)* om de risico's te bepalen. Zij bepalen de impact van de risico's ten opzichte van het betreffende business level object in plaats van, zoals bij veel andere assessmentmodellen, de hele cloud organisatie.

Daarbij gebruiken zij een semikwantitatieve BLO-gedreven cloud risico assessment (SEBCRA) om de volgorde en prioritering van de risico's bepalen. Het resultaat van deze vorm van risicomanagement is een overzicht van risico's met het bijbehorende, geschatte risiconiveau, welke individueel worden gespecificeerd voor elk risico en BLO.

Tanimoto et al. (2011) (Figuur 8 in bijlage 2) neemt een breakdownstructuur als uitgangspunt. In een breakdownstructuur wordt de informatie steeds verder in detail uitgewerkt. In dit geval wordt begonnen met de opsplitsing van de risico's in 3 typen. Daarna wordt per type aangegeven welke risico's er worden onderkend. Per risico wordt een classificatie verbonden waarna meer details worden gegeven over de maatregelen die worden gehanteerd.

In het framework van Tabaki et al. (2010a) (Figuur 9 in bijlage 2) worden de risico's bepaald voor service integrators en de service providers, waarbij een verdere uitsplitsing plaats vindt naar service, trust en security management. De samenwerking door verschillende service providers bij de ontwikkeling van nieuwe diensten, wordt gefaciliteerd door service integrators. De risico's hebben dan ook betrekking op de componenten die zorgen voor het opzetten en onderhouden van relaties tussen domeinen, aanbieders, afnemers etc.

Zhang et al. (2010) (Figuur 10 in bijlage 2) maakt gebruik van de "plan, do, check, act"-cyclus als uitgangspunt. In het kader van "Plan" worden de relevante kritische gebieden benoemd, zoals Business Continuity Management, Virtualisatie, Portabiliteit en interoperabiliteit. "Do" heeft betrekking op analyse, benoemen en beperken van de risico's. "Check" en "act" zijn continue lopende monitoring en control acties.

De hierboven genoemde risicomanagement methoden worden visueel getoond in bijlage 2. Bij alle vier de methoden wordt gebruik gemaakt van de standaard classificaties: accepteren, verminderen, vermijden en verzekeren. Indien een organisatie ervoor kiest om het risico te accepteren of te verzekeren, zal deze geen extra mitigerende acties ondernemen. De mitigerende maatregelen die in paragraaf 2.4 worden genoemd, worden dan ook enkel gebruikt indien een organisatie het risico heeft geclassificeerd als "verminderen" of "vermijden".

In paragraaf 2.3 worden, op basis van drie hoofdcategorieën, de risico's benoemd en besproken. Paragraaf 2.4 bespreekt mitigerende maatregelen die, indien gewenst, toegepast kunnen worden op de genoemde risico's. Paragraaf 2.5 bundelt de categorieën, risico's en mitigerende maatregelen samen in een risicomatrix. Hierbij worden de rijen opgesteld op basis van de breakdownstructuur conform Tanimoto et al. (2011). De kolommen zijn gebaseerd op de methode van Oriol Fitó & Guitart (2010).

2.3 Risico's voor de afnemer van cloud omgevingen

De risico's voor een afnemer van een cloud omgeving zijn grofweg in te delen in drie categorieën: Techniek, Organisatie en Juridisch (Enisa, 2009). In de artikelen wordt zeer beperkt onderscheid gemaakt tussen risico's voor een IaaS afnemer ten opzichte van een SaaS of PaaS afnemer. Om het volledige spectrum af te dichten is daarom in de literatuurstudie uitgegaan van een SaaS-afnemer. Deze maakt immers gebruik van het volledige cloud spectrum dat wordt geleverd. Daarnaast wordt uitgegaan van een public cloud omgeving die door een derde partij wordt verzorgd. Natuurlijk gelden de meeste risico's ook voor een private cloud in eigen beheer. Sommige risico's vallen echter weg door de keuze voor een private cloud. Het risico van slechte datascheiding valt bijvoorbeeld weg aangezien er geen andere afnemers van de cloud omgeving zijn. In verband met de omvang van het onderzoek is besloten om alleen de organisatorische en juridische risico's uitgebreid te behandelen. Technische risico's uit de literatuur worden voor de volledigheid benoemd, maar zijn niet verder behandeld in het empirisch onderzoek.

Daarnaast is er ook een groot aantal risico's die niet specifiek betrekking hebben op cloud computing. Iedere organisatie moet aan deze risico's aandacht besteden, ongeacht de wijze van inrichting van hun IT-omgeving. Dit zijn risico's op het gebied van het fysieke netwerk, ongeautoriseerde (fysieke) toegang, natuurrampen, etc. De hieronder genoemde risico's voldoen aan de twee voorwaarden dat ze specifiek voor een cloud omgeving zijn en in meerdere artikelen worden benoemd.

2.3.1 Technische risico's

Technische risico's hebben een directe, technische impact op de cloud waar de afnemer zijn applicaties en data heeft staan. Deze risico's hebben veelal betrekking op beschikbaarheid, integriteit en vertrouwelijkheid.

Data is niet goed afgeschermd voor andere afnemers van dezelfde omgeving

Doordat meerdere bedrijven van dezelfde inrichting en middelen gebruik maken, staat ook de data van meerdere organisaties op dezelfde locatie. De leverancier dient dan ook te voorkomen dat de afnemers bij elkaars data kunnen komen door middel van bijvoorbeeld hacking of code-injecties (Subashini & Kavitha, 2010). Omdat bijvoorbeeld traditionele beveiliging wel werkt tussen hardwarematig gescheiden onderdelen maar niet tussen twee virtuele machines op dezelfde server is het noodzakelijk om zowel externe als interne firewalls te plaatsen, zodat de toegang tot de eigen omgevingen bewaakt kan worden (Ertaul, Singhal & Saldamli, 2010). Dit risico heeft betrekking op de aspecten integriteit en vertrouwelijkheid.

Data wordt onderschept tijdens transport

Door gebruik van een cloud omgeving is het zeer waarschijnlijk dat er meer dataverkeer plaats vindt dan bij een traditionele infrastructuur. Daarbij geldt dat het dataverkeer in een traditionele omgeving plaatsvindt middels een beveiligde verbinding (Subashini & Kavitha, 2010), wat niet altijd het geval is bij gebruik van een cloud omgeving. Hierdoor ontstaat het risico dat de data gedurende het transport wordt bedreigd door bijvoorbeeld sniffing[1], port-scanning[2], man-in-the-middle[3] en Denial of Services aanvallen[4] (DoS) (Enisa, 2009). De mogelijkheid om snel extra capaciteit toe te voegen aan de omgeving kan door een DoS-aanval worden geactiveerd. Hierdoor wordt er onnodig veel extra capaciteit toegevoegd. Indien dit niet tijdig wordt ondervangen, kan dit enorme financiële consequenties met zich mee brengen (Khajeh-Hosseini, Sommerville & Sriram, 2010). Dit risico heeft betrekking op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.

Diensten zijn niet beschikbaar

Doordat de diensten worden aangeboden aan verschillende afnemers, met verschillende wensen en werkzaam op verschillende continenten, is het noodzakelijk dat de services 24/7 beschikbaar zijn. Dit heeft direct invloed op architectuurkeuzes voor applicaties en infrastructuur in het kader van schaalbaarheid en beschikbaarheid. Tevens is een plan voor behoud van bedrijfscontinuïteit en disaster recovery nodig, om onverwachte problemen zo goed mogelijk op te vangen (Subashini & Kavitha, 2010). Het uitgangspunt voor hoge beschikbaarheid is lange tijd het voorkomen van een “single-point-of-faillure” geweest. Door gebruik te maken van één cloud leverancier, zelfs indien deze leverancier beschikt over meerdere datacentra in meerdere regio’s, kan dit uitgangspunt te niet worden gedaan als er op verschillende punten gebruik wordt gemaakt van dezelfde software (Armbrust et al., 2009). Dit risico heeft betrekking op het aspect beschikbaarheid.

Problemen met bewaren of vernietigen

De leverancier is verantwoordelijk voor reguliere back-up van alle bedrijfsgevoelige data om eventuele snelle herstelacties mogelijk te maken. Hierbij is het belangrijk om ook gebruik te maken van encryptie om back-up te beveiligen. Sommige leveranciers zorgen niet standaard voor encryptie. In dit geval is het belangrijk dat de afnemer zelf hiervoor zorgt (Subashini & Kavitha, 2010).

[1] Sniffing betreft het binnenhalen van berichten die voldoen aan specifieke criteria.
[2] Port-scanning Identificeert open poorten.
[3] Bij man-in-the-middle lijkt het alsof er een veilige verbinding is opgezet, maar deze wordt echter volledig gecontroleerd door de aanvaller.
[4] DoS zorgt ervoor dat het netwerk een zeer grote hoeveelheid data ontvangt. De huidige server capaciteit kan dit niet verwerken.

Maar niet alleen het bewaren van de data heeft aandacht nodig. Ook het vernietigen van de data brengt risico's met zich mee. Data moet zorgvuldig worden vernietigd wanneer bijvoorbeeld naar een andere leverancier wordt overgestapt, fysieke hardware wordt verplaatst of data op een andere locatie wordt opgeslagen (Jansen & Grance, 2011). Indien dit niet zorgvuldig gebeurt kan bedrijfsgevoelige data openbaar beschikbaar komen met alle organisatorische en juridische gevolgen van dien. Dit risico heeft betrekking op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.

2.3.2 Organisatorische risico's

Organisatorische risico's zijn bedrijfsgerelateerde risico's waar een organisatie mee te maken krijgt zodra gebruik wordt gemaakt van een cloud omgeving met een cloud leverancier. Deze risico's hebben betrekking op onder andere besturing, leverancierskeuzes, mogelijkheden om over te stappen en imago.

De meest genoemde organisatorische risico's in de literatuur zijn risico's op het gebied van:

Leveranciers lock-in

Het meest genoemde en ook het grootste risico voor een organisatie is het niet kunnen veranderen van leverancier. Standaardisatie op het gebied van tools, procedures, interfaces, etc. is tot op heden slechts zeer beperkt gerealiseerd (Enisa, 2009). Daarbij ontbreekt de behoefte vanuit de leverancier om hier iets aan te doen, mede aangezien daarmee de overstap naar een concurrent wordt vereenvoudigd. Leveranciers staan juist bekend om het creëren van "sticky services" (Ertaul et al., 2010) zodat de overstapmogelijkheden zo veel mogelijk worden beperkt. Echter door de kans op afhankelijkheid van één leverancier die wellicht stopt, onbetrouwbaar blijkt, de technologische ontwikkelingen niet bijhoudt of zijn prijzen verhoogt, besluiten veel organisaties om geen gebruik te gaan maken van cloud computing (Armbrust et al., 2009).

Echter zelfs bij het gebruik van standaarden is een lock-in niet volledig te voorkomen. Slechts een aantal technische issues wordt verholpen middels standaardisatie. Ook indien er geen concurrerende producten bestaan of als een andere leverancier niet hetzelfde gewenste serviceniveau kan leveren (Hilley, 2009) ontstaat er een lock-in situatie. Daarnaast kunnen ontwikkeltools onderdeel zijn van een lock-in, aangezien sommige leveranciers speciale, waardevolle ontwikkelmogelijkheden aanbieden.

Data lock-in

Een speciale vorm van lock-in betreft data lock-in, waarbij de data is opgeslagen in een leveranciersspecifiek formaat (Chow et al., 2009). Veel discussies gaan over de mogelijkheden om de applicatie van de ene leverancier over te zetten naar een omgeving van een andere leverancier. Echter indien de data niet over te zetten is naar een andere leverancier, heeft het weinig meerwaarde om de applicaties wel te verplaatsen.

Het reproduceren van een volledige cloud-based applicatie is eenvoudiger, dan het reproduceren van alle data die in het verleden is opgeslagen. Hierdoor heeft data lock-in de grootste impact (Hilley, 2009).

Governance[5] is niet goed geregeld

Governance impliceert controle en toezicht op beleid, procedures en standaarden, alsmede toetsing van ontwerpen en monitoring. Door de grote beschikbaarheid van cloud diensten ontstaat er een risico met betrekking tot onvoldoende organisatorische controle op medewerkers die zich hiermee bezig houden. Terwijl, dankzij cloud computing, het eenvoudiger wordt gebruik te maken van een ander platform, neemt de noodzaak voor goede besturing hiermee toe.

Een voordeel van cloud computing is dat kapitaalinvesteringen kunnen worden beperkt en omgezet in operationele uitgaven, aangezien met lagere initiële kosten de implementatie van nieuwe diensten kan worden gerealiseerd. Ondanks dat er minder kapitaalinvesteringen worden gedaan, is het belangrijk om de aanschaf van cloud inrichtingen net zo zorgvuldig aan te pakken. Indien dit niet op strategisch en tactisch niveau door de organisatie wordt opgepakt, ontstaan er grote risico's voor de organisatie.

Besluiten kunnen vanuit operationeel oogpunt worden genomen. Het gevolg hiervan is dat onder andere kwetsbare systemen kunnen worden ingezet en wettelijke regels genegeerd, waardoor kosten en risico's alsnog stijgen tot onaanvaardbare niveaus (Jansen & Grance, 2011).

Organisatorische praktijken met betrekking tot het beleid, procedures en standaarden die worden gebruik voor ontwikkeling en dienstverlening in de ruimste zin des woords (ontwerp, implementatie, testen en beheer) moet worden uitgebreid om ook het gebruik binnen de cloud af te dekken. Dit geldt ook voor de afspraken die met de leveranciers worden gemaakt. Zeker indien de cloud leverancier gebruik maakt van een voor de afnemer onbekende, derde partij, ontstaat de kans dat niet alle afspraken volledig zijn afgedicht (Enisa, 2009).

[5] Governance: Term om aan te duiden hoe een onderneming goed, efficiënt en verantwoord geleid moet worden.

Gebruik maken van cloud diensten vereist dus aandacht voor rollen en verantwoordelijkheden, zeker met betrekking tot het beheer van risico's. In plaats van te bepalen hoe data opgeslagen en bewaard moeten blijven, is het noodzakelijker om controlemechanismen en -instrumenten zorgvuldig in te regelen. Daarnaast is het voor een organisatie belangrijk om flexibel om te kunnen gaan met de continu veranderende omgeving, en dus ook verschuivende risico's, zoals wijzigende servicevoorwaarden.

Het afsluiten van een Service Level Agreement (SLA) tussen afnemer en leverancier is dan ook van groot belang. Hierin worden afspraken vastgelegd over de service, prioritering, verantwoordelijkheden en garanties. Omdat de SLA van groot belang is om het gebruik van de IT-middelen te controleren, dient de naleving ervan goed te worden bewaakt (Tabaki, Joshi & Ahn, 2010b).

Imagoschade door toedoen van andere bedrijven

Doordat er meerdere bedrijven gebruik maken van dezelfde cloud omgeving bestaat het risico dat er imagoschade wordt geleden door toedoen van een andere afnemer (Enisa, 2009). Negatieve publiciteit van één afnemer kan uitstralen naar de overige afnemers binnen dezelfde cloud omgeving. Dit kan zelfs zover gaan dat de hele omgeving plat kan worden gelegd in verband met criminele activiteiten. Hierdoor kunnen ook de andere bedrijven in deze omgeving gedurende korte of langere tijd niet bij hun eigen data en applicaties met alle gevolgen van dien. In dit kader speelt ook een juridische issue over wie verantwoordelijk is voor de gevolgschade; de leverancier of de afnemer (Armbrust et al., 2009).

Cloud leverancier stopt met leveren van diensten

Er zijn verschillende redenen waarom een cloud leverancier stopt met het aanbieden van zijn diensten. Dit kan onder andere door het ontbreken van voldoende financiële middelen, een slechte bedrijfsstrategie of ontwikkelingen in de steeds veranderende en ontwikkelende markt, maar ook door teveel technische problemen, zoals veelvuldig en/of langdurig niet beschikbaar zijn, van de omgeving. Ook persoonlijke keuzes om andere diensten te gaan leveren of markten te gaan bedienen, kunnen ervoor zorgen dat de diensten niet meer worden aangeboden (Ertaul et al., 2010).

Wat ook de reden is, de gevolgen voor de afnemer kunnen zeer groot zijn. Het beëindigen van de dienst heeft altijd directe gevolgen voor de afnemer. De dienstverlening en performance nemen af of stoppen zelfs volledig, waarbij ook de investeringen als verloren kunnen worden beschouwd. Daarnaast kan er vervolgschade optreden, doordat de afnemers de dienstverlening aan hun eigen klanten niet meer waar kunnen maken (Enisa, 2009).

Onbekendheid met nieuwe IT-omgeving (bij overstap naar de cloud)

Zoals bij alle opties voor outsourcing is het ook bij de overstap naar een cloud omgeving erg belangrijk dat er goede afspraken worden gemaakt tussen de leverancier en afnemer. Het komt vaak voor dat de afnemersorganisatie, door gebrek aan kennis, beslissingen over details aan de leverancier overlaat. Daarbij is er vaak slechts beperkte kennis over de wijze waarop de diensten uitgevoerd zouden moeten worden en uitgevoerd worden. Door het verschil in kennis tussen de afnemer en de leverancier ontstaat het risico dat de contractuele voorwaarden worden gedicteerd door de leverancier met weinig tot geen input vooraf en ruimte voor onderhandelingen door de afnemer.

Hierdoor ontstaat een aanzienlijk voordeel voor de leverancier (Clarke, 2010). Tevens is de kans op veranderingen op het gebied van interfaces, beveiligingseisen en -investeringen, ten opzichte van de oorspronkelijke traditionele omgeving, nadrukkelijk aanwezig. Dit kan uiteindelijk zeer schadelijk zijn voor de reputatie van de afnemersorganisatie en het vertrouwen van zowel klanten als eigen personeel in de organisatie (Enisa, 2009).

2.3.3 Juridische risico's

Risico's vanuit juridisch oogpunt kunnen vaak met technische middelen worden vermeden of verminderd. Het betreft voornamelijk risico's die ontstaan door verschillen in de landelijke wetgevingen of doordat er meerdere partijen (afnemer, leverancier en eventueel onderleverancier) betrokken zijn bij het gebruik van de cloud.

Inbeslagname van data

In een public cloud worden de technische middelen gedeeld met andere bedrijven. Enkel al door het gebruik van dezelfde omgeving ontstaat het risico op inbeslagname van de bedrijfsdata. Deze inbeslagname kan plaatsvinden doordat een ander bedrijf, binnen dezelfde cloud, in aanraking komt met justitie (Jansen, 2011). Een dagvaarding verplicht de leverancier toegang te verlenen tot alle data in de betreffende omgeving (Ertaul et al., 2010). De omvang hiervan is door de gecentraliseerde opslag van data en de gedeelde fysieke hardware zeer groot. Bij inbeslagname van de fysieke hardware is de kans dat bedrijfsdata door ongewenste partijen wordt ingezien dan ook zeer groot (Enisa, 2009).

Documentatie niet (tijdig) beschikbaar voor onderzoeken

Aan het begin van een juridisch proces worden elektronische documenten geïdentificeerd, verzameld, verwerkt, geanalyseerd en geproduceerd. Dit wordt in de literatuur vaak e-discovery genoemd. Daarnaast zijn organisaties ook op andere momenten verplicht om documentatie op te leveren, bijvoorbeeld om te voldoen aan audit verzoeken.

Onder documentatie worden niet alleen e-mails en bijlagen verstaan, maar ook metadata zoals datum van ontwerp, wijzigingen, etc. (Jansen & Grance, 2011). Doordat deze informatie bij de cloud leverancier is opgeslagen ontstaat het risico dat de afnemer niet of niet tijdig de benodigde documentatie op kan leveren, wat negatieve gevolgen kan hebben op lopende onderzoeken.

Beperkingen door wet- & regelgeving

Door het gebruik van cloud omgevingen is het voor afnemers niet eenvoudig te achterhalen waar hun data is opgeslagen. Dit kan een probleem zijn in het kader van naleving van privacywetgevingen, welke afhankelijk zijn van het land waar de data is opgeslagen. Daarbij geldt dat niet alle landen de internationale regelingen respecteren (Enisa, 2009).

Om te weten onder welke wetgeving de data valt is het belangrijk om te weten waar de data is opgeslagen. Zodra data echter over de nationale grenzen gaat, wordt het extreem moeilijk om beveiliging door buitenlandse wet- en regelgeving te garanderen (Jansen, 2011). Daarnaast geldt in veel Europese en Zuid-Amerikaanse landen dat privacygevoelige data het land niet mag verlaten. Het belang om te weten onder welke wetgeving de data valt, is ook nadrukkelijk aanwezig wanneer er een onderzoek wordt ingesteld. Een extra risico in dit kader is dat bij een cloud de kans aanwezig is dat data op meerdere locaties gelijktijdig is opgeslagen, waarbij deze locaties verschillende juridische regelgeving kennen.

In de Verenigde Staten is de afgelopen jaren een groot aantal richtlijnen opgesteld om de juridische risico's af te hechten. Richtlijnen voor specifieke sectoren zijn het Health Insurance Portability and Accountability Act (HIPAA), welke vooral gericht is op medische informatie, en de Gramm-Leach-Bliley Act voor de financiële sector. Daarnaast zijn er nog State Information Security Laws, welke per staat zijn opgesteld. Ook zijn er State Breach Notification Laws en heeft de HITECH een Breach Notification opgesteld (Sotto, Treacy & McLellan, 2010).

De Patriot Act is opgesteld na de aanslagen van 11 september 2001 met als doel terrorisme te belemmeren. Middels deze wet heeft de Amerikaanse regering het recht om alle data op te eisen van alle computers van Amerikaanse bedrijven, zelfs wanneer deze zich niet op Amerikaans grondgebied bevinden (Mahmood, 2011). Hierdoor kan ook data die in Nederland op een server is geplaatst worden opgeëist indien de leverancier onder de Amerikaanse wetgeving valt.

In Europa is er pas sinds kort aandacht voor regelgeving omtrent cloud computing. De belangrijkste regelgeving hierin is dat het enkel is toegestaan om privacygevoelige data buiten de EU te transporteren, naar specifiek genoemde landen met een adequaat beveiligingsniveau (Clarke, 2010). Hierbij geldt tevens als restrictie dat het transport dient plaats te vinden door landen die ook voldoen aan het beveiligingsniveau. Doordat bij een cloud dit vaak erg ondoorzichtig is, is het van groot belang dat er goede afspraken worden gemaakt met de leverancier om aan deze vereisten te voldoen (Sotto, Treacy & McLellan, 2010).

Privacy van data niet voldoende geborgd

Cloud diensten bestaan, naast de zakelijke diensten, in veel variaties waaronder videosites, medische dossiers (EPD) en documentuitwisseling. Dit heeft een grote impact op de privacy van persoonlijke informatie en de vertrouwelijkheid van bedrijfs- en overheidsinformatie (Subashini & Kavitha, 2010). De borging van deze privacy varieert significant en is afhankelijk van het privacybeleid van de cloud leverancier. Daarnaast heeft ook de opslaglocatie impact op de privacy borging (zoals aangegeven bij het vorige punt).

Cloud leveranciers dienen te streven naar een hoger niveau van beveiliging en privacybescherming dan dat geldt voor een lokaal, traditioneel datacenter (Kim, 2009). Hierbij moet in ogenschouw worden gehouden dat de opslaglocaties een steeds aantrekkelijker doelwit worden voor aanvallen, doordat meerdere bedrijven van dezelfde locaties gebruik maken (Jansen, 2011), waardoor de impact van een succesvolle aanval groter is.

Onvoldoende inzicht in naleving van de regels

Er kunnen, met name voor Europese bedrijven, serieuze compliance problemen ontstaan in relatie tot de juridische aspecten. Als voorbeeld wordt genoemd dat het volgens de Europese wetgeving enkel is toegestaan om persoonlijke data te transporteren en op te slaan in landen met een adequaat beveiligingsniveau (Jansen & Grance, 2011). Om zeker te weten dat deze regels worden nageleefd is het noodzakelijk dat een leverancier aan kan tonen dat de data enkel via netwerken in deze landen wordt verplaatst, dan wel opgeslagen. Afnemers moeten juridisch gezien zelf kunnen aantonen dat zij voldoen aan de verschillende, van toepassing zijnde, wetgevingen. Hiervoor dienen goede afspraken te worden gemaakt met de leveranciers. Om dit alles mogelijk te maken, doen leveranciers er goed aan om verschillende technologieën te adopteren (Kim, 2009) .

2.4 Mitigerende maatregelen

Afhankelijk van de strategie van de organisatie worden bovengenoemde organisatorische en juridische risico's geaccepteerd, verzekerd, vermeden of verminderd. Voor de risico's met de classificatie verminderen en vermijden, kunnen verschillende maatregelen worden ingezet. De belangrijkste maatregelen worden hieronder benoemd. Sommige maatregelen zullen meerdere risico's in meer of mindere mate afdekken. Daarnaast kan het nodig zijn om meerdere maatregelen te nemen om het risico te vermijden of te verminderen tot een acceptabel niveau.

Standaardisatie

Standaardisatie zorgt ervoor dat de gevolgen van verschillende risico's worden beperkt. Dit kan door het gebruik van open source of leveranciers onafhankelijke technieken op onder meer het gebied van dataopslag, migratiestrategieën (om de overgang naar een andere provider te vereenvoudigen) of programmeertalen. Dankzij standaardisatie kan er marktwerking ontstaan met een positieve invloed op prijs en mogelijkheden. Tevens zorgt standaardisatie voor betere samenwerking met andere producten. Hierdoor wordt enerzijds de kans op een leveranciers- en/of een data lock-in verkleind. Anderzijds draagt standaardisatie ook bij aan het reduceren van de gevolgen wanneer de leverancier besluit te stoppen met het aanbieden van diensten.

Ook wordt de techniek voor de afnemer inzichtelijker waardoor bij de overstap naar een (andere) cloud leverancier de afnemersorganisatie betere afspraken kan maken met de nieuwe leverancier (Hilley, 2009). Standaardisatie draagt dus bij aan het beperken van meerdere, voornamelijk organisatorische, risico's.

Encryptie door leverancier en afnemer

Een reeds bekende maatregel in een fysiek datacenter is encryptie op afnemersniveau. Ook binnen de cloud is dit een belangrijke maatregel om de gevolgen van veel risico's te beperken. Vanuit technisch oogpunt worden met encryptie de risico's beperkt in het kader van toegang tot data door onbevoegden. Maar ook het niet volledig verwijderen van gevoelige data heeft minder verstrekkende gevolgen indien er gebruik wordt gemaakt van sterke encryptie (Enisa, 2009). Evenals dat het lekken van gevoelige informatie tijdens transport of back-up kan worden voorkomen door het gebruik van encryptie protocollen zoals SSL en TLS[6] (Subashini & Kavitha, 2010).

[6] SSL: Secure Socket Layer, TLS: Transport Layer Security: Protocol voor een beveiligde verbinding met internet door middel van cryptografie en authenticatie waardoor data niet kan worden afgeluisterd of vervalst.

Daarnaast heeft de organisatie ook een organisatorisch en juridisch voordeel van goede encryptie. Bij inbeslagname van de cloud omgeving, door problemen met een andere afnemer, wordt de leverancier verplicht om alle data en autorisaties daarvoor beschikbaar te stellen. Indien de afnemer zelf zorgt voor de encryptie van zijn data, beschikt de leverancier niet over autorisaties en kan deze dus ook niet overdragen aan de rechtbank. Om de data alsnog beschikbaar te krijgen, is er een afzonderlijke dagvaarding nodig om de afnemersorganisatie te verplichten zijn bedrijfsdata beschikbaar te stellen voor onderzoek (Ertaul et al., 2010).

Gebruik maken van meerdere leveranciers

Door gebruik te maken van meerdere leveranciers kunnen zowel organisatorische, juridische als technische gevolgen beperkt worden. De belangrijkste reden om voor meerdere leveranciers te kiezen betreft de garantie op beschikbaarheid van de bedrijfsomgevingen. Door gebruik te maken van geautomatiseerde, reguliere back-ups, zodat beide omgevingen identiek aan elkaar zijn, kan normaal worden doorgewerkt ook als één van de omgevingen onbereikbaar is (Ertaul et al., 2010). Daarnaast wordt de kans op een leveranciers of een data lock-in tot een minimum beperkt omdat reeds van meerdere diensten en technologieën gebruik wordt gemaakt. Dit zou theoretisch ook bij één leverancier kunnen, maar het is voor een leverancier zeer lastig om twee volledig verschillende inrichtingen aan te bieden (Armbrust et al., 2009). Onbekend is echter of het haalbaar is om bij verschillende leveranciers overeenkomstige diensten in te kopen, waarbij onderlinge uitwisselbaar haalbaar is. Een minimale vereiste hiervoor is vergevorderde standaardisatie op het gebied van onder andere applicaties, dataopslag en uitwisselingsprotocollen.

Een ander gevolg van het feit dat het bijna onmogelijk is om twee volledig verschillende clouds aan te bieden, is dat het creëren van “geen single-point-of-faillure” onmogelijk is. “Geen single-point-of-faillure” is lange tijd het uitgangspunt geweest voor hoge beschikbaarheid. De enige manier waarop de beschikbaarheid van services zo goed mogelijk gegarandeerd kan worden is door gebruik te maken van verschillende leveranciers (Armbrust et al., 2009). En zelfs dan is 100 procent beschikbaarheid niet mogelijk zonder gebruik te maken van een lokaal datacenter (Kim, 2009).

Tevens biedt het gebruik van meerdere leveranciers mogelijk oplossingen in het kader van de wetgeving dat privacygevoelige data niet door alle landen mag worden getransporteerd en/of mag worden opgeslagen. Door gebruik te maken van een lokale leverancier kan dit deel van de opslag worden geregeld, terwijl voor niet gevoelige data of applicaties gebruik kan worden gemaakt van andere leveranciers. Hierbij dient nog steeds rekening te worden gehouden met het risico van single-point-of-failure voor beide leveranciers, aangezien zij niet als back-up van elkaar kunnen worden ingezet.

Lokale opslag

Door te kiezen voor lokale opslag van data of applicaties in een eigen datacenter of private cloud worden sommige risico's acceptabel. Gevolg hiervan is wel dat er geen (volledige) overstap wordt gemaakt van een cloud omgeving. In het kader van beschikbaarheid kan worden besloten om een lokale versie van de applicatie te hebben. Op deze manier komt het werk niet stil te liggen, wanneer de cloud omgeving niet beschikbaar is. Dit zal met name worden ingezet door organisaties waar beschikbaarheid zeer grote invloed heeft op de core business, aangezien dit extra kosten met zich mee brengt.

Ook in het kader van bedrijfskritisch en/of privacygevoelige informatie kan lokale opslag zorgen voor het verminderen van de risico's voor organisaties. Door de lokale opslag nemen tevens de kans op het onderscheppen van data gedurende transport, ongeautoriseerde toegang binnen de cloud en imagoschade af. Daarnaast lost het problemen op in het kader van de privacy- en internationale wet- & regelgeving op, doordat bekend is waar de desbetreffende data is opgeslagen (Kim, 2009).

Afsluiten Service Level Agreement

Een andere maatregel die niet alleen dient om risico's te verminderen maar ook om ze te vermijden, betreft het opstellen van een Service Level Agreement (SLA) tussen afnemer en leverancier. Deze SLA dient met alle partijen opgesteld te worden, zodat inzichtelijk is welke afspraken er zijn gemaakt en wie verantwoordelijk is voor welke dienst, risico en gevolgen. In sommige gevallen kan het wenselijk zijn om een derde partij in te schakelen met specifieke expertise die zorgt voor goede afspraken en onafhankelijke controle.
De belangrijkste punten die volgens Ramgovid, Eloff & Smith (2010) in een SLA moeten worden opgenomen zijn:

- Geleverde diensten en de prestatieafspraken
- Bewaking en rapportages
- Probleembeheer
- Wettelijke eisen waaraan wordt voldaan
- Oplossen van geschillen, klachten
- Verantwoordelijkheden omtrent beveiliging
- Omgang met vertrouwelijke informatie, opslag en vernietiging

Deze afspraken helpen beide partijen op het moment dat er een geschil optreedt of dat er misbruik van buitenaf optreedt.

2.5 Literatuurresultaten en conclusies

Met behulp van een risicomatrix (zie matrix 1) kan een theoretisch antwoord worden gegeven op de centrale onderzoeksvraag. Vastgesteld is dat cloud computing bestaat uit een vijftal kenmerken (on-demand self service, broad network access, resourcepooling, rapid elasticity en measured services) welke vanuit een private, community, hybrid of public cloud aan de afnemer beschikbaar kunnen worden gesteld. Hierbij is het aan de afnemer om te bepalen in welke mate de IT diensten (infrastructuur, platform of software) worden afgenomen van een derde partij, dan wel door de organisatie zelf worden verzorgd.

In alle gevallen dient de afnemer te onderkennen dat er risico's zijn die kunnen leiden tot technische verstoringen of organisatorische problemen. De impact en kans van optreden van deze risico's zijn voor iedere organisatie anders en worden mede bepaald door de visie en strategie van de organisatie. Vanuit deze basis is het mogelijk geweest om een matrix op te stellen met de belangrijkste organisatorische, juridische en technische risico's welke in detail zijn uitgewerkt in paragraaf 2.3 in samenhang met mogelijke mitigerende maatregelen (paragraaf 2.4).

Uit de gecreëerde matrix wordt tevens duidelijk dat veelal de afnemer verantwoordelijk is voor het verminderen van de risico's. Niet verwonderlijk aangezien dit ook de partij is die de gevolgen van het optreden van een risico draagt.

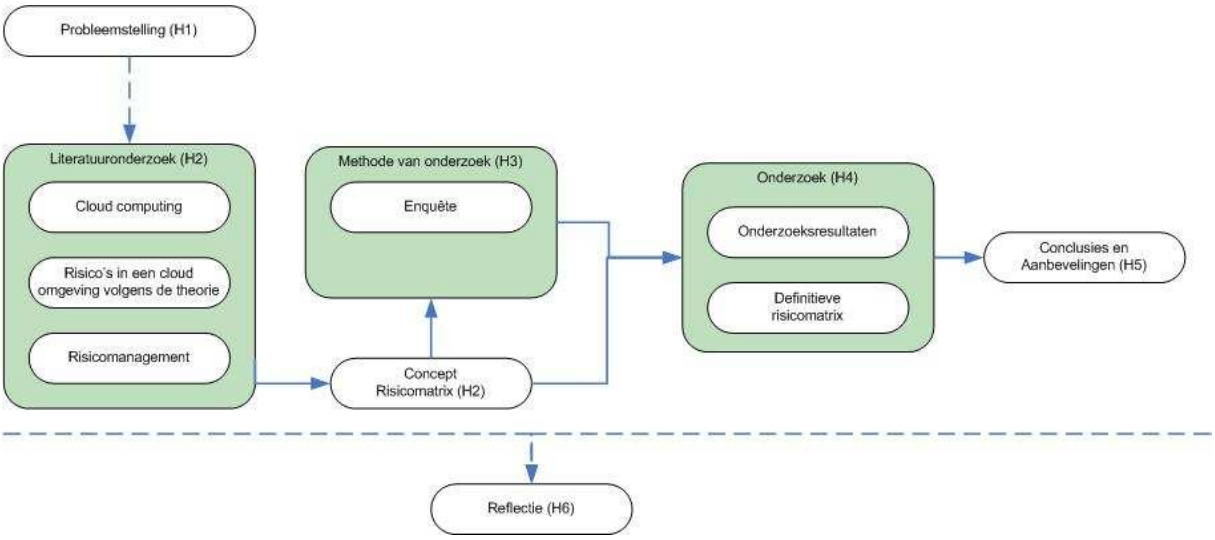
Categorie	Risico	Standaard-isatie	Gebruik meerdere leveranciers	Afsluiten SLA	Lokale Opslag	Encryptie	Leverancier	Afnemer
Organisatorisch	Leveranciers lock-in	x	x				x	x
	Data lock-in	x	x				x	x
	Governance is niet goed geregeld	x		x			x	x
	Imagoschade door toedoen van andere bedrijven		x					x
	Cloud leverancier stopt met leveren van diensten	x	x				x	x
	Onbekendheid met nieuwe IT-omgeving (bij overstap naar de cloud)	x		x			x	x
Juridisch	Inbeslagname van data				x	x		x
	Documentatie niet (tijdig) beschikbaar voor onderzoeken				x			x
	Beperkingen door wet- & regelgeving		x	x	x			x
	Privacy van data niet voldoende geborgd			x	x	x	x	x
	Onvoldoende inzicht in naleving van de regels				x			x
Technisch	Data is niet goed afgeschermd voor andere afnemers van dezelfde omgeving					x	x	
	Data wordt onderschept tijdens transport					x	x	
	Diensten zijn niet beschikbaar		x					x
	Problemen met bewaren of vernietigen			x	x	x	x	x
	Leverancier	x				x		
	Afnemer	x	x	x	x	x		

Matrix 1: Organisatorische, juridische en technische risico's uit de literatuur.

De matrix bevat de in de literatuur genoemde risico's met betrekking tot cloud computing. Deze matrix geldt, conform figuur 1, als input voor het vervolgonderzoek. In hoofdstuk 3 wordt meer aandacht besteed aan de onderzoeksaanpak.

3 Methode van onderzoek

Het literatuuronderzoek heeft een concept risicomatrix opgeleverd met eerste antwoorden op de onderzoeksvragen. Deze matrix wordt in de praktijk getoetst overeenkomstig het onderzoeksmodel zoals besproken in paragraaf 1.3. Dit hoofdstuk beschrijft de onderzoeksmethode middels een conceptueel en technisch onderzoeksontwerp. Ter verduidelijking wordt nogmaals het onderzoeksmodel getoond. Figuur 3 is volledig identiek aan figuur 1.



Figuur 3: Het onderzoeksmodel (= figuur 1)

3.1 Conceptueel onderzoeksontwerp

Het conceptueel onderzoeksontwerp bevat een overzicht van de onderzoeksdoelgroep en de geeft meer inzicht in de begrippen die gebruikt zijn tijdens het onderzoek.

3.1.1 Onderzoeksdoelgroep

Om inzicht te krijgen in algemeen geldende risico's is het noodzakelijk om het onderzoek uit te voeren onder een brede en omvangrijke doelgroep. Deze doelgroep diende te bestaan uit medewerkers van verschillende bedrijven en verschillende branches. Tevens mocht de doelgroep niet bestaan uit met name leveranciers, maar diende juist ook de afnemers deel uit te maken van de doelgroep.

Om deze doelgroep te bereiken is gekozen voor drie LinkedIn-groepen. De leden van deze groepen zijn afkomstig van verschillende organisaties en hebben vergaande belangstelling dan wel ervaring met het onderwerp. De keuze voor deze LinkedIn-groepen is gemaakt op basis van de twee onderwerpen: Risico's en Cloud computing. In alle drie de groepen vindt informatie-uitwisseling plaats over deze onderwerpen.

De LinkedIn groep Platform van InformatieBeveiliging (PvIB) betreft enkel leden van het PvIB. Dit platform verenigt betrokkenen in het vakgebied informatiebeveiliging en verzamelt kennis en ervaring op dit vakgebied. Deze groep is geselecteerd in het kader van risicomanagement en beveiliging en bestaat uit 483 leden.

Achter de groep Cloud Computing Nederland (CCN) zit onder andere EuroCloud. Deze stichting is een onafhankelijke community en legt een brug tussen industrie, eindgebruiker en politiek. Hierdoor wordt verwacht dat deze groep voldoende inzicht heeft in de risico's met betrekking tot cloud omgevingen. De 734 leden zijn onder andere werkzaam als consultant, ondernemer of engineer en bespreken uitgebreid hun kennis en ervaringen op het gebied van cloud computing en privacy.

De derde groep die gekozen is, betreft de Cloud Security Alliance (CSA). Zij hebben diverse artikelen geschreven over risico's in relatie tot cloud computing. De CSA gaf aan ook een Nederlandse afdeling te hebben. Doordat de behoefte bestond voornamelijk Europese bedrijven te hebben (in verband met het verschil in privacywetgevingen), is ervoor gekozen om deze groep te beperken tot de Nederlandse afdeling (CSA-N) met 101 leden.

Voorafgaand aan het onderzoek is contact geweest met de coördinatoren van de groepen. Aan deze coördinatoren is enerzijds toestemming gevraagd om het onderzoek uit te voeren. Anderzijds is geïnformeerd of zij verwachten dat hun leden zouden helpen bij het onderzoek. Beide vragen werden door alle coördinatoren positief beantwoord.

Desondanks blijft het risico bestaan dat deze wijze van onderzoek te weinig reacties genereert. Respondenten worden immers niet persoonlijk aangesproken en e-mailberichten belanden eenvoudig op een grote stapel door drukte, feestdagen en afwezigheid. Er waren twee maatregelen mogelijk om dit risico te verminderen. Enerzijds de mogelijkheid van persoonlijke interviews, maar hiermee werd de doelstelling om een zo breed mogelijke doelgroep te bereiken te niet gedaan. Anderzijds door het informeren van mijn eigen zakelijk netwerk over dit onderzoek. Diverse leden uit de drie groepen zijn ook hierin vertegenwoordigd en publiciteit is, door gebrek aan één-op-één communicatie, noodzakelijk om voldoende respons te ontvangen. Hiermee werd de doelstelling gehandhaafd en besloten is dan ook om deze maatregelen gelijktijdig in gang te zetten.

3.1.2 Respondenten

De bovenstaande onderzoeksdoelgroep heeft uiteindelijk geresulteerd in 63 respondenten. Deze respondenten werkten voornamelijk bij een Nederlandse organisatie. Slechts eenmaal is aangegeven dat voor een organisatie wordt gewerkt uit een ander land, namelijk Frankrijk. Door het ontbreken van Amerikaanse organisaties, zijn de reacties in het kader van de opslaglocatie van data, zeer unaniem.

Van 13 respondenten is niet alle informatie beschikbaar. Deze respondenten hebben om verschillende redenen de vragenlijst niet volledig ingevuld. Hierdoor is onbekend in de branche de respondent werkzaam is evenals bij de wijze waarop de respondenten de vragenlijst heeft ontvangen.

De core business van de organisaties waarvoor de respondenten werkzaam zijn, loopt uiteen van overheid en defensie tot ICT of juridische dienstverlening, ingenieursbureaus, farmaceutische industrie en gezondheidszorg.

Er zijn 11 branches vertegenwoordigd in dit onderzoek:
- 1 respondent uit de branche Bouwnijverheid
- 1 respondent uit de branche Groot- & detailhandel
- 1 respondent uit de branche Horeca
- 2 respondenten uit de branche Gezondheids- & welzijnszorg
- 2 respondenten uit de branche Overige dienstverlening
- 2 respondenten uit de branche Overig
- 3 respondenten uit de branche Industrie
- 4 respondenten uit de branche Financiële dienstverlening
- 8 respondenten uit de branche Informatie & Communicatie
- 11 respondenten uit de branche Zakelijke dienstverlening
- 15 respondenten uit de branche Openbaar bestuur/Overheid

Van 13 respondenten ontbreekt de informatie over welke branche zij vertegenwoordigen.

De respondenten zijn voornamelijk werkzaam als architect, consultant/adviseur, projectleider/manager of in leidinggevende functies in het midden of hoger kader. Aangezien risicoanalyse en beheersing ook met name bij het tactisch en strategisch management is belegd, komt dit overeen met de verwachtingen.

Het percentage gebruik van de cloud omgeving is wellicht nog de meest opvallende algemene informatie. Slechts een kwart van de respondenten werkt in een organisatie waar voor meer dan de helft van de IT-dienstverlening gebruik wordt gemaakt van een cloud omgeving. Dit verklaart wel de veelgenoemde maatregel om niet naar een cloud omgeving over te willen stappen zolang sommige risico's niet voldoende kunnen worden afgedekt.

Ondanks dat er voldoende respondenten zijn geweest, dient wel geconstateerd te worden dat het gebruik van LinkedIn-groepen niet zorgde voor voldoende respons. Slechts 32% van de reacties is ontvangen vanuit de aangegeven discussiegroepen. Hierbij is het PvIB met 24% het beste vertegenwoordigd. De CSA en CCN brachten een respons van respectievelijk 3% en 5% in. Daarnaast is het eigen zakelijke eerste- en voornamelijk tweedelijns netwerk verantwoordelijk voor 48% van de reacties. Van de overige 20% is onbekend op welke wijze de vragenlijst is ontvangen.

3.1.3 Operationalisering van begrippen

In het onderzoek komen diverse begrippen voor. Om de antwoorden van het onderzoek eenduidig te kunnen interpreteren is besloten om alle belangrijke begrippen te verklaren. Naast het begrip cloud computing (zie voor definitie paragraaf 2.1) zijn de volgende begrippen verklaard:

- O*rganisatorisch risico:* heeft betrekking op bedreigingen met een negatieve invloed op de strategische doelstellingen van de organisatie. Sterke afhankelijkheid van bijvoorbeeld leveranciers of producten leidt tot grotere risico's.
- J*uridisch risico:* betreft risico's van veranderingen in en naleving van wet- en regelgeving. Ook onjuist gedocumenteerde of niet afdwingbare contractuele bepalingen, alsmede de kans op bedreigingen van de rechtspositie vallen onder juridische risico's.

Voor het classificeren van de risico's wordt gebruik gemaakt van vier classificaties (Tanimoto et al., 2011).
- *Accepteren (acceptance)*: De risico's worden onvoorwaardelijk geaccepteerd.
- *Vermijden (avoidance)*: Een risico wordt vermeden en alternatieven worden ingezet.
- *Verminderen (mitigation)*: Het risico wordt verminderd tot een niveau dat het risico kan worden geaccepteerd.
- *Verzekeren (transference)*: Het risico wordt overgedragen aan een derde partij.

3.2 Technisch onderzoeksmodel

3.2.1 Onderzoeksstrategie

Voor de uitvoering van het onderzoek is gekozen voor een schriftelijke enquête. De keuze hierop is gevallen om een zo groot mogelijke onderzoeksgroep te bereiken. Aangezien de verwachting is dat risico's en risicowaardering door iedere organisatie anders worden bepaald, ontstaat het gevaar dat bij een zeer beperkte onderzoeksgroep geen overeenkomsten ontstaan. Door een grote onderzoeksgroep te raadplegen wordt de kans vergroot om te komen tot een overzicht van gemeenschappelijke risico's met bijbehorende maatregelen.

In de vragenlijst is duidelijk gemaakt dat de gegevens anoniem worden behandeld en dat in het onderzoeksrapport geen antwoorden te herleiden zijn naar specifieke organisaties.

Door op deze wijze het onderzoek uit te voeren is het mogelijk om dit onderzoek te repliceren op een later tijdstip, dan wel verdere detaillering toe te voegen voor specifieke doelgroepen.

3.2.2 Analyse

Gebruik wordt gemaakt van primaire gegevens die middels een vragenlijst zijn uitgezet bij de in paragraaf 3.1.1 genoemde partijen. Als input voor deze vragenlijst zijn de resultaten uit de risicomatrix gehanteerd. Daarbij wordt de respondenten de mogelijkheid geboden om eigen risico's te bespreken. De complete vragenlijst is opgenomen in bijlage 3. De onderzoeksresultaten worden afhankelijk van de vraag kwantitatief of kwalitatief geanalyseerd. Vragen over de genoemde risico's en de bijbehorende classificatie worden kwantitatief geanalyseerd. De maatregelen en acties worden kwalitatief geanalyseerd. De uiteindelijke resultaten worden verwerkt in de definitieve risicomatrix.

3.2.3 Validatie en betrouwbaarheid

Het is belangrijk om in dit onderzoek stil te staan bij de validatie en betrouwbaarheid van dit onderzoek. Op basis van de onderzoeksdoelgroep van 1318 personen zijn er minimaal 298 respondenten noodzakelijk voor een betrouwbaarheidspercentage van 95% en een foutmarge van 5%. Er zijn ongeveer 50 personen die binnen meerdere onderzoeksgroepen actief zijn. Dit is nog geen 5%, waardoor het effect op de foutmarge te verwaarlozen is. Voor de resultaten in het onderzoek is uitgegaan van de groep die de deelnemer zelf heeft aangegeven in de vragenlijst.

De doorlooptijd van het onderzoek is beperkt tot één maand, mede waardoor het aantal van 298 niet is gehaald. Bij het stopzetten van het onderzoek waren er 63 vragenlijsten voldoende ingevuld om te kunnen gebruiken bij dit onderzoek. Dit betekent dat 63 respondenten de vragen over de risicomethodiek en de organisatorische risico's volledig hadden beantwoord. Met een gelijkblijvend betrouwbaarheidspercentage van 95% levert dit een foutmarge op van 12,05% voor de organisatorische risico's. Concreet betekent dit dat bij een herhaling van het onderzoek 22 van de 25 antwoorden overeen komen met de huidige resultaten.

Niet in alle vragenlijsten waren ook de juridische risico's volledig ingevuld. Als duidelijke reden hiervoor is door verscheidene respondenten expliciet aangegeven in het onderzoek dat zij niet mogen communiceren hierover. Daarnaast zijn enkele vragenlijsten niet volledig ingevuld. Hierdoor is het aantal reacties op basis waarvan conclusies kunnen worden getrokken over de juridische risico's lager dan bij de organisatorische risico's. De juridische risico's hebben een foutmarge van 14,2% met het gelijkblijvende betrouwbaarheidspercentage van 95%.

3.2.4 Verwachte onderzoeksresultaten

De vragenlijst is opgesplitst in twee delen. In het eerste deel worden vragen gesteld over de maximaal tien belangrijkste risico's die de respondent onderkent op het gebied van organisatorische risico's. Hierbij worden enerzijds de risico's genoemd die in de literatuur zijn gevonden en anderzijds heeft de respondent de vrijheid om eigen risico's te verwoorden. Hierna wordt ingegaan op de classificatie die is toegekend aan deze risico's en welke maatregelen of acties er worden ondernomen om de risico's te verminderen of vermijden. Nadat de organisatorische risico's zijn behandeld wordt op dezelfde wijze ingezoomd op de juridische risico's.

Nadat alle inhoudelijke vragen zijn behandeld, worden in het tweede deel van de vragenlijst nog enkele algemene vragen gesteld. Deze vragen hebben met name betrekking op de organisatie en de functie van de respondent.

Op basis van deze vragenlijst worden de belangrijkste organisatorische risico's en de belangrijkste juridische risico's van alle respondenten inzichtelijk. Door de grote onderzoeksdoelgroep is de verwachting dat de genoemde risico's voor een groot gedeelte met elkaar overeen komen. Door ook vragen te stellen over de respondent is het waarschijnlijk mogelijk om verschillen in classificatie of tegenmaatregelen te verklaren.

4 Onderzoeksresultaten

Dit hoofdstuk behandelt de onderzoeksresultaten. Allereerst worden de onderzoeksgegevens behandeld. Daarna worden alle genoemde risico's één voor één behandeld. In bijlage 4 en 5 is een samenvatting van de onderzoeksdata opgenomen.

4.1 Onderzoeksgegevens

Op basis van het literatuuronderzoek is een risicomatrix opgesteld, welke als referentiekader heeft gediend voor het empirisch onderzoek. De bevindingen van het literatuuronderzoek zijn besproken in hoofdstuk 2. In het empirisch onderzoek is de risicomatrix getoetst. Met de resultaten van zowel het literatuuronderzoek als het empirisch onderzoek zijn de onderzoeksvragen beantwoord. De aanpak van het empirisch onderzoek is besproken in hoofdstuk 3. De beantwoording van de onderzoeksvragen zal plaatsvinden in hoofdstuk 5.

De vragenlijst is uitgezet bij een viertal doelgroepen:
1. LinkedIn-groep Platform voor Informatiebeveiliging (PvIB)
2. LinkedIn-groep Cloud Security Alliance – Nederland (CSA-N)
3. LinkedIn-groep Cloud Computing Nederland (CCN)
4. Zakelijk netwerk (ZN)

In paragraaf 4.2 en 4.3. worden de risico's afzonderlijk besproken met hun classificaties en maatregelen. In bijlage 4b is een overzicht opgenomen van de relatie tussen de risico's, de classificaties en de vier doelgroepen.

Vanuit de literatuur is matrix 2 opgesteld (afgeleid uit matrix 1). Op de verticale as wordt eerst een onderscheid gemaakt in organisatorische en juridische risico's. Daarna vindt er per onderdeel een verdere uitsplitsing in risico's plaats. Op de horizontale as worden tegenmaatregelen benoemd die gehanteerd kunnen worden om het risico te verminderen. Indien een maatregel kan worden ingezet om een risico te beperken, is dit vakje aangekruist. Zo kan bijvoorbeeld standaardisatie worden ingezet om een leveranciers lock-in tegen te gaan of om de gevolgen van een leverancier die stopt met het leveren van diensten te beperken. Andersom geldt dat een niet goed geregelde governance niet alleen beperkt kan worden door standaardisatie maar ook door het afsluiten van Service Level Agreements (SLA).

Aangezien het empirisch onderzoek zich enkel heeft gericht op de juridische en organisatorische risico's is de matrix beperkt tot deze twee categorieën:

Categorie	Risico	Standaardisatie	Gebruik meerdere leveranciers	Afsluiten SLA	Lokale Opslag	Encryptie
Organisatorisch	Leveranciers lock-in	x	x			
	Data lock-in	x	x			
	Governance is niet goed geregeld	x		x		
	Imagoschade door toedoen van andere bedrijven		x			
	Cloud leverancier stopt met leveren van diensten	x	x			
	Onbekendheid met nieuwe IT-omgeving (bij overstap naar de cloud)	x		x		
Juridisch	Inbeslagname van data				x	x
	Documentatie niet (tijdig) beschikbaar voor onderzoeken				x	
	Beperkingen door wet- & regelgeving		x	x	x	
	Privacy van data niet voldoende geborgd			x	x	x
	Onvoldoende inzicht in naleving van de regels				x	

Matrix 2: Organisatorische en juridische risico's uit de literatuur.

4.2 Organisatorische risico's

Bij het bespreken van de risico's worden percentages gebruikt. De percentages per classificatie zijn gebaseerd op het aantal respondenten dat positief heeft gereageerd op het risico. Alle classificaties bij elkaar opgeteld, leidt hierdoor altijd tot 100%.

4.2.1 Risico 1: Leveranciers lock-in

Op de vraag welke organisatorische risico's als belangrijkste worden onderkend binnen de organisatie geeft 52% van de respondenten de leveranciers lock-in aan.

Classificatie: Accepteren
38% van de respondenten heeft aangegeven het risico te accepteren. Deze respondenten zijn afkomstig van verschillende branches. Opmerkelijk is wel dat bijna alle respondenten uit de branche zakelijke dienstverlening deze classificatie hanteren. Dit kan verklaard worden doordat deze respondenten aangeven hun risicomethodiek af te stemmen op de klant. De mogelijkheid om anders met het risico om te gaan, ligt buiten de invloedsfeer van de respondent bij de klant. Accepteren is voor deze respondenten dan ook een begrijpelijke optie.

Classificatie: Vermijden
Van de respondenten gaf 31% aan het risico te vermijden. In tegenstelling tot bij de classificatie accepteren is er hier geen enkele branche die eruit springt. Als maatregelen om het risico te vermijden worden genoemd:
- Uitsluitende eis bij aan-/uitbesteding
- Expliciet afspreken van disengagement protocollen
- Looptijd in contract beperken
- Alternatieve leveranciers zoeken en deze achter de hand houden
- Meerdere leveranciers leveren een deel van de apparatuur

De maatregelen zijn duidelijk op te splitsen in twee onderdelen. Ten eerste contractueel goede afspraken maken over looptijden, overdrachtsmogelijkheden en standaarden. Ten tweede de inzet van meerdere leveranciers vanaf het begin of in ieder geval de mogelijkheid om dit op een later tijdstip alsnog te doen. Waarbij met name de financiële dienstverlening en de industrie de nadruk legt op de contractuele afspraken en de andere branches ook de optie van meerdere leveranciers benoemen.

Classificatie: Verminderen
De classificatie verminderen wordt door 28% van de respondenten benoemd. In tegenstelling tot de classificatie accepteren waarvoor de zakelijke dienstverlening zich het duidelijkste uitsprak, is dat bij deze classificatie de overheid. Een verklaring hiervoor kan het verplichte gebruik van mantels binnen de overheid zijn, waardoor men middels mantelcontracten toch al gebonden is aan een beperkt aantal leveranciers. Bij het afsluiten van deze mantels wordt wel gezorgd dat er meerdere leveranciers zijn, waardoor een algehele lock-in wordt voorkomen.
Maatregelen die worden genoemd zijn:
- Voldoen aan/Gebruik maken van open standaarden en/of open source
- Zorgvuldig contractmanagement
- Dual sourcing/Dual provider strategy
- Productselectiebeleid
- Alle data zelf ook loggen
- Zakelijk risico heroverwegen
- Afhankelijkheid van leverancier strategisch verminderen
- Clausules in contracten waarin insourcing/transitie naar andere leverancier is geregeld

Net als bij de classificatie vermijden ligt ook hier de nadruk erg op de mogelijke inzet van meerdere leveranciers. Deze inzet wordt op twee manieren mogelijk gemaakt. Enerzijds door het gebruik van open source en open standaarden. Anderzijds door zorgvuldige productselectie om te komen tot een dual vendor strategie.
Contractuele eisen worden bij het verminderen van het risico minder vaak genoemd. Hieruit wordt duidelijk dat de contracten meer gebruikt worden voor het stellen van harde eisen (vermijden) en minder geschikt worden geacht voor het verminderen van effecten.

Classificatie: Verzekeren
De laatste 3% van de respondenten kiest voor het verzekeren van dit risico. Deze respondent gaf aan zijn risicomethode aan te passen aan de klant. De verwachting is dat dit risico dan ook wordt verzekerd middels de contractafspraken met de klant. Dit lage percentage is niet vreemd, aangezien dit risico goed zelf te voorkomen is, zoals door veel respondenten al was aangegeven.

4.2.2 Risico 2: Data lock-in

Waar vanuit de literatuur data lock-in als een groter risico dan leveranciers lock-in wordt gezien, geven de respondenten juist het tegenovergestelde aan. 37% van alle respondenten geeft aan dit als één van de belangrijkste risico's te onderkennen. Aangezien maatregelen als "Alle data zelf loggen" bij de leveranciers lock-in zijn genoemd, is het mogelijk dat sommige respondenten geen duidelijke splitsing hebben gemaakt tussen de leverancier en de data. Daarnaast is bij dit risico duidelijk een verschil zichtbaar tussen de hoofddoelgroepen die de vragenlijst hebben ingevuld. Waar de reactie van het zakelijk netwerk en de onbekende groep respectievelijk 26% en 22% betreft, geven de groepen PvIB, CSA-N en CCN gezamenlijk aan dit risico met 52% te onderkennen. Doordat zowel de literatuur als de groepen PvIB, CSA-N en CCN aangeven dit als belangrijk risico te zien, kan worden verwacht dat het overall percentage hoger zou zijn geëindigd, indien er enkel respondenten uit de drie genoemde groepen hadden deelgenomen aan dit onderzoek.

Classificatie: Accepteren
13% van de respondenten accepteert het risico op data lock-in. Dit gaat opvallend genoeg bij alle respondenten gepaard met het ontbreken van risicomanagement.

Classificatie: Vermijden
Door 48% van de respondenten wordt aangegeven dat het risico wordt vermeden. Hierbij geven alle respondenten uitgebreid antwoord op de vraag welke risicomethode wordt gehanteerd. Als maatregelen om het risico te vermijden worden genoemd:
- Goede beveiliging
- Niet overstappen naar een cloud omgeving als er onvoldoende garanties zijn
- Inrichten compliance team
- Voorkomen door dedicated diensten
- Contractafspraken over eigenaarschap data
- Eisen aan data-export bij product/dienstselectie
- Zelf back-up van data
- Datamodel op basis van open standaarden

Classificatie: Verminderen
35% van de respondenten treft maatregelen om het risico te verminderen. Ook hier geven respondenten aan risicomethodieken te hanteren. Hieruit kan worden geconcludeerd dat een organisatie die zich bewust bezig houdt met risicobeheersing, het risico van data lock-in zichtbaar onderkent en hier maatregelen tegen neemt. Indien een organisatie weinig doet aan risicobeheersing, wordt dit risico niet al te kritisch onderkend en dus onderschat.
Maatregelen om het risico te verminderen zijn:
- Goede contractuele vastlegging, Service Level Agreements
- Governance afspraken
- Security agreement
- Auditable dienstverlening
- Open standaarden en protocollen
- Contractclausule omtrent eigenaar data
- Lokale of dubbele opslag
- Data exit strategie definiëren

Classificatie: Verzekeren
Van alle respondenten is er 4% die aangeeft dit risico te verzekeren. Hierbij wordt aangegeven gebruik te maken van RUP als risicomethodiek. Dit lijkt de eerdere conclusie tegen te spreken, dat bij gedegen risicoanalyse er maatregelen worden genomen om dit risico te vermijden of te verminderen. Echter RUP betreft een software ontwikkel- en projectmanagementmethodiek, waarbij risicoanalyse wordt gezien als onderdeel van het iteratief ontwikkelen en aansturen. Onduidelijk is of deze methode ook geschikt is en gebruikt wordt voor risicoanalyse van het dagelijkse bedrijfsproces of enkel voor ontwikkelingen.

4.2.3 Risico 3: Governance niet goed geregeld

Iets minder dan de helft van alle respondenten (44%) geeft aan het risico dat de governance niet goed is geregeld te onderkennen.

Classificatie: Accepteren
Het risico dat de governance niet goed is geregeld wordt door 10% van de respondenten geaccepteerd. Naast werken met gezond verstand zijn er ook organisaties die conform ISO9001 werken en dit risico accepteren. Dit kan verklaard worden door het feit dat in deze organisaties de governance waarschijnlijk goed is ingeregeld, waardoor de kans van optreden van dit risico reeds tot een minimum is beperkt.

Classificatie: Vermijden
30% van de respondenten geeft aan maatregelen te nemen om het risico te vermijden:
- Geen afname clouddiensten indien onvoldoende garanties
- Inrichten compliance team of governance
- Kleine projecten
- Verlagen ambitie
- Gedogen governance-variaties
- Handelen naar en bijstellen van lange termijnvisie en governance
- Voorkomen van tegenstrijdigheden door ontwikkelingen (fusie etc.)

Met name in de dienstverlenende sectoren wordt gekozen voor het vermijden van dit risico. Dit in tegenstelling tot de overheid waar juist voornamelijk wordt gekozen om het risico te verminderen.

Classificatie: Verminderen
Naast de overheid kiezen ook andere branches zoals de gezondheid/welzijnszorg en informatie/communicatie voor het verminderen van het governance risico. De meerderheid van de respondenten (57%) treft maatregelen hiervoor:
- Afdwingbare controle naar de leverancier
- Contractafspraken / Service Level Agreements
- Eisen "in control" leverancier (ISAE3402)
- Regelmatig overleg met alle partijen
- Expliciet beleggen verantwoordelijkheden (primair en secundair)
- Uitkristalliseren processen in vastgelegde procedures en werkinstructies
- Ontkoppelen van bestaande organisatie / opzetten compliance center
- Aanstellen leveranciersmanager
- Vaststellen en vastleggen verantwoordelijkheden en processen
- Interne governance goed inrichten voor samenwerking met derde partij

Classificatie: Verzekeren
Naast alle andere mogelijkheden geeft 3% van de respondenten aan het risico te verzekeren.

4.2.4 Risico 4: Imagoschade door toedoen van andere bedrijven

Evenals het governance risico geeft ook 49% van de respondenten aan dat het risico op imagoschade erg belangrijk is. Dit zijn in de helft van de gevallen dezelfde respondenten.

Classificatie: Accepteren
10% van de respondenten heeft dit risico geclassificeerd met accepteren. Dit betreffen respondenten uit verschillende branches, met uiteenlopend gebruik van de cloud (tussen de 0 en 95%) en risicomethodieken.

Classificatie: Vermijden
De classificatie vermijden is door 44% van de respondenten toegekend aan dit risico. Bij de risicomethodiek wordt zeer wisselend geantwoord. Ongeveer de helft geeft aan uitgebreide risicoanalyses uit te voeren, terwijl de andere helft aangeeft geen specifieke methode te hanteren. De maatregelen hebben veelal wel het overkoepelend kenmerk leveranciersmanagement.
De maatregelen die worden genoemd zijn:
- Onderaannemersselectie
- Supplier code of conduct
- Audits / Beoordelingssysteem inrichten
- Ingangscontrole bij nieuwe leverancier
- Preventieworkshops
- Supplier relation management
- Contractuele afspraken
- Inrichten compliance team
- Voorwaarden aan personeel en materieel voor optimale dienstverlening
- Zo veel mogelijk zelf doen
- Standaardisatie
- Uitsluiten specifieke leveranciers
- Encryptie
- In de doofpot stoppen

Met name deze laatste maatregel is verrassend vanuit een respondent in de zakelijke dienstverlening.

Classificatie: Verminderen
Vertegenwoordigd door voornamelijk de dienstverlenende branches en de overheid geeft 33% van de respondenten aan maatregelen te nemen ter vermindering van het risico op imagoschade. Als maatregelen worden genoemd:
- Gedegen risicoanalyse
- Gedragscode interne medewerkers
- Eigen kwaliteitstoetsing
- Eigen beheerverantwoordelijkheid
- ESCROW (gebruik onafhankelijke derde partij)
- Leveranciersmanagement
- Goede virusapparatuur
- Duidelijke afspraken met derden
- Interne organisatie aangesloten bij alle lopende projecten en processen

Waar bij de classificatie vermijden de nadruk nog lag op leveranciersmanagement, wordt bij de classificatie verminderen expliciet de risico's bij de eigen organisatie gezien.

Classificatie: Verzekeren
In tegenstelling tot eerdere risico's geeft bij dit risico 13% aan de gevolgen te verzekeren. Dit is niet vreemd, aangezien de gevolgen van imagoschade te verhelpen zijn, door onafhankelijke partijen. Positieve publiciteit speelt hierbij vaak een grote rol.

4.2.5 Risico 5: Cloudleverancier stopt met leveren van diensten

Van alle respondenten geeft 41% aan dat dit een belangrijk risico is. Het vertrouwen in het voortbestaan van leveranciers op een snel ontwikkelende en innovatieve markt is dus relatief hoog.

Classificatie: Accepteren
15% accepteert het risico dat de leverancier stopt. Opmerkelijk aangezien deze respondenten ook aangegeven voor maximaal 80% gebruik te maken van een cloud omgeving. De respondenten geven aan wel risicoanalyses uit te voeren, waaruit geconcludeerd kan worden dat de delen van de IT-voorziening die in de cloud zijn ondergebracht, geen organisatiekritische informatie bevatten.

Classificatie: Vermijden
Van de respondenten geeft 31% aan het risico te vermijden. Hiervoor worden de volgende maatregelen genomen:
- Contractafspraken
- Eigen omgeving als back-up
- Periodiek testen op andere cloud
- Focus op dienst en service, in plaats van op techniek
- Dual vendor policy
- Eigen kwaliteitscontrole

De nadruk in de maatregelen ligt op het beperken van de afhankelijkheid van de cloud omgeving.

Classificatie: Verminderen
De meeste respondenten geven echter aan het risico te verminderen (39%). Hierbij worden voornamelijk maatregelen genomen om de overstap te kunnen realiseren, dan wel terug te kunnen vallen op een eigen omgeving:
- Standaard services zodat overstap naar alternatieve cloud provider mogelijk is
- Ontwikkelen cloud uitwijkdienst
- Contractafspraken
- Kennis eigen organisatie op peil houden
- Zorgen voor alternatieve omgeving
- Data- en cloud-exitstrategie bepalen
- Meerdere aanbieders
- Leverancierskeuze met stabiele historie

Classificatie: Verzekeren
Van alle respondenten geeft 15% aan het risico te verzekeren.

4.2.6 Risico 6: Onbekendheid met nieuwe omgeving

Van alle respondenten ziet 37% de onbekendheid met de nieuwe omgeving als serieus risico. Voor een aantal is dit een gegeven, terwijl anderen er alles aan doen om dit risico te verminderen.

Classificatie: Accepteren
36% van de respondenten accepteert het gebrek aan kennis en de afhankelijkheid die hiermee richting de leverancier ontstaat.

Classificatie: Vermijden
Van de respondenten geeft 14% aan dit risico te vermijden. Maatregelen ter vermijding van dit risico zijn:
- Zoeken van kennispartner (anders dan de leverancier)
- Interne standaardisatie van ontwikkelomgeving en ontwikkeltaal, waardoor afhankelijkheid van de leverancier wordt beperkt
- Pas adoptie van nieuwe mogelijkheden en technieken zodra er voldoende ervaring in de markt is.

De duidelijke terughoudendheid bij deze respondenten wordt vaak genoemd in de literatuur. Opvallend is daarbij dat slechts een klein deel van de respondenten deze terughoudendheid ook toont.

Classificatie: Verminderen
De behoefte om gebruik te maken van de cloud is duidelijk groter dan de hierboven geconstateerde terughoudendheid. Toch zijn organisaties wel voorzichtig, gezien het feit dat 45% van de respondenten aangeeft maatregelen te nemen om de gevolgen van het risico te beperken:
- Informatie/contactbijeenkomsten ter verkenning
- Training en opleiding algemeen en specifiek
- Uitwerken strategie
- Private cloud als tussenstap
- Open communicatie met betrokken partijen
- Registratie meldingen die te herleiden zijn tot onbekendheid
- Standaardisatie, waardoor minder diversiteit

De nadruk ligt duidelijk op het vergaren van kennis over de omgeving en dus de afhankelijkheid van de leverancier verminderen.

Classificatie: Verzekeren
Ondanks de afhankelijkheid van de leverancier geeft 5% aan het risico te verzekeren en daarmee voldoende maatregelen te hebben genomen om de gevolgen van het risico beheersbaar te houden.

4.2.7 Overige organisatorische risico's

Naast de bovengenoemde risico's uit de literatuur zijn er door de respondenten ook nog eigen risico's genoemd. Deze risico's zijn opgesplitst in vier onderwerpen die de risico's het beste typeren: Afnemer, Data, Leverancier en Techniek.

Afnemersrisico's:

Volwassenheidsaspecten van de diensten
Dit risico wordt vermeden. Indien de volwassenheid van verschillende aspecten onvoldoende is zal niet worden overgegaan naar een cloud omgeving.

Het niet kunnen afdwingen van compliance aspecten
Dit risico wordt vermeden. De respondent geeft hier zeer stellig aan dat indien er niet aan een aantal harde criteria wordt voldaan er niet tot contractering wordt overgegaan. Het betreft een harde "No go", met als gevolg on-premise diensten.

Risico's op het gebied van contracten
Dit risico wordt vermeden door het opbouwen van eigen deskundigheid.

Compliance moeilijk te regelen
Dit risico wordt vermeden door te voldoen aan wet- en regelgeving binnen de landsgrenzen.

Onvoldoende kennis in de eigen organisatie
Dit risico wordt vermeden door het gebruik van standaardisatie, waardoor er minder diversiteit is. Het risico lijkt veel op risico 6, echter de respondent heeft ze expliciet allebei genoemd.

Imagoschade door eigen toedoen
Dit risico wordt vermeden door het organisatiebewustzijn te vergroten.

Uit de markt prijzen door te lange doorlooptijd
Dit risico wordt verzekerd.

Snelheid van besluitvorming
De respondent vindt het risico belangrijk te vermelden, maar geeft wel aan dat de gevolgen hiervan geaccepteerd worden.

Medewerkers voldoen niet aan de door hen beschreven kennis, ervaring en competenties
De respondent geeft aan dit risico te verminderen. Als maatregel hiervoor wordt genoemd het testen op persoonlijke voorkeuren, talenten en werkelijke kennis en ervaring. Dit risico en de bijbehorende maatregel dragen bij aan het beperken van het risico omtrent de onbekendheid van de omgeving.

Diffuus aanbod van specialistische diensten
Dit risico wordt geaccepteerd.

Geen eenduidig zicht op omgevingsontwikkelingen
Dit risico wordt verminderd door analyse op huidige trends in te richten.

Datarisico's:

Imagoschade en financiële schade door data lekkage naar andere cloud gebruikers
De imagoschade is reeds meegeteld bij risico 4. De financiële schade wordt als afzonderlijk risico gezien. Deze heeft de classificatie vermijden gekregen van de respondent. Als maatregel geeft de respondent encryptie te gebruiken.

Onvoldoende beveiliging data in de cloud
Door het gebruik van een private cloud wordt dit risico vermeden.

Problemen met back-up data in de cloud
Dit risico wordt vermeden door geen gebruik te maken van een public cloud omgeving, maar de risico's te beperken in een private cloud.

Verlies van data
Het risico wordt vermeden door het gebruik van back-up en een uitwijk datacenter.

Compromitteren van data
De respondent geeft aan dit risico te vermijden door opslag van data op desktops en laptops te versleutelen.

Onvoldoende informatiebeveiliging
Dit risico wordt vermeden door verschillende elkaar aanvullende maatregelen:
- Alle documenten kennen een beveiligingsclassificatie
- Alleen gebruik geautoriseerde hardware
- Op alle data wordt encryptie doorgevoerd
- Geen gebruik van USB
- Clean desk policy

Data lock-out
Hiermee wordt bedoeld dat de data niet meer beschikbaar is voor de cloud afnemer. De respondent geeft aan dit risico te verzekeren.

Beveiliging (exclusiviteit) van de data is niet goed geregeld
Dit risico wordt vermeden door geen gebruik te maken van een cloud omgeving zolang dit niet is geregeld.

Is data bij de leverancier veilig
De respondent geeft aan dit risico te verzekeren.

Gegevens komen in handen van derden
Dit risico wordt vermeden door sterke encryptie.

Al deze datarisico's hebben betrekking op de beveiliging en beschikbaarheid van data. Deze risico's worden samengevat onder organisatorisch risico 7: Databeschikbaarheid en beveiliging aangezien 16% van de respondenten hier nadrukkelijk aandacht aan schenkt.

<u>Leveranciersrisico's:</u>

Verandering van voorwaarden door de leverancier
Classificatie verminderen.

Gebrek aan inzicht en "auditbaarheid" van de toeleverancier
De respondent geeft aan dit risico te vermijden. Als maatregel wordt gegeven dat er eerst audit protocollen dienen te zijn uitgewerkt, zowel technische als procedureel, voor de kritische diensten. Zodra dit is gebeurd wordt pas de overstap naar de cloud gerealiseerd.

Licentiestructuur ondoorzichtig en op termijn duur
Dit risico wordt vermeden. De respondent geeft aan dat bij onvoldoende garanties de overstap naar een cloud omgeving niet wordt gemaakt.

Onduidelijke end-to-end service levels
Dit risico wordt vermeden door transparantie en juridische disclaimers.

Past de dienst bij de organisatie en blijft deze passen
Risico wordt vermeden door zorgvuldige leverancierskeuze.

Betrouwbaarheid provider/Service level agreements
Dit risico wordt vermeden door zorgvuldige leverancierskeuze.

Geen audit mogelijkheiden
Dit risico wordt verminderd door hierover afspraken te maken in een contract clausule.

Technische risico's:

Geen mogelijkheid om bevindingen opgelost te krijgen
Classificatie verminderen.

Integratie met legacy/private cloud/on-premise problematisch
Dit risico is twee keer genoemd. De ene respondent geeft aan dit risico te verminderen door standaard koppelvlakken aan te leggen, terwijl de andere respondent het risico classificeert als verzekeren.

Onbeheersbaarheid van techniek
Dit risico wordt verminderd door het outsourcen van de techniek inclusief de diensten.

Shared gebruik infrastructuur in de cloud
Dit risico wordt vermeden door gebruik te maken van een private cloud.

Uitval stroom
Dit risico wordt vermeden door de inzet van noodstroom.

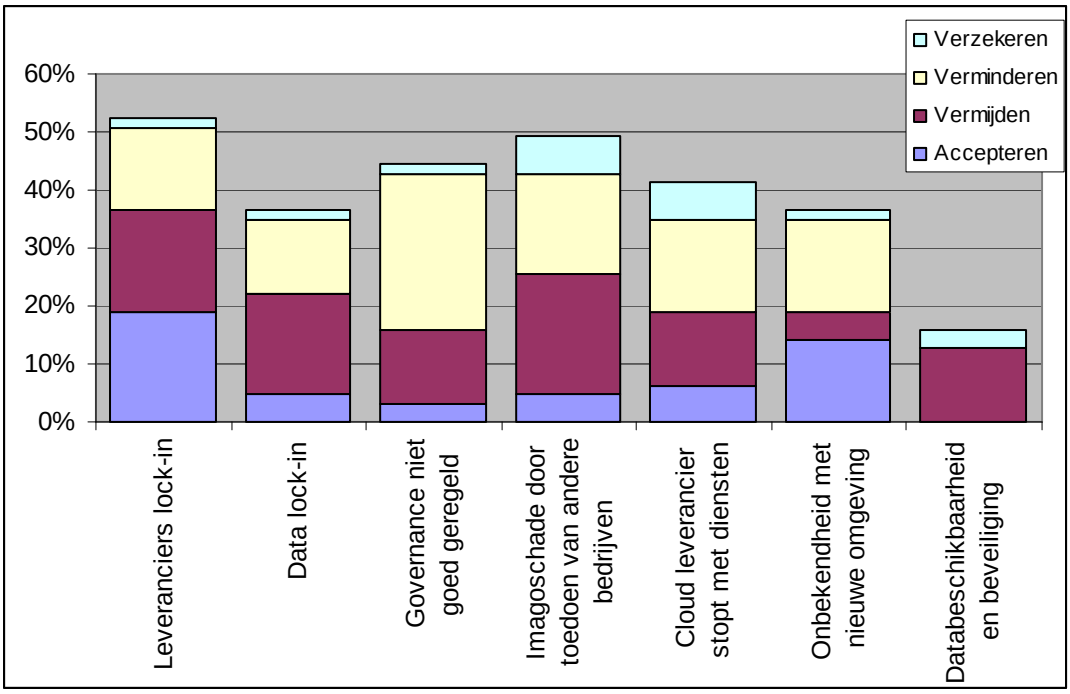
Uitval netwerk
Dit risico wordt vermeden door het dubbel uitvoeren van de netwerkverbindingen.

Bedreigingen van buitenaf
Dit risico wordt vermeden door middel van procedures en uitwijk.

Het niet beschikbaar zijn van diensten/data
Het risico wordt vermeden door geen gebruik te maken van een cloud omgeving.

Onbekende performance cloud
Dit risico wordt verminderd door de leverancier te verplichten inzicht te geven in de performance van de omgeving.

Naast deze vier categorieën zijn er risico's genoemd die eigenlijk vallen onder de juridische risico's. Deze risico's worden dan ook verder behandeld in paragraaf 4.3



Figuur 4: Overzicht percentages organisatorische risico's

4.3 Juridische risico's

Ook de classificatie van de juridische risico's wordt behandeld op basis van percentages. De percentages per classificatie zijn gebaseerd op het aantal respondenten dat positief heeft gereageerd op het risico. Alle classificaties bij elkaar opgeteld, leidt dit altijd tot 100%.

Overall valt op dat bij ieder organisatorisch risico alle classificaties werden gehanteerd. Bij de juridische risico's zijn er meerdere waar de classificatie verzekeren niet is toegekend.

4.3.1 Risico 1: Inbeslagname van data

30% van de respondenten geeft aan de inbeslagname van data als een belangrijk risico te identificeren.

Classificatie: Accepteren
7% van de respondenten geeft aan het risico te accepteren. Deze respondenten maken gebruik van uitgebreide risico-inventarisaties gebaseerd op onder andere ISO9001.

Classificatie: Vermijden
Ondanks het relatief lage percentage respondenten dat dit risico identificeert, geeft 79% aan maatregelen te nemen om het risico te vermijden. De genoemde maatregelen zijn:
- Zorgvuldige contracten
- Garanties/afspraken met leverancier
- Geen gebruik van (internationale) cloud leveranciers
- Encryptie van data
- Medewerkers goed informeren

Expliciet wordt door meerdere respondenten aangegeven dat dit risico een "Go/No go"-criteria betreft.

Classificatie: Verminderen
De overige 14% geeft aan het risico te verminderen door het voorkomen van connecties met de USA.

Classificatie: Verzekeren
Er zijn geen respondenten die het risico verzekeren.

4.3.2 Risico 2: Documentatie niet (tijdig) beschikbaar voor onderzoeken

Voor 39% van de respondenten is dit een belangrijk juridisch risico. De wijze waarop de respondenten met het risico omgaan is zeer divers.

Classificatie: Accepteren
22% van de respondenten geeft aan het risico te accepteren. Kijkend naar de gehanteerde risicomethodiek wordt zichtbaar dat dit respondenten zijn die geen vaste methodiek hanteren. Enerzijds omdat zij de methode aanpassen aan de methode van de klant, anderzijds omdat wordt uitgegaan van gezond verstand.

Classificatie: Vermijden
44% van de respondenten heeft de classificatie vermijden toebedeeld aan dit risico. Als maatregelen worden benoemd:
- Contract afspraken
- Leveranciersmanagement
- Procedures opstellen
- Dubbele datavoorziening
- Inzet private cloud
- Eigen beheerorganisatie
- Borging in enterprise architectuur

Tevens wordt aangegeven geen gebruik te gaan maken van de cloud, als dit risico niet kan worden voorkomen.

Classificatie: Verminderen
De overige 34% van de respondenten geeft duidelijk aan maatregelen te nemen om het risico te verminderen, maar voor hen is het geen onoverkomelijk risico.
Maatregelen die worden genoemd zijn:
- Gebruik van afdelingsbibliotheken
- Regelmatige risicoanalyse en inventarisatie van behoeften
- Procedureel oplossen met kwaliteitsmanagementsysteem
- Contractuele afspraken meetbaar en controleerbaar
- Reservekopie beschikbaar

Classificatie: Verzekeren
Er zijn geen respondenten die dit risico verzekeren.

4.3.3 Risico 3: Beperkingen door wet- en regelgeving

Van alle respondenten geeft 41% aan het risico belangrijk te vinden.

Classificatie: Accepteren
Bijna een derde (32%) van de respondenten accepteert dit risico. Deze respondenten komen uit verschillende branches en voeren hun risicoanalyse uit op basis van verschillende methodieken, waaronder MoR, ISO9001 en BCM.

Classificatie: Vermijden
Ruim de helft van de respondenten (53%) geeft echter aan het risico te vermijden. Dit doen zij door de processen zo aan te passen, dat wordt voldaan aan de wet- en regelgeving. Dit risico wordt door deze respondenten vooral als beleid gezien, welke kaderstellend is voor de organisatie.
Als aanvullende maatregelen worden genoemd:
- Inzet van private cloud
- Dataopslag in Nederland
- Eigen beheerorganisatie
- Inrichten compliance team

Classificatie: Verminderen
10% geeft aan het risico te verminderen. Hiervoor wordt extern advies geworven.

Classificatie: Verzekeren
De overige 5% geeft aan het risico te verzekeren.

4.3.4 Risico 4: Privacy van data is niet voldoende geborgd

Direct zichtbaar wordt dat dit het belangrijkste juridische risico is. 80% van de respondenten geeft dit aan, waarbij het merendeel ook dezelfde classificatie toekent aan het risico.

Classificatie: Accepteren
11% van de respondenten accepteert dit risico. Dit kan verklaard worden door het feit dat de respondenten slechts beperkt gebruik maken van risicomethodieken. Opvallend is wel dat deze respondenten voornamelijk afkomstig zijn uit de informatie/communicatie branche. Deze branche is meer bezig met openbare informatie, waardoor de gevolgen waarschijnlijk beperkter zijn.

Classificatie: Vermijden
Ruim de helft van de respondenten (64%) treft maatregelen om dit risico te vermijden. De maatregelen die worden genoemd:
- Leverancier moet voldoen aan strenge eisen (ISO2700x; Cobit; ISAE 3402)
- Proces aanpassen om privacy te borgen
- Compliance team inrichten
- Data versleutelen; encryptie
- Informatie classificatie, beleid en oplossingsrichting per klasse
- Borging binnen enterprise architectuur
- Inzet private cloud
- Betrokkenheid juridisch personeel
- Toegang tot data beperken
- Wet- en regelgeving; data op Nederlands grondgebied

Verschillende respondenten geven aan dat het gebruik van een cloud omgeving wordt beperkt door dit risico. De mogelijkheden die een private cloud biedt in dit kader worden vaak niet of slechts beperkt gezien.

Classificatie: Verminderen
Ondanks dat het merendeel heel stellig aangeeft het risico te vermijden, geeft toch nog 17% aan het risico te verminderen. De maatregelen die hiervoor worden genoemd zijn:
- Goede beveiligingssoftware
- Contractuele vastlegging
- Periodieke audits c.q. hackpogingen
- Externe dienstverlening

Op basis van deze maatregelen lijkt men zich niet zo'n zorgen te maken over het risico. Dit is verbazingwekkend gezien het grote aantal respondenten dat het risico belangrijk vond.

Classificatie: Verzekeren
De classificatie verzekeren wordt door 8% van de respondenten toegekend aan dit risico.

4.3.5 Risico 5: Onvoldoende inzicht in naleving van de regels

Van alle respondenten geeft 44% aan dit juridische risico belangrijk te vinden

Classificatie: Accepteren
Van de respondenten geeft 20% aan dit risico te accepteren. Deze respondenten zijn voornamelijk werkzaam als IT-adviseurs bij klanten. Onduidelijk is of ze bedrijven adviseren op het gebied van cloud computing.

Classificatie: Vermijden
In 45% van de gevallen wordt aangegeven dat het risico wordt vermeden. Hiervoor worden maatregelen ingezet als:
- Het inrichten van een compliance team
- De inzet van een private cloud
- Het opstellen en handhaven van audits en regelgeving
- Maken van contractuele afspraken met de leverancier

Daarbij wordt aangegeven dat dit risico een "Go/No go"-criterium is voor verschillende respondenten.

Classificatie: Verminderen
Een kwart (25%) van de respondenten treft maatregelen om het risico te verminderen:
- Training en opleiding
- Extern advies
- Uitvoeren van frequente audits
- Toetsing bij nieuwe producten/applicaties
- Aanpassen bestaande applicaties gedurende de levenscyclus

Classificatie: Verzekeren
De overige 10% verzekert zich voor dit risico.

4.3.6 Overige juridische risico's

Naast de bovengenoemde risico's uit de literatuur hebben de respondenten ook andere risico's benoemd. Deze worden hieronder aangegeven.

Deze risico's zijn opgesplitst in de categorieën datalocatie en contractissues.

Datalocatie:

- *Legal Issue: Data op grondgebied ander land*
- *Cloud leverancier is onderhevig aan patriot act*
- *Overheden/bedrijven krijgen toegang tot gegevens middels wetgeving in een ander land*
- *Opslag data buiten de EU*
- *Niet voldoen aan wet- en regelgeving zoals het buiten de EU stallen van data.*
- *Onvoldoende transparante gegevensbescherming (patriot act bijv.)*
- *Data weliswaar binnen europa, maar beheer niet via euro-landen*

De hierboven genoemde risico's hebben allemaal betrekking op het risico dat data beschikbaar kan/moet worden gesteld aan een derde partij enkel doordat wetgeving uit andere landen dit voorschrijft. Dit gebeurt bijvoorbeeld door de Patriot Act in de USA. Duidelijk hieruit wordt dat dit als groot risico wordt gezien en dat alle respondenten aangeven dit risico te vermijden. Bij het benoemen van maatregelen is men ook zeer helder. Indien niet kan worden gegarandeerd dat de data niet ter beschikking komt aan een derde partij, wordt de overstap naar een cloud omgeving niet gemaakt. Een enkeling geeft nog wel de optie voor een private cloud aan. 24% van de respondenten benoemt dit risico. Dit lijkt niet zo veel. Echter dit risico wordt veelal naast risico 4 "privacy van data niet voldoende geborgd" genoemd en toont dus aan dat de respondenten zich hier echt zorgen over maken. Het gaat hierbij niet specifiek om privacygevoelige data, maar ook om andere organisatiedata die men niet openbaar wil geven.

Contractissues:

Juridische risico's rondom aansprakelijkheid
Dit risico wordt verminderd door niet alles in een cloud te plaatsen, maar gedeeltelijk gebruik te blijven maken van een lokale omgeving.

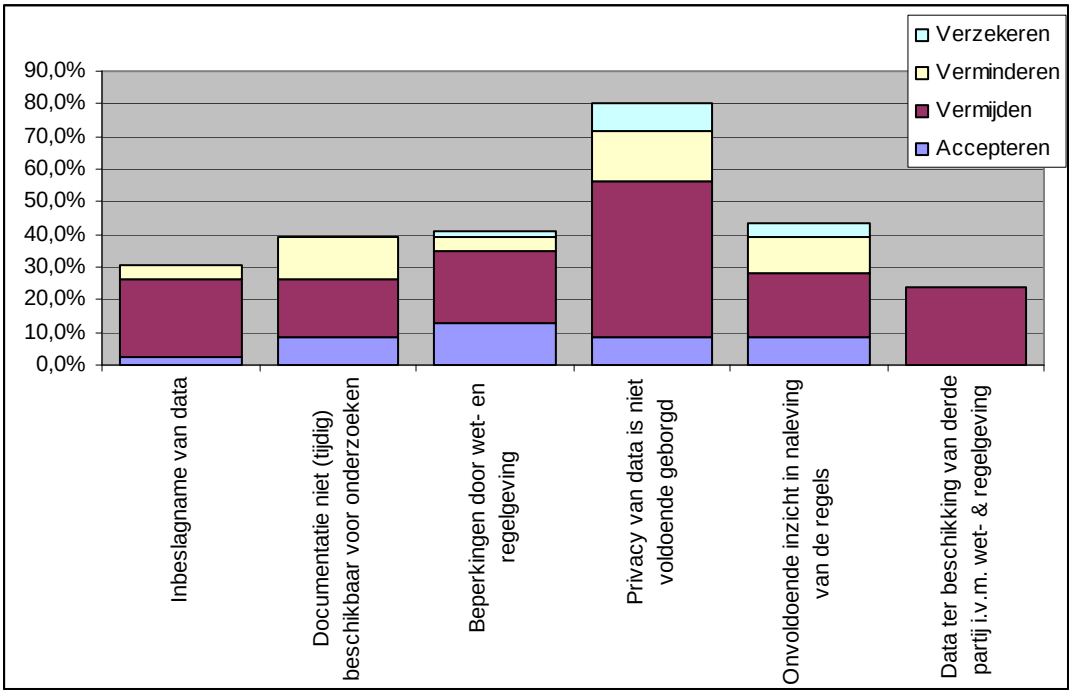
Aansprakelijkheid bij niet naleven contractuele afspraken
Dit risico wordt verminderd door het contract te laten toetsen door juristen.

Eigenaarschap data
Het risico wordt door de respondent geaccepteerd. Deze respondent is werkzaam in de informatie/communicatie branche.

Onduidelijkheden en multi-interpretatie van afspraken
Niet alleen controle door juristen ook de controle door inhoudelijk specialisten wordt ingezet om dit risico te verminderen.

Juridische houdbaarheid van boetes en aansprakelijkheden
Evenals de andere contractissues wordt ook dit risico verminderd door een extra controle door de juristen.

Onbekendheid met van toepassing zijnde wet- en regelgeving
Dit risico wordt verzekerd. Het risico is waarschijnlijk een combinatie van de eerder genoemde juridische risico's "Onvoldoende inzicht in naleving van de regels" en "Beperkingen door wet- en regelgeving". De respondent had het risico aangegeven bij de organisatorische risico's en heeft in het tweede deel van de vragenlijst beide juridische risico's geselecteerd.



Figuur 5: Overzicht percentages juridische risico's

4.4 Verdeling risico's over de doelgroepen

Bij de opstart van het onderzoek werd de keuze gemaakt omgebruik te maken van LinkedIn-groepen om zo een diverse en omvangrijke onderzoeksgroep te hebben. Als extra maatregel om voldoende reacties te genereren was besloten om naast de LinkedIn-groepen ook het eigen eerste- en tweedelijns zakelijk netwerk in te zetten.

Hierdoor is het risico ontstaan dat de onderzoeksgroep is uitgebreid met personen zonder kennis over risico's bij het gebruik van cloud computing. Het is dan ook noodzakelijk om inzicht te krijgen in de verschillen en overeenkomsten in de reacties van de oorspronkelijke onderzoeksgroep, bestaande uit leden van de groepen PvIB, CSA-N en CCN, en het zakelijk netwerk. Aangezien tijdens het onderzoek is geconstateerd dat niet alle respondenten de vragenlijst volledig hebben ingevuld, zal ook deze groep afzonderlijk bekeken moeten worden. Hiervan is immers onbekend of zij afkomstig zijn uit de LinkedIn-groepen of uit het zakelijk netwerk.

Matrix 3 toont de verdeling van de organisatorische risico's per classificatie over de drie onderzoeksgroepen. De percentages zijn gebaseerd op het aantal respondenten dat de classificatie heeft genoemd ten opzichte van de omvang van de betreffende onderzoeksgroep. Dit betekent dat het totale percentage is gebaseerd op 63 respondenten, het percentage van de LinkedIn-groepen is gebaseerd op 20 respondenten, het percentage van het zakelijk netwerk is gebaseerd op 30 respondenten en voor de groep onbekend is uitgegaan van 13 respondenten. Hierdoor geven de percentages een gewogen beeld van de reacties.
Met blauw zijn de percentages aangegeven die zorgen voor een andere prioritering dan de prioritering van de totale groep.

Risico		Totaal (63)		LinkedIngroepen (20) PvIB, CSA-N CCN		Zakelijk netwerk (30)		Onbekend (13)	
		Aantal	%	Aantal	%	Aantal	%	Aantal	%
Leveranciers lock-in	Accepteren	12	19,0%	5	25,0%	3	10,0%	4	30,8%
	Vermijden	11	17,5%	5	25,0%	3	10,0%	3	23,1%
	Verminderen	9	14,3%	2	10,0%	6	20,0%	1	7,7%
	Verzekeren	1	1,6%	0	0,0%	1	3,3%	0	0,0%
	Totaal	33	52,4%	12	60,0%	13	43,3%	8	61,5%
Data lock-in	Accepteren	3	4,8%	2	10,0%	1	3,3%	0	0,0%
	Vermijden	11	17,5%	5	25,0%	4	13,3%	2	15,4%
	Verminderen	8	12,7%	4	20,0%	1	3,3%	3	23,1%
	Verzekeren	1	1,6%	1	5,0%	0	0,0%	0	0,0%
	Totaal	23	36,5%	12	60,0%	6	20,0%	5	38,5%
Governance niet goed geregeld	Accepteren	2	3,2%	1	5,0%	1	3,3%	0	0,0%
	Vermijden	8	12,7%	3	15,0%	2	6,7%	3	23,1%
	Verminderen	17	27,0%	5	25,0%	8	26,7%	4	30,8%
	Verzekeren	1	1,6%	1	5,0%	0	0,0%	0	0,0%
	Totaal	28	44,4%	10	50,0%	11	36,7%	7	53,8%
Imagoschade door toedoen van andere bedrijven	Accepteren	3	4,8%	1	5,0%	1	3,3%	1	7,7%
	Vermijden	13	20,6%	5	25,0%	6	20,0%	2	15,4%
	Verminderen	11	17,5%	2	10,0%	6	20,0%	3	23,1%
	Verzekeren	4	6,3%	1	5,0%	2	6,7%	1	7,7%
	Totaal	31	49,2%	9	45,0%	15	50,0%	7	53,8%
Cloud leverancier stopt met diensten	Accepteren	4	6,3%	1	5,0%	3	10,0%	0	0,0%
	Vermijden	8	12,7%	2	10,0%	4	13,3%	2	15,4%
	Verminderen	10	15,9%	5	25,0%	4	13,3%	1	7,7%
	Verzekeren	4	6,3%	1	5,0%	0	0,0%	3	23,1%
	Totaal	26	41,3%	9	45,0%	11	36,7%	6	46,2%
Onbekendheid met nieuwe omgeving	Accepteren	9	14,3%	5	25,0%	1	3,3%	3	23,1%
	Vermijden	3	4,8%	1	5,0%	2	6,7%	0	0,0%
	Verminderen	10	15,9%	2	10,0%	6	20,0%	2	15,4%
	Verzekeren	1	1,6%	0	0,0%	1	3,3%	0	0,0%
	Totaal	23	36,5%	8	40,0%	10	33,3%	5	38,5%

Matrix 3: Verdeling organisatorische risico's per klasse over de hoofddoelgroepen

Uit matrix 3 wordt duidelijk dat de LinkedIn-groepen in 54% van de gevallen procentueel een hoger percentage per risico scoren dan de totale groep. In tegenstelling tot het zakelijk netwerk dat slechts in 37,5% van de mogelijkheden een hoger percentage vertoond. Hieruit kan worden opgemaakt dat de gemiddelde resultaten uit het onderzoek omlaag zijn gehaald door de inzet van het zakelijk netwerk. De respondenten waarvan onbekend is tot welke groep zij behoren valt met 45,8% hier tussenin. In hoofdstuk vijf zullen bij de conclusies de gevolgen van deze verschillen worden besproken.

Risico		Totaal (46)		LinkedIngroepen (18) PvIB, CSA-N CCN		Zakelijk netwerk (27)		Onbekend (1)	
		Aantal	%	Aantal	%	Aantal	%	Aantal	%
Inbeslagname van data	Accepteren	1	2,2%	1	5,6%	0	0,0%	0	0,0%
	Vermijden	11	23,9%	6	33,3%	5	18,5%	0	0,0%
	Verminderen	2	4,3%	1	5,6%	1	3,7%	0	0,0%
	Verzekeren	0	0,0%	0	0,0%	0	0,0%	0	0,0%
	Totaal	14	30,4%	8	44,4%	6	22,2%	0	0,0%
Documentatie niet (tijdig) beschikbaar voor onderzoeken	Accepteren	4	8,7%	3	16,7%	1	3,7%	0	0,0%
	Vermijden	8	17,4%	4	22,2%	4	14,8%	0	0,0%
	Verminderen	6	13,0%	4	22,2%	2	7,4%	0	0,0%
	Verzekeren	0	0,0%	0	0,0%	0	0,0%	0	0,0%
	Totaal	18	39,1%	11	61,1%	7	25,9%	0	0,0%
Beperkingen door wet- en regelgeving	Accepteren	6	13,0%	4	22,2%	2	7,4%	0	0,0%
	Vermijden	10	21,7%	5	27,8%	5	18,5%	0	0,0%
	Verminderen	2	4,3%	0	0,0%	2	7,4%	0	0,0%
	Verzekeren	1	2,2%	1	5,6%	0	0,0%	0	0,0%
	Totaal	19	41,3%	10	55,6%	9	33,3%	0	0,0%
Privacy van data is niet voldoende geborgd	Accepteren	4	8,7%	1	5,6%	3	11,1%	0	0,0%
	Vermijden	22	47,8%	10	55,6%	12	44,4%	0	0,0%
	Verminderen	7	15,2%	4	22,2%	3	11,1%	0	0,0%
	Verzekeren	4	8,7%	2	11,1%	1	3,7%	1	100,0%
	Totaal	37	80,4%	17	94,4%	19	70,4%	1	100,0%
Onvoldoende inzicht in naleving van de regels	Accepteren	4	8,7%	1	5,6%	3	11,1%	0	0,0%
	Vermijden	9	19,6%	6	33,3%	3	11,1%	0	0,0%
	Verminderen	5	10,9%	2	11,1%	2	7,4%	0	0,0%
	Verzekeren	2	4,3%	0	0,0%	2	7,4%	0	0,0%
	Totaal	20	43,5%	9	50,0%	10	37,0%	0	0,0%

Matrix 4: Verdeling juridische risico's per klasse over de hoofddoelgroepen

Uit bovenstaand overzicht wordt duidelijk dat de LinkedIn-groepen in 80% van de reacties hoger scoren dan de gemiddelde reactie. Dit in tegenstelling tot het zakelijk netwerk dat slechts in 20% van de mogelijkheden een hoger percentage vertoont. Daarnaast is er één respondent geweest waarvan de doelgroep onbekend is. Hieruit kan worden opgemaakt dat de resultaten op het gebied van de juridische risico's niet hoeven worden uitgesplitst per hoofddoelgroep, aangezien de belangrijkste doelgroep de grootste invloed heeft gehad.

4.5 Verdeling risico's over de branches

De elf branches die vertegenwoordigd zijn in dit onderzoek kunnen worden verdeeld in drie hoofdbranches.
Onder de branche dienstverlening vallen:
- respondenten uit de branche Zakelijke dienstverlening
- respondenten uit de branche Financiële dienstverlening
- respondenten uit de branche Overige dienstverlening

De tweede hoofdbranche Overheid betreft de respondenten uit de branche Openbaar bestuur/Overheid

En onder de branche Overig zijn de volgende branches geplaatst:
- Bouwnijverheid
- Groot- & detailhandel
- Horeca
- Gezondheids- & welzijnszorg
- Industrie
- Informatie & Communicatie
- Overig

Indien op basis van deze drie hoofdbranches naar de organisatorische risico's wordt gekeken worden, ontstaat matrix 5.

Risico		Totaal		Dienstverlening (17)		Overheid (15)		Overige branches (18)	
		Aantal	%	Aantal	%	Aantal	%	Aantal	%
Leveranciers lock-in	Accepteren	12	19%	3	17,6%	1	6,7%	4	22,2%
	Vermijden	11	17%	4	23,5%	1	6,7%	3	16,7%
	Verminderen	9	14%	3	17,6%	3	20,0%	2	11,1%
	Verzekeren	1	2%	1	5,9%	0	0,0%	0	0,0%
	Totaal	33	52%	11	64,7%	5	33,3%	9	50,0%
Data lock-in	Accepteren	3	5%	2	11,8%	1	6,7%	0	0,0%
	Vermijden	11	17%	1	5,9%	2	13,3%	6	33,3%
	Verminderen	8	13%	3	17,6%	1	6,7%	1	5,6%
	Verzekeren	1	2%	0	0,0%	0	0,0%	1	5,6%
	Totaal	23	37%	6	35,3%	4	26,7%	8	44,4%
Governance niet goed geregeld	Accepteren	2	3%	1	5,9%	0	0,0%	1	5,6%
	Vermijden	8	13%	3	17,6%	1	6,7%	1	5,6%
	Verminderen	17	27%	3	17,6%	6	40,0%	4	22,2%
	Verzekeren	1	2%	0	0,0%	0	0,0%	1	5,6%
	Totaal	28	44%	7	41,2%	7	46,7%	7	38,9%
Imagoschade door toedoen van andere bedrijven	Accepteren	3	5%	1	5,9%	0	0,0%	1	5,6%
	Vermijden	13	21%	2	11,8%	4	26,7%	5	27,8%
	Verminderen	11	17%	4	23,5%	3	20,0%	1	5,6%
	Verzekeren	4	6%	2	11,8%	0	0,0%	1	5,6%
	Totaal	31	49%	9	52,9%	7	46,7%	8	44,4%
Cloud leverancier stopt met diensten	Accepteren	4	6%	1	5,9%	0	0,0%	3	16,7%
	Vermijden	8	13%	1	5,9%	1	6,7%	4	22,2%
	Verminderen	10	16%	6	35,3%	0	0,0%	3	16,7%
	Verzekeren	4	6%	1	5,9%	0	0,0%	0	0,0%
	Totaal	26	41%	9	52,9%	1	6,7%	10	55,6%
Onbekendheid met nieuwe omgeving	Accepteren	9	14%	2	11,8%	2	13,3%	2	11,1%
	Vermijden	3	5%	1	5,9%	0	0,0%	2	11,1%
	Verminderen	10	16%	1	5,9%	3	20,0%	4	22,2%
	Verzekeren	1	2%	0	0,0%	0	0,0%	1	5,6%
	Totaal	23	37%	4	23,5%	5	33,3%	9	50,0%

Matrix 5: Organisatorische risico's per branchegroep

Uit de matrix wordt zichtbaar dat de overheid sterk risicomijdend en risicobeperkend gedrag vertoond. Slechts in enkele gevallen wordt een risico geaccepteerd. Dit komt overeen met het uitgangspunt van de overheid om voornamelijk gebruik te maken van "proven technology". De meeste risico's zijn dan reeds bekend en kunnen daardoor eenvoudiger worden vermeden of beperkt.
De meeste risico's zijn redelijk evenwichtig verdeeld over de branches. Hierin zijn twee opvallende, maar verklaarbare, uitzonderingen:

1. het risico dat de cloud leverancier stopt met het leveren van diensten. Respondenten uit de overheid geven slechts eenmaal aan dit risico te onderkennen. Door mantelafspraken binnen de overheid is de levering van diensten voor een vaste tijd gegarandeerd. Daarna moeten opnieuw mantelafspraken worden gemaakt. De overheid is gewend dan over te moeten stappen naar nieuwe leveranciers.

2. het risico met betrekking tot de onbekendheid van de nieuwe omgeving.
   De helft van de respondenten uit de overige branches onderkent dit risico. Dit zou te verklaren zijn uit het feit dat deze branches eerder de overstap zetten naar nieuwe technologieën en hierdoor dus meer met onbekende omgevingen te maken krijgen.

Ook de juridische risico's kunnen worden ingedeeld per hoofdbranche.

Risico		Totaal (46)		Dienstverlening (15)		Overheid (14)		Overige branches (16)	
		Aantal	%	Aantal	%	Aantal	%	Aantal	%
Inbeslagname van data	Accepteren	1	2,2%	0	0,0%	0	0,0%	1	6,3%
	Vermijden	11	23,9%	5	33,3%	2	14,3%	4	25,0%
	Verminderen	2	4,3%	0	0,0%	1	7,1%	1	6,3%
	Verzekeren	0	0,0%	0	0,0%	0	0,0%	0	0,0%
	Totaal	14	30,4%	5	33,3%	3	21,4%	6	37,5%
Documentatie niet (tijdig) beschikbaar voor onderzoeken	Accepteren	4	8,7%	4	26,7%	0	0,0%	0	0,0%
	Vermijden	8	17,4%	1	6,7%	5	35,7%	2	12,5%
	Verminderen	6	13,0%	2	13,3%	1	7,1%	3	18,8%
	Verzekeren	0	0,0%	0	0,0%	0	0,0%	0	0,0%
	Totaal	18	39,1%	7	46,7%	6	42,9%	5	31,3%
Beperkingen door wet- en regelgeving	Accepteren	6	13,0%	2	13,3%	1	7,1%	3	18,8%
	Vermijden	10	21,7%	4	26,7%	4	28,6%	2	12,5%
	Verminderen	2	4,3%	0	0,0%	1	7,1%	1	6,3%
	Verzekeren	1	2,2%	0	0,0%	0	0,0%	1	6,3%
	Totaal	19	41,3%	6	40,0%	6	42,9%	7	43,8%
Privacy van data is niet voldoende geborgd	Accepteren	4	8,7%	1	6,7%	1	7,1%	2	12,5%
	Vermijden	22	47,8%	8	53,3%	8	57,1%	6	37,5%
	Verminderen	7	15,2%	2	13,3%	1	7,1%	4	25,0%
	Verzekeren	4	8,7%	2	13,3%	0	0,0%	1	6,3%
	Totaal	37	80,4%	13	86,7%	10	71,4%	13	81,3%
Onvoldoende inzicht in naleving van de regels	Accepteren	4	8,7%	3	20,0%	0	0,0%	1	6,3%
	Vermijden	9	19,6%	3	20,0%	5	35,7%	2	12,5%
	Verminderen	5	10,9%	0	0,0%	2	14,3%	3	18,8%
	Verzekeren	2	4,3%	0	0,0%	1	7,1%	1	6,3%
	Totaal	20	43,5%	6	40,0%	8	57,1%	7	43,8%

Matrix 6: Juridische risico's per branchegroep

De conclusies van de organisatorische risico's komen ook terug bij de juridische risico's. De overheid verzekert en accepteert zeer beperkt de risico's en neemt voornamelijk maatregelen te vermijding en beperking van de risico's. Daarnaast zijn de percentages redelijk gelijkmatig verdeeld over de branches. Als opvallende uitkomst kan het percentage van 57,1% voor de overheid worden gezien op het risico dat er onvoldoende inzicht is in de naleving van de regels. Voor een branche die zelf de wet- en regelgeving bepaald, zou verwacht mogen worden dat dit percentage beduidend lager ligt.

4.6 Hoofdvraag: Wat zien organisaties als de belangrijkste organisatorische en juridische risico's bij het gebruik van cloud computing en hoe gaan zij met deze risico's om?

De literatuur benoemde zes organisatorische risico's en hun mogelijke maatregelen. Hierbij werd geen verschil gemaakt tussen de risico's op het gebied van gevolgen, kans van optreden of impact.

Dezelfde risico's worden in de praktijk onderkend. Op basis van het aantal respondenten dat het risico adresseert, kan hieruit wel een prioriteitstelling plaatsvinden. Tevens werd in de literatuur slechts beperkt de maatregelen aangestipt. In de definitieve risicomatrix wordt zowel de prioritering van de risico's als een uitgebreider overzicht van de maatregelen weergegeven. Hierbij geldt dat veelal het inzetten van meerdere maatregelen helpt bij goede risicobeheersing.

Bij het onderzoek naar de juridische risico's is duidelijk geworden, dat cloud computing een moderne toepassing is die de afgelopen jaren steeds meer aandacht heeft gekregen. De risico's genoemd in de literatuur zijn zeker van toepassing en worden door alle respondenten onderkend. Het belangrijkste juridische risico was echter in de literatuur nog niet naar boven gekomen.

Ondanks dat de Patriot Act in de USA al sinds de aanslagen van 11 september 2001 bestaat, krijgt deze wet het laatste jaar steeds meer aandacht. Voor veel bedrijven worden de risico's van deze wet voor hun eigen organisatie duidelijk. Het meest genoemde risico is dan ook het risico dat data beschikbaar kan/moet worden gesteld aan andere bedrijven/overheden, doordat de data niet enkel is opgeslagen op Nederlands grondgebied en bij Nederlandse bedrijven. Maatregelen tegen dit risico worden amper genomen. Voor veel organisaties betekent dit risico een No Go voor de overstap naar een cloud omgeving.

4.6.1 Definitieve versie risicomatrix

In de definitieve risicomatrix worden de risico's getoond waarbij op basis van de respons de prioriteit is bepaald. De relatie van het risico met de maatregelen wordt opgesplitst in maatregelen voor het vermijden en het verminderen van het risico. Indien de maatregel helpt bij het vermijden van het risico staat er een ▲ in de matrix. Helpt de maatregel bij het verminderen van het risico, dan is een ▽ geplaatst in de matrix. Maatregelen die worden zowel bij vermijden als bij verminderen zijn benoemd, bevatten beide tekens.

De categorie organisatorische maatregelen is aangevuld met één extra risico. Naast de risico's, genoemd in de literatuur, zijn er ook meerdere risico's benoemd met betrekking tot de beschikbaarheid en beveiliging van data. Van de overige risico's kan niet worden geconcludeerd dat ze voor meerdere organisaties belangrijk zijn en zijn dus niet afzonderlijk opgenomen in de matrix. Dit zelfde geldt voor de juridische risico's waar het risico dat data ter beschikking komt van een derde partij door wet- en regelgeving is opgenomen. Ook hier waren de respondenten zeer uitgesproken over in tegenstelling tot de andere extra genoemde risico's.

De definitieve matrix is te vinden in paragraaf 5.1.6. Voor de leesbaarheid wordt de matrix opgeknipt in twee delen. Eerst wordt de matrix voor de organisatorische risico's getoond. Op de pagina erna wordt de matrix met de juridische risico's getoond.

5 Conclusies en aanbevelingen

5.1 Conclusies

Hieronder worden de deelvragen in aparte paragrafen behandeld. Daarna volgt het antwoord op de hoofdvraag. In paragraaf 5.2 volgen aanbevelingen voor een vervolgonderzoek.

5.1.1 Welke organisatorische risico's worden door organisaties als meest risicovol aangeduid?

Uit het onderzoek is duidelijk geworden dat er zeven risico's benoemd kunnen worden die voor alle branches van toepassing zijn bij het gebruik maken of overstappen naar een cloud omgeving.
Het betreft de volgende zeven risico's:

1. Leveranciers lock-in
2. Imagoschade door toedoen van andere bedrijven
3. Governance niet goed geregeld
4. Cloud leverancier stopt met leveren van diensten
5. Data lock-in
6. Onbekendheid met de nieuwe omgeving
7. Databeschikbaarheid en beveiliging

De eerste zes risico's waren reeds gedefinieerd vanuit de literatuur. Hieruit kan worden geconcludeerd dat in de literatuur daadwerkelijk de belangrijkste risico's worden besproken. De redenering dat respondenten de risico's hebben gekozen omdat ze waren benoemd en dus geen moeite hoefden te doen, wordt teniet gedaan door het aantal andere risico's dat zij zelf aangaven. Hierbij is het zevende risico meerdere keren besproken, zodat dit risico met een reactie van 16% als belangrijk risico geclassificeerd kan worden. Wel kan de volgorde hierdoor zijn beïnvloed. Ondanks de snelle technologische ontwikkelingen rondom cloud computing blijven de risico's op organisatorisch niveau dus zeer constant.

Waar de risico's minimaal veranderen, kan er wel een grote afwijking worden geconstateerd bij de maatregelen die ingezet kunnen worden. Werden in de literatuur de maatregelen slechts beperkt genoemd, in de definitieve matrix (matrix 7) worden er achttien maatregelen ingezet om de risico's te vermijden of te verminderen. Door de toename van kennis op het gebied van de risico's en de mogelijke gevolgen kunnen specifieke maatregelen worden genomen om (een deel van) het risico af te dekken. De toekomstige literatuur zal waarschijnlijk een breder spectrum aan maatregelen belichten.

Nuancering hoofddoelgroepen

De zeven risico's zijn hierboven genoemd gerangschikt op basis van het totale aantal respondenten. Zoals in paragraaf 4.4 is geconcludeerd zijn verschillen tussen de hoofddoelgroepen. Dit verschil komt in de rangschikking duidelijk naar voren.
Bij de LinkedIn-groepen blijft de volgorde gelijk op 1 risico na. Het data lock-in risico verschuift van de vijfde naar de eerste plaats. Dit is niet vreemd aangezien in de literatuur reeds werd aangegeven dat een belangrijk onderdeel van de lock-in de data lock-in betreft en dat deze lastiger te voorkomen is.

Bij het zakelijk netwerk wisselt de data lock-in daarentegen met de onbekendheid met de nieuwe omgeving naar een lagere positie. Tevens wordt imagoschade door toedoen van andere bedrijven als grootste risico gezien.
De prioritering van de groep waarvan niet bekend is tot welke doelgroep ze behoren, komt volledig overeen met de gemiddelde reactie.

Doordat zowel de prioritering van de onbekende groep als de LinkedIn-groep, op de data lock-in na, overeenkomen met de overall reactie kan worden geconstateerd dat deze prioritering correct is. Alleen de plaats van de data lock-in in het overzicht is zeer wisselend. Overall geeft slechts 37% van de respondenten aan dit risico belangrijk te vinden, terwijl 60% van de LinkedIn-respondenten en de literatuur aangeven dat data lock-in een groot risico betreft. De keuze is dan ook gemaakt om het risico op de tweede plaats neer te zetten. Op basis hiervan dient het overzicht van de zeven belangrijkste risico's te worden aangepast tot het volgende overzicht:

1. Leveranciers lock-in
2. Data lock-in
3. Imagoschade door toedoen van andere bedrijven
4. Governance niet goed geregeld
5. Cloud leverancier stopt met leveren van diensten
6. Onbekendheid met de nieuwe omgeving
7. Databeschikbaarheid en beveiliging

De leveranciers lock-in heeft een zelfde score gehaald als de data lock-in. Aangezien de leveranciers lock-in door alle doelgroepen zijn benoemd, neemt deze de eerste plaats in en wordt deze op de voet gevolgd door de data lock-in.

5.1.2 Wat zijn voor organisaties de belangrijkste juridische risico's?

Naast de eerder genoemde organisatorische risico's worden ook door zowel de literatuur als de respondenten juridische risico's onderkend. Op basis van beide onderzoeken worden de volgende zes risico's als meest belangrijk geclassificeerd:

1. Privacy van data niet voldoende geborgd
2. Onvoldoende inzicht in naleving van de regels
3. Beperkingen door wet- & regelgeving
4. Documentatie niet (tijdig) beschikbaar voor onderzoek
5. Inbeslagname van data
6. Data ter beschikking van derde partij i.v.m. wet-/regelgeving

De eerste vijf risico's worden in de literatuur van de afgelopen jaren uitgebreid besproken en zijn ook door de respondenten bevestigd als belangrijke risico's. Het zesde risico werd tot voor kort echter slechts zijdelings behandeld in de literatuur. De laatste tijd wordt echter steeds duidelijker wat de impact is van wetgeving zoals de Amerikaanse Patriot Act, waardoor de overheid alle data op kan eisen van Amerikaanse bedrijven of buitenlandse bedrijven op Amerikaans grondgebied. Hierdoor is dit risico in zeer korte tijd één van de belangrijkste risico's geworden voor het gebruik van een cloud omgeving.
De reden waarom het risico met 24% op plaats zes staat, dient te worden bezien vanuit het gegeven dat de overige risico's reeds benoemd waren in het onderzoek. Hierdoor wordt eerder voor een risico gekozen, dan wanneer alles zelf moet worden geformuleerd. Tevens liggen risico 1 en risico 6 dicht bij elkaar. Doordat menig respondent naast risico 1 ook risico 6 heeft benoemd, is ook dit laatste risico met een lager percentage opgenomen in het overzicht.

De verwachting is dat de komende tijd er veel literatuur beschikbaar komt omtrent regels zoals de Patriot Act. Deze komen waarschijnlijk niet alleen vanuit de juridische hoek, maar ook vanuit de techniek zal aandacht worden besteed aan het voorkomen van dit risico.

5.1.3 Op basis van welke methode en afspraken zijn deze risico's geïdentificeerd?

De eerste conclusie die kan worden getrokken is dat de respondenten geen vaste methodiek voor risicomanagement gebruiken. Waar in de literatuur weinig verbanden werden gelegd tussen methodieken en de gevonden risico's, is dat ook na het uitvoeren van dit onderzoek niet mogelijk.

Veel respondenten geven aan geen specifieke risicomanagementmethode te hanteren, maar vooral logisch na te denken.

Bij de respondenten die aangeven gebruik te maken van methodieken is dit zeer afhankelijk van hun achtergrond.
Veelgenoemde methoden als Prince2, Management of Risk (MoR) en Managing Successful Programmes (MSP) komen voornamelijk voor bij projectleiders.
Daarnaast worden ook methoden als Cobit framework, FIRM, NIST, ISF en Octave Allegro gebruikt. Deze methodieken verdiepen zich meer in risico's binnen de gehele organisatie, in tegenstelling tot een RUP[7]-methodiek die met name gericht is op softwareontwikkeling.

De risicomethodieken zijn zo divers dat hieruit geen conclusies kunnen worden getrokken. Wel valt op dat er veel organisaties geen expliciete methodiek hanteren, maar gebruik maken van ervaringen en best practices om op deze manier hun eigen risicomethodiek te creëren.

5.1.4 Hoe classificeren de organisaties de benoemde risico's?

In de literatuur wordt hier helemaal niet over gesproken. Er is dan ook geen vergelijking met de theorie te maken. De verwachting dat de classificatie afhankelijk is van de branche waarin een organisatie werkzaam is, kan ook niet worden aangetoond in dit onderzoek.

Geconstateerd kan enkel worden dat alle organisatorische risico's alle vier de classificaties accepteren, vermijden, verminderen en verzekeren hebben gekregen. Bij de juridische risico's is hier een klein verschil zichtbaar. De risico's "Inbeslagname van data", "Documentatie niet tijd beschikbaar" kennen niet de classificatie verzekeren. De overige classificaties zijn wel toebedeeld.

De grote uitzondering betreft de classificaties van het risico "Data ter beschikking van derde partij i.v.m. wet-/regelgeving". Waar eerder al was geconstateerd dat dit een relatief nieuw risico was, waar veel aandacht voor is, dient nu ook geconstateerd te worden dat dit een echte showstopper is. Dit risico is het enige risico waaraan enkel de classificatie vermijden is toebedeeld. Dit is goed verklaarbaar omdat bij het optreden van dit risico de kans van optreden van alle andere risico's wordt vergroot.

In bijlage 4a is een extractie van de onderzoeksdata opgenomen, waarin per risico en per classificatie het aantal respondenten en de branches wordt weergegeven.

[7] RUP: Rational Unified Process

5.1.5 Welke maatregelen worden ingezet om risico's te beperken of te vermijden?

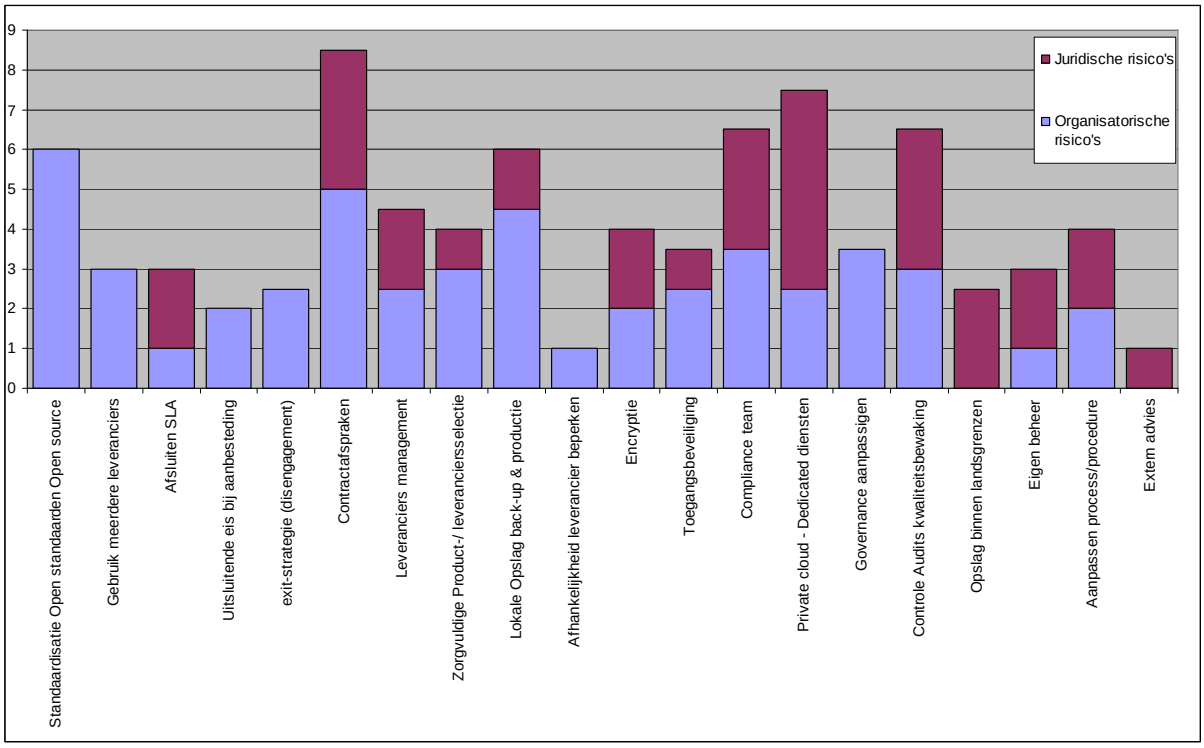
Zoals in matrix 7 is aangegeven zijn er veel maatregelen mogelijk om de risico's te beheersen. De maatregelen zijn per risico benoemd en in de matrix samengevat onder overkoepelende woorden. Hierbij wordt inzichtelijk dat een aantal maatregelen voor zowel als risicomijdende als risicobeperkende acties kan worden ingezet.

Het afsluiten van goede Service Level Agreements (SLA) wordt echter door iedereen enkel ingezet als risicobeperkende maatregel. Dit is verklaarbaar doordat deze pas worden afgesloten als de organisatie reeds gebruik maakt van de cloud omgeving, waardoor sommige risico's niet meer vermeden kunnen worden. Dit in tegenstelling tot de contractafspraken die vooraf worden gemaakt en die dus ook wel als risicomijdende actie wordt ingezet. Twee andere maatregelen die enkel als beperkende maatregel worden gebruikt zijn het beperken van de afhankelijkheid van de leverancier en het gebruik maken van extern advies. Deze maatregelen hebben tevens invloed op elkaar. Door het binnenhalen van extern advies (anders dan de leverancier) wordt de afhankelijkheid verminderd en dus ook de risico's die hierdoor op kunnen treden.

Het gebruik van een private cloud daarentegen wordt vooral gezien als risicomijdende actie. Het biedt de mogelijkheid om met minder risico's een aantal voordelen uit de cloud ter beschikking te hebben. Risico's met betrekking tot andere gebruikers van dezelfde omgevingen worden volledig voorkomen. Of risico's met betrekking tot de leveranciers worden voorkomen is afhankelijk van de wijze waarop de private cloud is ingericht. Indien dit bij een derde partij gebeurt en dus voornamelijk gericht is op het hebben van een dedicated dienst, blijft een aantal risico's wel degelijk bestaan. Indien de organisatie zelf een datacenter inricht gebaseerd op de techniek achter een private cloud omgeving komen verschillende risico's daadwerkelijk te vervallen.

Door aan de maatregelen een waarde toe te kennen, is inzichtelijk geworden welke maatregelen het vaakst worden ingezet. Hiertoe krijgen risicobeperkende maatregelen een waarde van 0,5 en risicomijdende maatregelen een waarde van 1. Overall gezien wordt hierdoor duidelijk dat extern advies en het beperken van de afhankelijkheid van de leverancier de minst belangrijke maatregelen zijn, in tegenstelling tot contractafspraken en de inzet van een private cloud.
Voor enkel de organisatorische risico's is de inzet van standaardisatie de meest gebruikte maatregel ter vermijding en vermindering van de risico's. Als minst gebruikte maatregel geldt hier het afsluiten van SLA's en, net als bij het totale overzicht, het beperken van de afhankelijkheid van de leverancier.
Voor de juridische risico's is de private cloud de meest gehanteerde maatregel.

Zoals in figuur 6 wordt getoond zijn er een verschillende maatregelen die niet worden ingezet bij juridische risico's. Dit betreffen maatregelen die geen betrekking hebben op juridische aspecten.



Figuur 6: Inzet maatregelen bij organisatorische en juridische risico's

Tevens is het mogelijk om de maatregelen in te delen in drie hoofdcategorieën:
- Techniek
- Afspraken
- Organisatie-inrichting

De technische maatregelen beperken de afhankelijkheid van andere partijen door middel van standaardisatie, exit-strategieën en het gebruik van meerdere leveranciers. Maar ook encryptie en het gebruik van lokale opslag of een private cloud biedt een technische oplossing voor de geconstateerde risico's.

Afspraken met leveranciers in contracten en SLA's zorgen voor een goede relatie tussen afnemer en leverancier(s), waarbij afspraken en verantwoordelijkheden duidelijk onderling zijn afgestemd en vastgelegd. De juridische risico's worden voornamelijk met deze categorie maatregelen beperkt of vermeden.

De laatste categorie betreft organisatie aanpassingen. Door de inrichting van onder andere compliance teams, leveranciersmanagement en auditteams zorgen afnemers ervoor dat zij aan het roer blijven en niet te afhankelijk worden van externe adviseurs of leveranciers.

Waar de juridische risico's voornamelijk worden afgehecht met maatregelen op het gebied van afspraken, zijn er voor de organisatorische risico's meer mogelijkheden. Dit blijkt ook uit figuur 6, waarin zes maatregelen zichtbaar zijn die enkel voor de organisatorische risico's gelden in tegenstelling tot één specifiek juridische maatregel. Maatregelen voor organisatorische risico's kunnen vanuit organisatorisch oogpunt (organisatie-inrichting en afspraken) worden genomen, maar ook kan vanuit de techniek worden gehandeld. Dit zal veelal de eerste stap zijn, omdat hiermee ook eventuele technische risico's worden afgehecht. Daarnaast heeft een organisatie meestal niet de behoefte om de organisatie te wijzigingen bij de implementatie van nieuwe technologieën.

Terugkijkend naar de literatuur werden daar vijf maatregelen genoemd, namelijk standaardisatie, encryptie, gebruik meerdere leveranciers, lokale opslag en afsluiten SLA's. Standaardisatie en lokale opslag worden ook door de respondenten als meest gebruikte maatregel genoemd ter vermijding en vermindering van de risico's. Het afsluiten van SLA's daarentegen wordt in het kader van de organisatorische risico's als minst belangrijke maatregel gezien. Overall is de maatregel belangrijker, maar staat de maatregel nog steeds niet bij de belangrijkste 10.

5.1.6 Conclusie hoofdvraag

Op basis van bovenstaande conclusies kan worden vastgesteld dat matrix 7 de belangrijkste risico's op organisatorisch en juridisch gebied bevat voor organisaties die gebruik (gaan) maken van een cloud omgeving. Indien organisaties in ieder geval deze risico's onderkennen en classificeren, worden de grootste gevaren voorkomen. Tevens zorgt de risico-inventarisatie en classificatie voor een betere onderbouwing bij de besluitvorming om wel of niet gebruik te gaan maken van een cloud omgeving.

Organisatorische risico's

Risico	Standaardisatie / Open standaarden / Open source	Gebruik meerdere leveranciers	Afsluiten SLA	Uitsluitende eis bij aanbesteding	exit-strategie (disengagement)	Contractafspraken	Leveranciersmanagement	Zorgvuldige Product-/ leverancierselectie	Lokale Opslag back-up & productie	Afhankelijkheid leverancier beperken	Encryptie	Toegangsbeveiliging	Compliance team	Private cloud - Dedicated diensten	Governance aanpassigen	Controle, Audits kwaliteitsbewaking	Opslag binnen landsgrenzen	Eigen beheer	Aanpassen process/procedure	Extern advies
Leveranciers lock-in	▲▽	▲▽		▲	▲▽	▲▽	▽	▽	▽	▽										
Governance is niet goed geregeld			▽			▽	▽						▲▽		▲▽	▽			▲▽	
Imagoschade door toedoen van andere bedrijven	▲			▲			▲▽	▲			▲		▲			▲▽		▽	▽	
Cloud leverancier stopt met leveren van diensten	▽	▲▽			▽	▲▽		▽	▲▽						▲	▲		▽		
Data lock-in	▲▽		▽		▽	▲▽		▲	▲▽			▲▽	▲	▲	▽					
Onbekendheid met nieuwe IT-omgeving (bij overstap naar de cloud)	▲▽									▽				▽	▽					
Databeschikbaarheid & beveiliging									▲		▲	▲		▲						

Legenda: ▲ Risico vermijdende maatregel ▽ Risico verminderende maatregel

Juridische risico's

Risico	Standaardisatie / Open standaarden / Open source	Gebruik meerdere leveranciers	Afsluiten SLA	Uitsluitende eis bij aanbesteding	exit-strategie (disengagement)	Contractafspraken	Leveranciers management	Zorgvuldige Product-/ leverancierselectie	Lokale Opslag back-up & productie	Afhankelijkheid leverancier beperken	Encryptie	Toegangsbeveiliging	Compliance team	Private cloud - Dedicated diensten	Governance aanpassigen	Controle Audits kwaliteitsbewaking	Opslag binnen landsgrenzen	Eigen beheer	Aanpassen process/procedure	Extern advies
Privacy van data niet voldoende geborgd						▽		▲			▲	▲	▲	▲		▲▽	▲		▲	
Onvoldoende inzicht in naleving van de regels			▲			▲							▲	▲		▲▽				▽
Beperkingen door wet- & regelgeving													▲	▲			▲	▲		▽
Documentatie niet (tijdig) beschikbaar voor onderzoeken						▲	▲		▲▽					▲		▽		▲	▲	
Inbeslagname van data			▲			▲	▲				▲						▽			
Data ter beschikking van derde partij ivm wet-/regelgeving														▲						

Legenda: ▲ Risico vermijdende maatregel ▽ Risico verminderende maatregel

Matrix 7: Organisatorische en juridische risico's gerelateerd aan risicovermijdende en risicoverminderende maatregelen.

5.2 Aanbevelingen voor vervolgonderzoek

Tijdens de literatuurstudie werd al geconstateerd dat er slechts beperkt aandacht is in de literatuur voor het afnemersperspectief in relatie tot cloud computing. De aandacht gaat voornamelijk uit naar de leverancierszijde. Extra aandacht en informatie vanuit het afnemersperspectief kan juist zorgen voor een betere en soepelere adoptie van cloud computing door organisaties.

Vervolgonderzoeken die in dit kader zeer wenselijk zijn zouden zich kunnen richten op specifieke branches en ervaringen van andere afnemers. Hierdoor worden sommige resultaten uit dit onderzoek zeer waarschijnlijk versterkt en andere resultaten verzwakt, doordat er meer nadruk komt te liggen op een klein deel van het onderzoeksspectrum.

Tevens is het waardevol om onderzoek te doen naar welk deel van de IT-voorziening veilig en verantwoord in een cloud omgeving kan worden geplaatst en welke delen van de IT-voorziening beter in eigen beheer kunnen worden verzorgd. Meer inzicht hierin biedt organisaties de kans om gedeeltelijk over te stappen en toekomstige ontwikkelingen op de gewenste onderdelen te volgen. Op basis van de genoemde risico's zou een eerste conclusie zijn dat enkel niet-bedrijfskritische data kan worden geplaatst in een cloud omgeving. Of de overstap naar de cloud dan nog de moeite waard is, is hiermee nog niet beantwoord.

Naast onderzoeken omtrent cloud computing is het ook waardevol om onderzoek te doen naar risicomanagement en welke factoren van invloed zijn op de classificatie van risico's. De verwachting is dat deze classificatie wordt beïnvloed door meerdere factoren dan enkel de bedrijfsstrategie en de branche waarbinnen de organisatie werkzaam is. Door deze factoren te kennen, kunnen onderzoeken naar risico's zich richten op de factoren die hierop invloed uitoefenen. Tevens is uit dit onderzoek gebleken dat veel bedrijven geen expliciete risicomethodiek hanteren. Nader onderzoek ter bevestiging van deze conclusie en de gevolgen voor organisaties kan wellicht leiden tot nieuwe inzichten waarom bedrijven in de problemen raken, zodra er problemen optreden in de landelijk of internationale economie.

6 Reflectie

6.1 Product terugblik

Het onderzoek toont aan dat veel bedrijven nog terughoudend zijn met het volledig overgaan naar een cloud omgeving. Veel risicobeperkende of vermijdende maatregelen hebben betrekking op het zelf uitvoeren van beheeractiviteiten. Ook wordt vaak genoemd dat de data of een back-up hiervan in een eigen omgeving wordt geplaatst, om zo voldoende beschikbaar te zijn en te kunnen voldoen aan alle eisen en wensen die door de eigen organisatie of door andere organisaties worden gesteld.

Tevens is door veel respondenten aangegeven dat juridische risico's zeker onderkend worden, maar dat zij daar geen nadere informatie over mogen geven. Hierdoor wordt duidelijk dat dit punt niet onderschat moet worden, ondanks de relatief geringe reacties in het onderzoek. Ook in vervolgonderzoeken zal dit een lastig onderwerp zijn, niettemin is het wel belangrijk om ook hier onderzoek naar te doen. Wellicht dat bij onderzoek vanuit een juridische faculteit er meer informatie beschikbaar wordt gesteld, door het verschil in doelgroep en achtergrond.

Onderkend wordt dat het aantal respondenten slechts beperkt is. Het onderzoek kan daarom ook niet formeel als representatief worden aangemerkt. Voor een betrouwbaarheidspercentage van 95% en een steekproefmarge van 5% hadden 298 personen de vragenlijst moeten invullen. Een betrouwbaarheid van 95% is noodzakelijk om een resultaat te verkrijgen waaruit conclusies getrokken kunnen worden. Met het huidige aantal respondenten betekent dit dat de steekproefmarge oploopt naar 12,05% (bij een betrouwbaarheidspercentage van 95%). Daarbij is er een extra issue dat niet alle respondenten afkomstig zijn uit de LinkedIn-groepen. Hierdoor is het kennis- en ervaringsniveau op het gebied van cloud computing niet volledig gegarandeerd. Op basis van de uitkomsten uit het onderzoek, wordt er voornamelijk op het gebied van data lock-in een grote discrepantie herkend. De overige uitkomsten brengen geen grote veranderingen met betrekking tot prioritering of belang met zich mee. De verschillen tussen de gemiddelde reactie en de reactie van de LinkedIn-groepen zijn daarvoor te beperkt.

Het onderzoek kan op basis van deze cijfers dan ook worden gezien als een goed startpunt voor verder onderzoek. Daarbij moet worden onderkend dat bij het onderzoek verschillende organisaties en branches zijn betrokken. Indien dit onderzoek had plaatsgevonden binnen één branche was een nauwkeurigheidsafwijking van 12% zeer groot geweest.

Echter door de diversiteit aan branches en organisaties tonen de resultaten een overall overzicht, waardoor deze afwijking minder invloedrijk is en het onderzoek een bredere basisinformatie bevat.

Om de resultaten zo veel mogelijk meerwaarde te geven is ervoor gekozen om ook de relatie tussen het risico, de classificatie en de branche weer te geven. Hierdoor is inzichtelijk geworden dat ook binnen een branche er diverse classificaties aan hetzelfde risico worden toegekend. Onbekend is of indien het onderzoek binnen een specifieke branche gehouden zou worden, de classificaties duidelijke overeenkomsten zouden vertonen, doordat respondentengroep voor de branche dan omvangrijker is.

6.2 Procesreflectie

Door te kiezen voor een onbekend onderwerp met een snelle dynamische marktontwikkeling, was het lastig om te starten met het onderzoek. Ieder artikel bracht nieuwe kennis, informatie en mogelijkheden voor het onderzoek. Na veel zwerven en lezen is er een beeld ontstaan over cloud computing en is de onderzoeksopdracht geformuleerd met betrekking tot een klein onderdeel uit het grote cloud spectrum. Op basis van deze opdracht kon opnieuw de literatuur worden bekeken met behulp van lichtdoorschijnende oogkleppen. Deze hielpen om niet te veel te worden afgeleid door alle interessante extra informatie die voortdurend beschikbaar kwam, maar om wel zicht te blijven houden op de informatie in de grensgebieden. Dit alles heeft geleid tot een redelijk beeld van een specifiek onderdeel, namelijk risico's.

Tijdens het uiteindelijke onderzoek is gebleken dat zakelijke social media en de bijbehorende netwerken gedeeltelijk helpen bij het bereiken van een grote doelgroep. Geconstateerd is dat mensen geneigd zijn iets te doen voor een ander omdat ze deze persoon waarderen en respecteren. Dit effect werkt door in omliggende lagen. Hierdoor is het mogelijk om met een beperkt netwerk een groot tweedelijns netwerk te mobiliseren met hierin een diversiteit aan kennis, ervaringen, organisaties en branches. Algemene informatiegroepen waarin mensen elkaar niet persoonlijk kennen, bieden een zeer vrijblijvende omgeving waardoor mensen minder snel geneigd zijn om iets voor elkaar te doen. Dit is duidelijk zichtbaar geworden uit het feit dat een groot deel van de respondenten afkomstig is uit mijn eerste- en voornamelijk tweedelijns zakelijk netwerk. Om te voorkomen dat er onvoldoende reacties kwamen vanuit de eerdere aangegeven interessegroepen is besloten om ook gebruik te maken van mijn eigen zakelijk netwerk. Geconcludeerd kan dan ook worden dat voor het bereiken van grote groepen onbekende mensen social media niet de aangewezen constructie is.

Maar dat voor het bereiken van een brede groep van beperkte omvang social media zeker toegevoegde waarde biedt, al dient hierbij de kanttekening gemaakt te worden dat de representativiteit van de groep wordt gelimiteerd doordat het allemaal mensen zijn die gebruik maken van de betreffende netwerksites.

Toch heb ik geen spijt van de gekozen werkwijze. Indien de onderzoeksmethode had bestaan uit het voeren van interviews, waren er slechts enkele organisaties betrokken geweest. Deze organisaties zouden allemaal werkzaam zijn geweest in dezelfde branche. De resultaten waren dan ook slechts voor enkele organisaties in de desbetreffende branche interessant geweest. De huidige resultaten bieden een basis voor een veel omvangrijkere doelgroep en kunnen als input dienen voor verscheidene vervolgonderzoeken.

Door het uitvoeren van deze masterscriptie is de nut en noodzaak van een goede opdrachtformulering heel duidelijk geworden. Indien een opdracht te veel ruimte biedt voor interpretaties levert dit later in het traject problemen op. Ook het achterhalen van de juiste literatuur, het uitvoeren van onderzoeken en het verwoorden van onderbouwde conclusies is waardevolle kennis en ervaring voor toekomstige onderzoeken. Daarnaast hebben reacties op conceptdocumenten van zowel mijn begeleider als mensen uit mijn omgeving geholpen om voldoende diepgang in het onderzoek te brengen en de informatie die in mijn hoofd zat ook op papier te laten belanden. Hierbij kan ik constateren dat deze kennis en ervaring niet alleen van belang is bij een eventueel volgend wetenschappelijk onderzoek, maar ook in het dagelijks werk toegevoegde waarde biedt.

7 Referenties

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2009), *Above the clouds: a Berkeley View of Cloud Computing*, Technical Report No UCB/EECS-2009-28, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Buyya, R., Yeo, C., Venugopal, S., Broberg, J. & Brandic, I. (2009), Cloud omputing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future generation Computer Systems,* 25(6), 599-616 DOI: 10.1016/j.future.2008.12.001

Chen, Y., Paxson, V. & Katz, R.H. (2010), *"What's new about cloud computing security?"*, Technical Report No UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009), Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW, 2009, 85-90 DOI: 10.1145/1655008.1655020

Clarke, C. (2010), Computing Clouds on the Horizon? Benefits and Risks from the User's Perspective. *23rd Bled eConference*, Slovenia, 20-23, www.rogerclarke.com/II/CCBR.html

Enisa (2009), *Cloud Computing: Benefits, risks and recommendations for Information Security*. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Ertaul, L., Singhal, S. & Saldamli, G. (2010), Security Challenges in Cloud Computing, *Security and Management, 2010*, 36-42

Hilley, D. (2009), *Cloud Computing: A taxonomy of Platform and Infrastructure-level Offerings*, Techical Reports GIT-CERCS-09-13, 2009, Georgia Institute of Technology

Jansen, W. (2011), Gloud Hooks: Security and Privacy Issues in Cloud Computing, *System Sciences (HICSS)*, 44th Hawaii International Conference, http://www.hicss.hawaii.edu/hicss_44/bp44/st1.pdf

Jansen, W. & Grance, T. (2011), *Guidelines on Security and Privacy in Public Cloud Computing*. NIST, Draft Special Publication 800-144

Khajeh-Hosseini, A., Sommerville, I. & Sriram, I. (2010), Research Challenges for Enterprise Cloud Computing,*1st ACM Symposium on Cloud Computing (SOCC 2010)*, http://arxiv.org/abs/1001.3257

Kim, W. (2009), Cloud Computing: Today and Tomorrow, *Journal of Object Technology*, *8*(1), 65-72

Mahmood, Z. (2011), Data Location and Security Issues in Cloud Computing, *International Conference on Emerging Intelligent Data and Web Technologies (2011),* DOI: 10.1109/EIDWT.2011.16

Mell, P., Grance, T. (2011), *The NIST Definition of Cloud Computing (Draft),* National Institute of Standards and Technology U.S. Department of Commerce, http://www.nist.gov/itl/cloud/

Mirzaei, N. (2008), *Cloud Computing,* Indiana University, http://grids.ucs.indiana.edu/ptliupages/publications/ReportNarimanMirzaeiJan09.pdf

Oriol Fitó, J. & Guitart, J. (2010), *Introducing Risk Management into Cloud Computing*, Computer Architecture Department, Technical University of Catalonia, Tech. Rep. UPC-DAC-RR-2010-33, http://gsi.ac.upc.edu/apps/reports/2010/33/cnsm10.pdf

Overbeek, P., Lindgreen, E. & Spruit, M, (2005), *Informatiebeveiliging onder controle* (2de ed.). Amsterdam, Pearson Education Benelux.

Ramgovind, S., Eloff, M. & Smith, E. (2010), The Management of Security in Cloud Computing, *Information Security for South Asia (ISSA)*, 1-7, http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/27_Paper.pdf

Sotto, L., Treacy, B. & McLellan, M. (2010), Privacy and Data Security Risks in Cloud Computing, *Electronic Commerce & Law Report,* 15 ECLR(186).

Subashini, S. & Kavitha, V. (2010), A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,*34(1), 1-11
DOI: 10.1016/j.jnca.2010.07.006

Tabaki, H., Joshi, J. & Ahn, G. (2010a), SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Enviroments, *IEEE 34th Annual Computer Software and Applications Conference Workshops*, IEEE CS Press, 393-398, DOI 10.1109/COMPSACW.2010.74

Tabaki, H., Joshi, J., Ahn, G. (2010b), Security and Privacy Challenges in Cloud Computing Enviroments, *IEEE Security and Privacy*, 8, 24-31, http://ldc.usb.ve/~figueira/cursos/Seguridad/Material/W_SP_SecurityPrivacyChallenges.pdf

Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H. & Kanai, A. (2011), Risk Management on the Security Problem in Cloud Computing, *Computers, Networks, Systems and Industrial Engineering (CNSI)*, 2011, 147-152, DOI: 10.1109/CNSI.2011.82

Zhang, X., Wuwong, N., Li, H. & Zhang, X. (2010), Information Security Risk Management Framework for the Cloud Computing Environments, *Computer and Information Technology (CIT)*, 2010, 1328-1334

Bijlage 1 Samenvattingen literatuur

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2009), *Above the clouds: a Berkeley View of Cloud Computing*, Technical Report No UCB/EECS-2009-28, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS- 2009-28.html
Het artikel is in een beknoptere versie in 2010 nogmaals gepubliceerd in *Communications of the ACM, 53*(4), 50-58.
Samenvatting: Cloud computing heeft de potentie om een groot deel van de IT-industrie te transformeren door het nog aantrekkelijker maken van software als een service en de wijze waarop IT-hardware is ontworpen en gekocht. Ontwikkelaars met innovatieve ideeën voor nieuwe internetdiensten hebben geen grote kapitaaluitgaven meer nodig voor de hardware om de dienst te leveren of voor de inhuur van personeel om de hardware te bedienen. Ze hoeven niet bezorgd te zijn voor verspilling van kostbare middelen of gebrek aan middelen, waardoor potentiële klanten en omzet kon worden misgelopen. De elasticiteit van de middelen, zonder het onnodig betalen hiervan, is ongekend in de geschiedenis van IT. Cloud computing heeft betrekking op zowel de applicaties, die als diensten via het internet beschikbaar worden gesteld, als de hardware en systeemsoftware in de datacenters die deze diensten bieden. Wanneer een cloud beschikbaar wordt gesteld in een pay-as-you-go manier aan het grote publiek, noemen we het een public cloud. De term private cloud wordt gebruikt om te verwijzen naar interne datacenters van een bedrijf of andere organisatie.
Vanuit hardwareoogpunt zijn er drie aspecten nieuw in cloud computing:

1. De illusie van oneindige IT-middelen beschikbaar op aanvraag, zodat er geen noodzaak voor cloud computing afnemers is om ver vooruit te plannen voor de inzet van extra middelen.
2. Het ontbreken van een afnameverplichting door cloud afnemers is, waardoor bedrijven klein kunnen beginnen en de toename van IT-middelen pas plaatsvindt als er behoefte aan is.
3. De mogelijkheid om te betalen voor tijdelijk gebruik van IT-middelen (bijvoorbeeld processors per uur en opslag van de dag) en het gebruik te beperken wanneer de middelen niet langer nodig zijn.

Buyya, R., Yeo, C., Venugopal, S., Broberg, J. & Brandic, I (2009), Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future generation Computer Systems,* 25(6), 599-616, DOI: 10.1016/j.future.2008.12.001
Samenvatting: Met de aanzienlijke vooruitgang van de informatie- en communicatietechnologie (ICT) in de afgelopen half eeuw, bestaat de verwachting dat de computer op een dag de 5de basisvoorziening (na water, elektriciteit, gas en telefonie) wordt.

Deze voorziening zal, net als de andere vier, worden beschouwd als essentieel voor de dagelijkse behoeften van de algemene gemeenschap. Voor deze visie zijn een aantal computerparadigma's voorgesteld, waarvan de laatste staat bekend als cloud computing. In dit paper wordt cloud computing gedefinieerd en wordt een architectuur geboden voor het creëren van cloud omgevingen, met marktgerichte toewijzing van middelen door gebruik te maken technologieën zoals virtuele machines.

Ook wordt inzicht geboden in strategieën voor middelenmanagement die zowel klantgericht (service management) als IT-gericht (risicobeheer) zijn, om Service Level Agreement (SLA)-georiënteerde toewijzing van middelen te ondersteunen. Daarnaast worden gedachten uit het verleden onthuld over onderling verbonden cloud omgevingen voor het dynamisch maken van de wereldwijde cloud markten. Tevens worden enkele representatieve Cloud platformen gepresenteerd samen met de mogelijkheid om marktgerichte toewijzing van middelen aan de clouds te realiseren. Ook worden de verschillen tussen de werklast met hoge performance computing (HPC) en op internet gebaseerde services besproken.

Chen, Y., Paxson, V. & Katz, R.H. (2010), "*What's new about cloud computing security?*", Technical Report No UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf
Samenvatting: Naast de economische argumenten vóór cloud computing, zijn de beveiligingsuitdagingen even opvallend. In dit artikel wordt geprobeerd het volledige kader van beveiligingsproblemen te benoemen in een poging de bezorgdheid te scheiden van overbezorgdheid. Hierbij wordt gekeken naar de hedendaagse en historische perspectieven uit het bedrijfsleven, de academische wereld en de overheid. Gesteld wordt dat enkele cloud computing beveiligingsproblemen fundamenteel hardnekkig of fundamenteel nieuw zijn ten opzichte van de traditionele computer. Veel problemen zijn door de tijd al onder de aandacht gebracht. Toch zijn er twee facetten tot op zekere hoogte nieuw en fundamenteel voor cloud computing: De complexiteit van het gebruik door meerdere partijen van dezelfde omgeving en de daaruit voortvloeiende behoefte aan wederzijdse controleerbaarheid.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009), Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW, 2009, 85-90, DOI: 10.1145/1655008.1655020

Samenvatting: Cloud computing is een aantrekkelijke technologie door zijn mogelijkheden van kostenefficiëntie en flexibiliteit. Echter er zijn, ondanks de stijging van activiteiten en interesse, aanzienlijke en aanhoudende zorgen over cloud computing. Deze belemmeren het momentum en vragen om een compromis voor de visie van cloud computing als nieuw IT-aankoopmodel. In dit artikel worden de problemen en hun impact op de adoptie besproken. Daarnaast, en even belangrijk, wordt beschreven hoe de combinatie van bestaande onderzoeksrichtingen de potentie heeft om veel zorgen te verlichten die adoptie verhinderen. In het bijzonder wordt gesteld dat met onderzoek naar de vooruitgang in trusted computing en encryptie, het gebruik van de cloud vanuit een business intelligence standpunt zeer gunstig kan zijn in tegenstelling tot het geïsoleerde alternatief dat nog steeds zeer gangbaar is.

Clarke, C. (2010), Computing Clouds on the Horizon? Benefits and Risks from the User's Perspective. *23rd Bled eConference*, Slovenia, 20-23, www.rogerclarke.com/II/CCBR.html

Samenvatting: Er zijn reeds analyses uitgevoerd vanuit het perspectief van de service providers, waardoor de noodzaak ontstaat voor analyses vanuit het oogpunt van de toekomstige afnemers. Dit artikel geeft een kritisch onderzoek van het onderwerp. De gekozen aanpak is het voeren van een grondige herziening van academische, commerciële en populaire literatuur aangevuld door de praktijk.
Tot op heden zijn er weinig formele publicaties die het perspectief van de afnemers bespreken. Het artikel kijkt naar de betekenis van het woord, een werkdefinitie, de omvang, en een architectonische model.

De potentiële voordelen voor de afnemers worden, in gestructureerde vorm, gepresenteerd. Nadelen en risico's worden daarna beschouwd. Hoewel de specifieke elementen reeds zijn besproken in verschillende eerdere publicaties zijn er weinig bronnen beschikbaar die geprobeerd hebben een uitgebreid overzicht te geven van de problemen die zich voordoen. Implicaties zijn getrokken voor de organisatorische en individuele afnemers, en de mogelijkheden voor onderzoekers zijn benoemd.

Enisa (2009), *Cloud Computing: Benefits, risks and recommendations for* Information Security. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Samenvatting: Cloud computing is een nieuwe manier van het leveren van IT-middelen, geen nieuwe technologie. Diensten, variërend van dataopslag en verwerking tot software, zoals e-mail afhandeling, zijn nu onmiddellijk en op aanvraag beschikbaar en vrij inzet. Omdat we in een tijd van bezuinigingen leven heeft dit nieuwe economische model voor IT-voorzieningen een vruchtbare grond gevonden.

De belangrijkste conclusie van dit paper is dat de schaalvoordelen en flexibiliteit van de cloud zowel vriend als vijand zijn vanuit het oogpunt van veiligheid. De enorme concentratie van middelen en gegevens vormen een aantrekkelijk doelwit voor aanvallers, maar de cloud gebaseerde verdediging betreft een robuuste, schaalbare en kosteneffectieve manier.

Dit document geeft een verantwoord oordeel van de veiligheidsrisico's en de voordelen van het gebruik van cloud computing - het bieden van veiligheid en begeleiding van potentiële en bestaande afnemers van cloud computing. De beoordeling van de veiligheid is gebaseerd op drie use case scenario's. Daarnaast wordt uitgelegd, op basis van concrete scenario's, wat cloud computing betekent voor netwerk- en informatiebeveiliging, gegevensbescherming en privacy. Gekeken wordt naar de beveiligingsvoordelen en risico's van cloud computing. Tevens worden concrete aanbevelingen gedaan over hoe de risico's kunnen worden beperkt en de voordelen gemaximaliseerd.

Ertaul, L., Singhal, S. & Saldamli, G. (2010), Security Challenges in Cloud Computing, *Security and Management, 2010*, 36-42
Samenvatting: Cloud Computing is momenteel een van de grootste modewoorden in de computerwereld. Het benoemt het delen van middelen op het gebied van software, platform en infrastructuur door middel van virtualisatie. Virtualisatie is de kerntechnologie achter het delen van IT-middelen in de cloud. De omgeving streeft ernaar om dynamisch, betrouwbaar en aanpasbaar te zijn met een gegarandeerde kwaliteit van de dienstverlening. Beveiliging is een even groot risico in de cloud als in andere omgevingen. Er zijn veel verschillende meningen over cloud computing, waarbij sommigen geloven dat het onveilig is om gebruik te maken van een cloud. Dit artikel onderzoekt enkele grote veiligheidsproblemen met cloud computing en de bestaande tegenmaatregelen voor de veiligheidsuitdagingen in de wereld van cloud computing.

Hilley, D. (2009), *Cloud Computing: A taxonomy of Platform and Infrastructure-level Offerings*, Techical Reports GIT-CERCS-09-13, 2009, Georgia Institute of Technology
Samenvatting: Cloud computing is een modewoord en overkoepelende term die toegepast wordt op de verschillende trends in het turbulente landschap van de informatietechnologie. Computing in de "cloud" zinspeelt op alomtegenwoordige en onuitputtelijke op afroep beschikbare IT-bronnen die toegankelijk zijn via het internet. Vrijwel elke nieuwe op internet gebaseerde service heeft het label "cloud". Ondanks de interesse in cloud computing hebben factoren, zoals onduidelijke terminologie, niet-bestaand producten en opportunistische marketing, ertoe geleid dat er een aanzienlijk gebrek aan duidelijkheid is over cloud computing technologieën en -producten.

Aanbieders noch potentiële consumenten weten hoe het cloud computing productaanbod eruit zou moeten zien en welke categorieën van producten geschikt zijn. Producten zijn niet gestandaardiseerd en dus ook niet eenvoudig vergelijkbaar. De reikwijdte van de verschillende productaanbiedingen verschillen en overlappen op ingewikkelde manieren.

Het doel van deze studie is het creëren van een gedetailleerd overzicht van de verschillende aanbiedingen inclusief classificatie en de overeenkomsten en verschillen te verduidelijken langs verschillende productdimensies. Verduidelijking van de relatie van de verschillende cloud computing producten zal zowel consumenten als dienstverleners helpen om hun huidige en geplande toekomstige aanbod te beoordelen in het licht van de gewenste eigenschappen en de markt positioneren.

Jansen, W. (2011), *Gloud Hooks: Security and Privacy Issues in Cloud Computing*, System Sciences (HICSS), 44th Hawaii International Conference, http://www.hicss.hawaii.edu/hicss_44/bp44/st1.pdf

Samenvatting: In dit artikel worden de belangrijkste issues geïdentificeerd, waarvan wordt verondersteld dat ze langdurig van invloed zijn op cloud computing. Het gaat in op de veiligheids- en privacyonderwerpen die relevant zijn voor cloud computing, omdat ze betrekking hebben op het uitbesteden van de organisatorische IT-omgeving. Zorgpunten worden benoemd voor public clouds, die extra aandacht nodig en die de noodzakelijke achtergrond inzichtelijk maken die nodig is voor het maken van goedonderbouwde beveiligingsbesluiten.

Jansen, W. & Grance, T. (2011), *Guidelines on Security and Privacy in Public Cloud Computing*. NIST, Draft Special Publication 800-144

Samenvatting: Cloud computing betekent verschillende dingen voor verschillende mensen. De gemeenschappelijke kenmerken zijn op afroep beschikbaar en schaalbaarheid van betrouwbare IT-middelen met hoge beschikbaarheid, overal veilige toegang tot diensten en opslag van data buiten de organisatie. Terwijl de aspecten van deze kenmerken tot op zekere hoogte zijn gerealiseerd, blijft cloud computing in ontwikkeling. Deze publicatie geeft een overzicht van de aandachtspunten op het gebied van veiligheid en privacy, die relevant zijn voor de public cloud omgeving. En wijst op keuzes die organisaties moeten maken bij het uitbesteden van data, applicaties en infrastructuur aan een public cloud omgeving.

Khajeh-Hosseini, A., Sommerville, I. & Sriram, I. (2010), Research Challenges for Enterprise Cloud Computing,*1st ACM Symposium on Cloud Computing (SOCC 2010)*, http://arxiv.org/abs/1001.3257

Samenvatting: Cloud computing betekent een verschuiving van een product dat wordt gekocht, naar een dienst die aan consumenten wordt geleverd via het internet door grootschalige datacenters of clouds. Dit paper bespreekt een aantal uitdagingen voor cloud computing vanuit een onderneming of organisatorisch oogpunt en zet ze in de context door ze te vergelijken met de bestaande literatuur. Aan bod komen de organisatorische veranderingen als gevolg van cloud computing, de economische en organisatorische gevolgen van het facturatiemodel, de veiligheid en juridische en privacykwesties met betrekking tot cloud computing. Het is belangrijk om deze punten te belichten, omdat cloud computing niet alleen betrekking heeft op technologische verbetering van de datacenters, maar tevens een fundamentele verandering met zich meebrengt in de manier waarop IT van middelen wordt voorzien en deze middelen gebruikt.

Kim, W. (2009), Cloud Computing: Today and Tomorrow, *Journal of Object Technology*, *8*(1), 65-72

Samenvatting: In de afgelopen jaren is cloud computing uitgegroeid tot een belangrijke IT mode woord, ondanks dat de definitie van cloud computing nog steeds niet helder is. Cloud computing staat in de kinderschoenen voor wat betreft marktadoptie. Het is echter een belangrijke IT-trend, waarvan verwacht wordt dat deze zal beklijven. Dit artikel bespreekt de definitie, de status en adoptiekwesties. Tevens biedt het een glimp van de toekomst en bespreekt technische problemen die naar verwachting worden aangepakt.

Mahmood, Z. (2011), Data Location and Security Issues in Cloud Computing, *International Conference on Emerging Intelligent Data and Web Technologies (2011),* DOI: 10.1109/EIDWT.2011.16

Samenvatting: Cloud computing is een generieke term voor het leveren van services op het internet op basis van pay-as-you-go. Cloud computing biedt veel voordelen voor organisaties, maar er zijn ook aandachtspunten, zoals bij iedere nieuwe technologie. Eén van de belangrijkste aandachtspunten is gerelateerd aan beveiliging en betrouwbaarheid van data in relatie tot opslaglocatie, verplaatsen en beschikbaarheid. Dit artikel geeft kort een overzicht van cloud computing en zijn delivery en deployment modellen. Daarnaast wordt er in detail stil gestaan bij de aandachtspunten in relatie tot data in de cloud. Het doel is om belangrijke achtergrond informatie te geven voor organisaties die een migratie voorbereiden naar de cloud.

Mell, P., Grance, T. (2011), The NIST Definition of Cloud Computing (Draft), National Institute of Standards and Technology U.S. Department of Commerce, http://www.nist.gov/itl/cloud/

Samenvatting: Deze presentatie geeft inzicht in de NIST definitie voor cloud computing. Daarnaast worden de bijbehorende service & deployment modellen besproken. Hierbij wordt aandacht geschonken aan beveiligingsissues en standaarden voor de verschillende modellen.
In het tweede deel van de presentatie wordt gekeken naar het aanbod van cloud computing in de markt op basis van onder andere casestudies.

Mirzaei, N. (2008), *Cloud Computing*, Indiana University, http://grids.ucs.indiana.edu/ptliupages/publications/ReportNarimanMirzaeiJan09.pdf
Samenvatting: Cloud computing, een relatief recente term, definieert de paden in de IT-wereld. Hierbij wordt gebruik gemaakt van alle recente prestaties op het gebied van virtualisatie, distributed computing, utility computing en netwerken.
Het impliceert een service georiënteerde architectuur door middel van het aanbieden van software en platforms als diensten, lagere IT-overhead voor de eindgebruiker, grotere flexibiliteit, lagere total cost of ownership, op afroep beschikbare diensten en vele andere dingen. Dit document is een kort onderzoek op basis van literatuur over cloud computing. Daarnaast wordt geprobeerd om gerelateerde onderzoeksonderwerpen, uitdagingen en mogelijke toepassingen te benoemen.

Oriol Fitó, J. & Guitart, J. (2010), *Introducing Risk Management into Cloud Computing*, Computer Architecture Department, Technical University of Catalonia, Tech. Rep. UPC-DAC-RR-2010-33, http://gsi.ac.upc.edu/apps/reports/2010/33/cnsm10.pdf
Samenvatting: Het cloud computing paradigma biedt een innovatieve en veelbelovende visie op IT. Het verandert de manier waarop hardware en software worden ontworpen en ontwikkeld. Daar staat tegenover dat het gebruik van cloud middelen, wat meestal externe middelen zijn, risico's met zich mee brengt waar aandacht aan dient te worden geschonken. In dit artikel wordt een cloud computing risico management oplossing op basis van Business Level Objects (BLO) besproken voor een bestaande cloud organisatie. Daarbij wordt een semi-kwantitatieve risico beoordeling op basis van deze BLO's uitgevoerd als subproces in het hele risico management proces. In een use case wordt de procedure toegepast op een organisatie.

Overbeek, P., Lindgreen, E. & Spruit, M, (2005), *Informatiebeveiliging onder controle* (2de ed.). Amsterdam, Pearson Education Benelux.
Samenvatting: We kunnen niet meer zonder Informatietechnologie (IT). We gebruiken IT om zaken te doen, ondernemingen te besturen en te communiceren met de wereld om ons heen. Informatiesystemen vormen het zenuwstelsel van onze economie. Ze zorgen ervoor dat we razendsnel kunnen reageren op veranderende omstandigheden en dat we scherp aanvoelen wat de markt van ons verlangt.

Daardoor kunnen we optimaal profiteren van de kansen die de nieuwe economie ons biedt. Zonder informatiesystemen zouden de meeste organisaties niet meer functioneren. Echter, de technologie is kwetsbaar en de risico's zijn talrijk. 'Informatiebeveiliging onder controle' stelt het inrichten van informatiebeveiliging als een beheerst proces centraal. Aan de orde komen managementgerelateerde onderwerpen als beveiligingsbeleid, risicoanalyse en juridische aspecten en certificering. Ook de menselijke factor en techniek komen aan de orde. Speciale aandacht daarbij wordt geschonken aan moderne technieken op het gebied van cryptografie en netwerkbeveiliging.

Ramgovind, S., Eloff, M. & Smith, E. (2010), The Management of Security in Cloud Computing, *Information Security for South Asia (ISSA)*, 1-7, http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/27_Paper.pdf

Samenvatting: Cloud computing heeft nieuwe IT-grenzen gesteld door het aanbieden van dataopslag en flexibel schaalbare rekencapaciteit, waarbij de investeringen verminderen. In plaats van investeringen dienen er wel kosten gemaakt te worden voor het effectief beheren van de toepassingen en de beveiliging van de omgeving. Dit artikel heeft tot doel om de aandacht te vestigen op de veiligheidsproblemen die ontstaan in de nieuwe omgeving en de mogelijkheden van cloud computing zichtbaar te maken.

Sotto, L., Treacy, B. & McLellan, M. (2010), Privacy and Data Security Risks in Cloud Computing, *Electronic Commerce & Law Report,* 15 ECLR(186).

Samenvatting: In de afgelopen jaren is cloud computing naar voren gekomen als een van de snelst groeiende segmenten van de IT-industrie. De mogelijkheid om gebruik te maken van schaalvoordelen, de geografische distributie, open source software en geautomatiseerde systemen om kosten te verlagen maakt van cloud computergebruik een aantrekkelijke optie voor bedrijven. Maar veel van de voordelen van cloud computing worden begeleid door juridische en reputatierisico's. Dit artikel schetst de wettelijke voorschriften van zowel de Verenigde Staten als de Europese Unie met betrekking tot gegevens die zijn opgeslagen door de cloud providers. Teven worden een aantal risico's belicht die verbonden zijn aan het gebruik van cloud computing.

Subashini, S. & Kavitha, V. (2010), A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,*34(1), 1-11 DOI: 10.1016/j.jnca.2010.07.006

Samenvatting: Cloud computing is een manier om de capaciteit te verhogen of dynamisch mogelijkheden toevoegen zonder te investeren in nieuwe infrastructuur, opleiden van nieuwe medewerkers of licenties voor nieuwe software. In de afgelopen jaren is cloud computing uitgegroeid van een veelbelovend business concept naar één van de snelst groeiende segmenten in de IT industrie.

Maar naarmate er meer informatie over personen en bedrijven in de cloud worden geplaatst, nemen de zorgen de veiligheid van de omgeving toe. Ondanks alle hype rond de cloud zijn zakelijke klanten nog steeds terughoudend om hun bedrijf (gedeeltelijk) te verplaatsen naar de cloud. Beveiliging is een van de belangrijkste kwesties die de groei van cloud computing beperkt en complicaties met data privacy en de bescherming van gegevens blijven de markt tergen. De architectuur van de cloud vormt een bedreiging voor de veiligheid van de bestaande technologieën wanneer deze worden ingezet in een cloud omgeving. Afnemers van cloud diensten moeten waakzaam zijn in het begrijpen van de risico's van datalekkage in deze nieuwe omgeving.

In dit artikel is een overzicht gepresenteerd van de verschillende beveiligingsrisico's die een bedreiging voor de cloud vormen. Dit paper is een onderzoek gericht op de verschillende beveiligingsproblemen die voorkomen door de aard van de service delivery modellen van cloud computing systemen.

Tabaki, H., Joshi, J. & Ahn, G. (2010a), SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Enviroments, *IEEE 34th Annual Computer Software and Applications Conference Workshops*, IEEE CS Press, 393-398, DOI 10.1109/COMPSACW.2010.74

Samenvatting: Ondanks dat cloud computing nog in de kinderschoenen staat, heeft het de potentie om aanzienlijke kostenreductie en efficiency te creëren. Hoewel beveiligingsvraagstukken de adoptie vertragen, is het belangrijk om hier toch bij stil te staan. In dit artikel wordt een uitgebreid beveiligingskader voor cloud computing omgevingen besproken. Hierbij wordt aandacht geschonken aan mogelijkheden, bestaande oplossingen, inzichten en acties die nodig zijn om een betrouwbare omgeving te bieden.

Tabaki, H., Joshi, J., Ahn, G. (2010b), Security and Privacy Challenges in Cloud Computing Enviroments, *IEEE Security and Privacy*, 8, 24-31, http://ldc.usb.ve/~figueira/cursos/Seguridad/Material/W_SP_SecurityPrivacyChallenges.pdf

Samenvatting: Cloud computing kan naast kostenoptimalisatie en hogere efficiëntie ook bijdragen aan betere samenwerking, behendigheid en schaalbaarheid waardoor wereldwijd computergebruik mogelijk wordt gemaakt. Indien echter te weinig aandacht wordt besteed aan de juiste beveiligingsmaatregelen en privacyoplossingen kan deze ontwikkeling volledig mislukken. Beveiliging en privacy zijn dan ook de eerste belemmeringen voor adoptie. In dit artikel worden unieke aspecten benoemd die hierop van invloed zijn. Daarnaast worden ook verschillende benaderingen voor deze uitdagingen besproken en wordt aangegeven wat er nog moet gebeuren om een betrouwbare omgeving aan te kunnen bieden.

Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H. & Kanai, A. (2011), Risk Management on the Security Problem in Cloud Computing, *Computers, Networks, Systems and Industrial Engineering (CNSI)*, 2011, 147-152, DOI: 10.1109/CNSI.2011.82

Samenvatting: Diverse studies zijn uitgevoerd met betrekking tot cloud computing. Deze studies zijn voornamelijk gericht op de dienstenkant, waarbij het beveiligingsoogpunt slechts beperkt aan bod is gekomen. In dit artikel worden de verschillende risico's onderzocht vanuit afnemersoogpunt. De risico's zijn bepaald op basis van een Risico Breakdown Structuur. Hierna zijn deze risico's geanalyseerd en geëvalueerd. Gedetailleerde tegenmaatregelen en voorstellen zijn bepaald op basis van de resultaten.

Zhang, X., Wuwong, N., Li, H. & Zhang, X. (2010), Information Security Risk Management Framework for the Cloud Computing Environments, *Computer and Information Technology (CIT)*, 2010, 1328-1334

Samenvatting: De veiligheidsrisico's die met de verschillende delivery modellen worden geassocieerd variëren en zijn afhankelijk van verschillende factoren, waaronder gevoeligheid van de informatie, architecturen en beveiliging. Na verloop van tijd zijn organisaties geneigd om de beveiliging te laten versoepelen. Om dit te voorkomen dienen er regelmatig risicoanalyses te worden uitgevoerd. In dit artikel wordt een risico management kader gegeven voor inzicht in de kritieke gebieden. Zichtbaar wordt waar de focus moet liggen. Tevens worden bedreigingen en kwetsbaarheden geïdentificeerd. Dit kader is geschikt voor alle service en delivery modellen binnen de cloud omgevingen en kan door organisaties gebruikt worden voor risicobeperkende inzichten.

Bijlage 2 Risicomanagement modellen

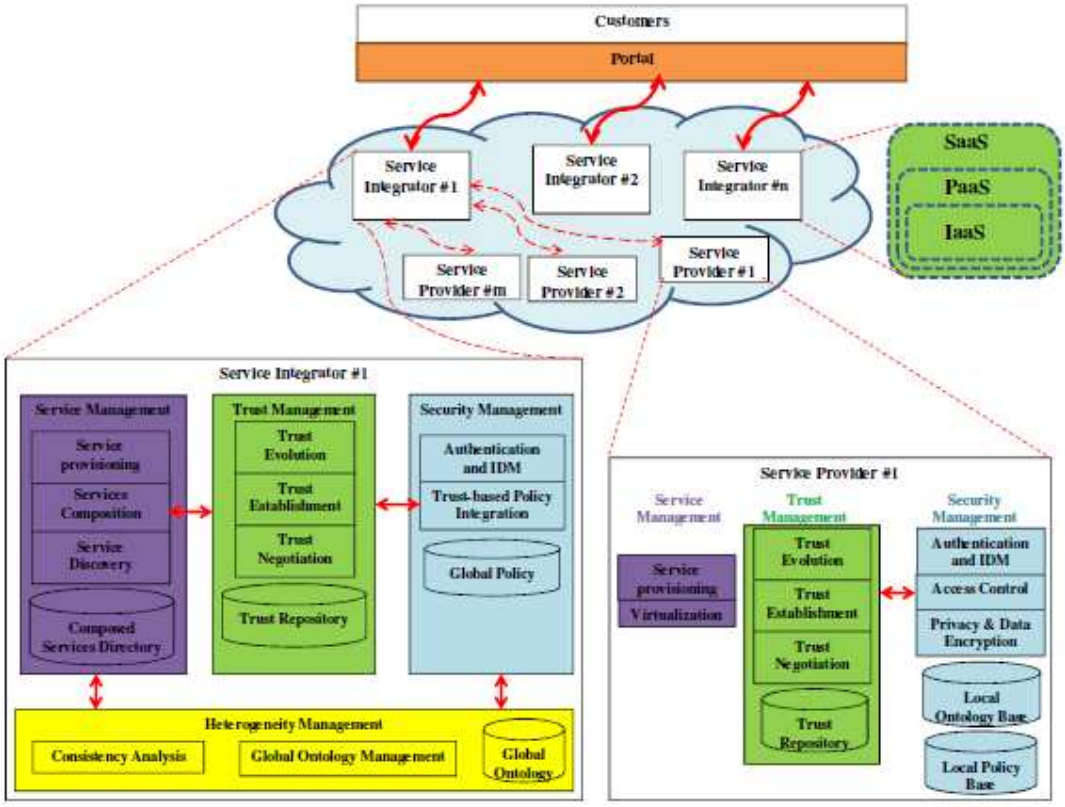
In paragraaf 4.2 zijn vier risicomanagement modellen besproken. Hieronder worden deze modellen visueel weergegeven.

$Risk_i$	Probability (P_i)	Impact		$RLE_i(B_i)$	Action(s)	Consequences		$RLE_p(B_i)$
		Benefit	Threat			Benefit	Threat	
Under-provisioning	Frequent	0	Very High	Critical	Transfer	Very high	0	High profit.
Over-provisioning	Frequent	0	Medium	Critical	Transfer	Very high	0	High profit.
Accept new Cloud Service	Likely	High	Low	Profitable	Accept / Avoid	Very high	0	High profit.
SLA violations	Likely	Very low	Medium	Unacceptable	Reduce / Avoid	0	Very low	Negligible
Service disruptions	Possible	0	Medium	Unacceptable	Reduce / Avoid	0	Very low	Negligible
Performance loss	Possible	0	Medium	Unacceptable	Reduce / Avoid	0	Very low	Negligible
Outsourcing hidden costs	Unlikely	0	High	Unacceptable	Avoid	0	Very low	Negligible
VM isolation	Very unlikely	0	High	Negligible	Accept	0	High	Negligible
Virt. performance overhead	Very unlikely	0	High	Negligible	Accept	0	High	Negligible
Data integrity loss	Very unlikely	0	Medium	Negligible	Accept	0	Medium	Negligible
Destruction of data	Very unlikely	0	Medium	Negligible	Accept	0	Medium	Negligible
Loss of governance	Very unlikely	0	Medium	Negligible	Accept	0	Medium	Negligible
Power loss of IT systems	Very unlikely	0	Very low	Negligible	Accept	0	Very low	Negligible
Natural disasters, fire, etc.	Very unlikely	0	Very low	Negligible	Accept	0	Very low	Negligible

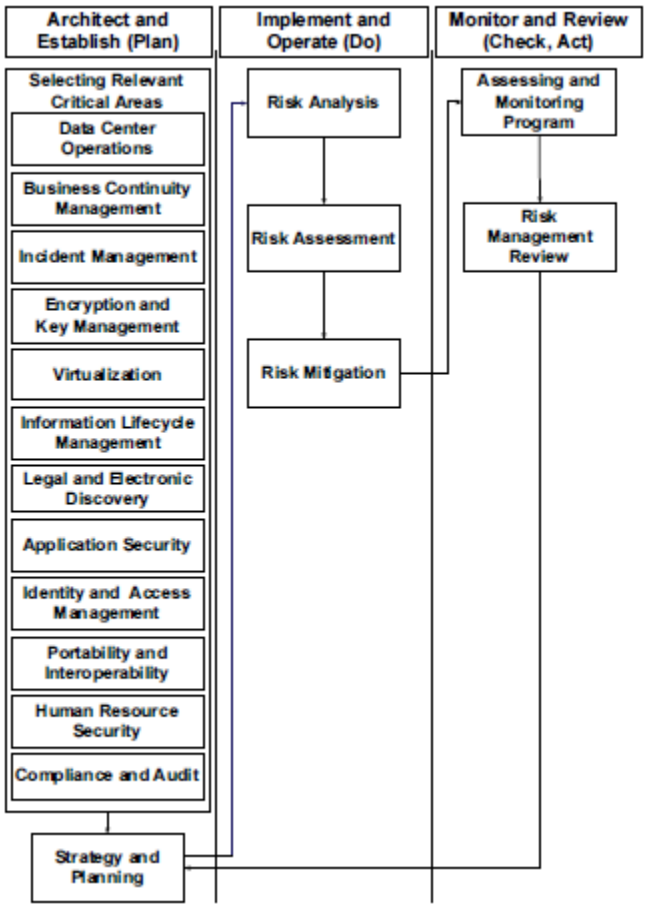
Figuur 7: Risicomanagement op basis van Business Level Objectives met als subproces semi-kwantitatieve BLO-gedreven cloud risico-assessment
(Oriol Fitó & Guitart, 2009)

Level 1: Major division	Level 2: Middle division	Level 3: Risks
1. Risks for Company Introducing Cloud Computing	1.1 System	1.1.1 Problem of Cooperation with Existing System
		1.1.2 Problem of Removing Data when Finishing Use of Cloud Service
		1.1.3 Problem of Unique Specification of Service Provider
		1.1.4 Problem with Supervisor of Service Provider
		1.1.5 Problem of Service Provider Leaking, Altering, and Wrongly Using Data
		1.1.6 Problem of Data Being Deleted After Cloud Service Use
	1.2 Operation	1.2.1 Problem of Regulatory Non-compliance by Service Provider
		1.2.2 Problem of Service Provider Limiting Information Disclosure
		1.2.3 Problem of Requirements for Authentication
		1.2.4 Problem of Managing Confidential Information
		1.2.5 Bad Influence when Data of Other Company Using the Same Service are Seized
	1.3 Facility	1.3.1 Problem of Environmental Impact, Such as Carbon-dioxide Emissions

Figuur 8: Risico Breakdown Structure
(Tanimoto, Hiramoto, Iwashita, Sato & Kanai, 2011)



Figuur 9: Beveiligingsframework voor cloud computing omgeving (Tabaki, Joshi & Ahn, 2010a)



Figuur 10: Informatiebeveiliging risicomanagement framework (Zhang, Wuwong, Li & Zhang, 2010)

Bijlage 3 Vragenlijst onderzoek

De onderstaande vragenlijst is voorgelegd aan de respondenten.

Geachte heer/mevrouw,

In het kader van mijn masterscriptie aan de Open Universiteit doe ik onderzoek naar de risico's voor cloud afnemers bij het gebruik van een cloud omgeving. Hiervoor is een korte vragenlijst opgesteld met vragen over de belangrijkste organisatorische en juridische risico's die u(w organisatie) onderkent bij het gebruik van cloud computing. Tevens ben ik geïnteresseerd in de classificatie die u(w organisatie) aan deze risico's heeft toegewezen en welke maatregelen en acties helpen bij het verminderen en vermijden van de risico's.

Graag nodig ik u uit om deze vragenlijst in te vullen. De vragenlijst bevat 20 vragen en vraagt maximaal 10 minuten van uw tijd. Uit privacyoogpunt is ervoor gekozen om de vragenlijst zodanig op te stellen dat er geen cookie wordt geïnstalleerd. Hierdoor is het echter niet mogelijk om op een later tijdstip de vragenlijst af te maken. Alle antwoorden worden zeer vertrouwelijk behandeld en anoniem in mijn scriptie verwerkt. Alle verwijzingen naar organisaties, specifieke methoden of personen worden in algemene verwoordingen verwerkt.

Als dank voor uw hulp stuur ik u graag mijn masterscriptie toe na afronding van mijn studie. Aan het eind van de vragenlijst kunt u aangeven of u hier interesse in heeft.

U kunt de vragenlijst starten door op de knop "verder" te drukken.

Ter verduidelijking volgt hier eerst de definitie van cloud computing. Hiervoor wordt de definitie van Enisa gehanteerd:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort of service provider interaction.

Vraag 1: Welke methodiek voor risicomanagement gebruikt uw organisatie? Kunt u deze kort omschrijven?
Dit is een open vraag waardoor meer inzicht wordt verkregen in de verschillende methodieken en mogelijke overeenkomsten

Vraag 2: Welke risico's zijn in uw organisatie onderkend als belangrijkste organisatorische risico's?
Dit is een meerkeuzevraag waarbij de respondent er maximaal 10 mag selecteren of invullen. De eerste zes opties zijn reeds genoemd vanuit de literatuurstudie. Naast deze zes zijn er nog tien vrije invulvelden.

Vraag 3: Kunt u per risico aangeven welke risicoclassificatie deze heeft in uw organisatie?
Hierbij kan de respondent per gekozen risico uit vraag 2 aangeven of de classificatie accepteren, vermijden, verminderen of verzekeren is.

Vraag 4: U heeft onderstaande risico's geclassificeerd met verminderen. Kunt u aangeven welke maatregelen u hiervoor inzet.
Op basis van de antwoorden uit vraag 2 en 3 kan per risico de maatregelen worden genoemd.

Vraag 5: De classificatie "vermijden" heeft u toebedeeld aan onderstaande risico's. Kunt u aangeven welke acties u hiertoe onderneemt?
Op basis van de antwoorden uit vraag 2 en 3 kunnen acties per risico worden aangegeven.

Vraag 6: Hieronder heeft u de ruimte om nog extra opmerkingen te plaatsen naar aanleiding van de vragen die u zojuist zijn gesteld.
Dit is een open invoerveld welke niet verplicht is om in te vullen.

Vraag 7: Wat zijn de belangrijkste juridische risico's die uw organisatie heeft geïdentificeerd in relatie tot cloud computing.
Dit is een meerkeuzevraag waarbij de respondent er maximaal 10 mag selecteren of invullen. De eerste vijf opties zijn reeds genoemd vanuit de literatuurstudie. Naast deze zes zijn er nog tien vrije invulvelden.

Vraag 8: Kunt u per risico aangeven welke classificatie uw organisatie hieraan heeft toegekend?
Hierbij kan de respondent per gekozen risico uit vraag 7 aangeven of de classificatie accepteren, vermijden, verminderen of verzekeren is.

Vraag 9: U heeft onderstaande risico's aangegeven dat u deze wil verminderen. Kunt u aangeven welke maatregelen u hiervoor inzet?
Op basis van de antwoorden uit vraag 7 en 8 kan per risico de maatregelen worden genoemd.

Vraag 10: De classificatie "vermijden" heeft u toebedeeld aan onderstaande juridische risico's. Kunt u aangeven welke acties hiervoor ondernomen worden?
Op basis van de antwoorden uit vraag 7 en 8 kunnen acties per risico worden aangegeven.

Vraag 11: Hieronder heeft u de ruimte om nog extra opmerkingen te plaatsen naar aanleiding van de vragen die u zojuist zijn gesteld.
Dit is een open invoerveld welke niet verplicht is om in te vullen.

Hartelijk dank voor het invullen van de inhoudelijke vragenlijst. Hierna volgen nog enkele vragen over de organisatie en de functie waarin u werkzaam bent.

Vraag 12: Is het hoofdkantoor van uw organisatie in Nederland of in het buitenland gevestigd?
De respondent heeft de keus om te kiezen voor 1 antwoord. Indien wordt gekozen voor buitenland, dient aan te worden gegeven in welk land.

Vraag 13: Wat is de core business van uw organisatie?
Dit is een open vraag. De uitkomst kan keuzes in classificatie verder verklaren.

Vraag 14: In welke branche bent u werkzaam?
De respondent heeft de keuze uit een aantal branches.

Vraag 15: Wat is uw functie?
Deze open vraag geeft inzicht in de achtergrond van de respondent.

Vraag 16: Voor hoeveel % van de IT-voorziening maakt uw organisatie gebruik van een cloud-omgeving? Maakt u eventueel een schatting.
Het percentage kan worden aangegeven op een schaal van 0 tot 100%.

Vraag 17: Tot slot zou ik nog graag willen weten op welke manier u de vragenlijst heeft ontvangen.
Hierbij zijn de drie onderzoeksdoelgroepen benoemd alsmede een invoeroptie.

Vraag 18: Indien u graag het eindrapport van dit onderzoek wilt ontvangen, kunt u dit hieronder aangeven.
Aangegeven kan worden of er interesse is en als dit het geval is, kan het e-mailadres worden achtergelaten.

Hartelijk dank voor de moeite die u heeft genomen om de vragenlijst volledig in te vullen. Indien u heeft aangegeven mijn scriptie te willen ontvangen, zal deze, na het afronden van mijn studie, naar u worden toegezonden.

U kunt nu het venster sluiten.

Met vriendelijke groet
Yvonne van Boxmeer

Bijlage 4 Onderzoeksresultaten

In deze bijlage worden samenvattingen van de ruwe onderzoeksresultaten getoond. per respondent. In hoofdstuk 4 wordt deze data besproken per risico.

Bijlage 4a Relatie tussen risico, classificatie en branche

Organisatorische risico's

Risico	**Classificatie**	**Aantal respondenten**	**Branches**
Leveranciers lock-in	Accepteren	12	Horeca (1) Informatie/communicatie (2) Openbaar bestuur/Overheid (1) Zakelijke dienstverlening (3) Overig (1) Onbekend (4)
	Vermijden	11	Financiële dienstverlening (2) Gezondheids/welzijnszorg (1) Groot/detailhandel (1) Industrie (1) Openbaar bestuur/Overheid (1) Zakelijke dienstverlening (2) Onbekend (3)
	Verminderen	9	Financiële dienstverlening (1) Industrie (1) Informatie/Communicatie (1) Openbaar bestuur/Overheid (3) Overige dienstverlening (1) Zakelijke dienstverlening (1) Onbekend (1)
	Verzekeren	1	Zakelijke dienstverlening (1)
Data lock-in	Accepteren	3	Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (2)
	Vermijden	11	Bouwnijverheid (1) Financiële dienstverlening (1) Gezondheids- en welzijnszorg (1) Industrie (2) Informatie / Communicatie (1) Openbaar bestuur / Overheid (2) Overig (1) Onbekend (2)

Risico	Classificatie	Aantal respondenten	Branches
	Verminderen	8	Financiële dienstverlening (3) Horeca (1) Openbaar bestuur / Overheid (1) Onbekend (3)
	Verzekeren	1	Industrie (1)
Governance niet goed geregeld	Accepteren	2	Bouwnijverheid (1) Zakelijke dienstverlening (1)
	Vermijden	8	Financiële dienstverlening (1) Industrie (1) Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (2) Onbekend (3)
	Verminderen	17	Financiële dienstverlening (3) Gezondheids- en welzijnszorg (2) Informatie / Communicatie (2) Openbaar bestuur / Overheid (6) Onbekend (4)
	Verzekeren	1	Industrie (1)
Imagoschade door toedoen van andere bedrijven	Accepteren	3	Financiële dienstverlening (1) Informatie / Communicatie (1) Onbekend (1)
	Vermijden	13	Bouwnijverheid (1) Industrie (2) Informatie / Communicatie (2) Openbaar bestuur / Overheid (4) Overige dienstverlening (1) Zakelijke dienstverlening (1) Onbekend (2)
	Verminderen	11	Financiële dienstverlening (1) Informatie / Communicatie (1) Openbaar bestuur / Overheid (3) Overige dienstverlening (1) Zakelijke dienstverlening (2) Onbekend (3)
	Verzekeren	4	Financiële dienstverlening (1) Informatie / Communicatie (1) Zakelijke dienstverlening (1) Onbekend (1)

Risico	Classificatie	Aantal respondenten	Branches
Cloud leverancier stopt met leveren van diensten	Accepteren	4	Gezondheids- en welzijnszorg (2) Informatie / Communicatie (1) Zakelijke dienstverlening (1)
	Vermijden	8	Horeca (1) Industrie (1) Informatie / Communicatie (2) Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (1) Onbekend (2)
	Verminderen	10	Financiële dienstverlening (4) Informatie / Communicatie (2) Zakelijke dienstverlening (2) Overig (1) Onbekend (1)
	Verzekeren	4	Zakelijke dienstverlening (1) Onbekend (3)
Onbekendheid met nieuwe omgeving	Accepteren	9	Informatie / Communicatie (2) Openbaar bestuur / Overheid (2) Zakelijke dienstverlening (2) Onbekend (3)
	Vermijden	3	Industrie (1) Informatie / Communicatie (1) Zakelijke dienstverlening (1)
	Verminderen	10	Bouwnijverheid (1) Financiële dienstverlening (1) Gezondheids- en welzijnszorg (2) Openbaar bestuur / Overheid (3) Overig (1) Onbekend (2)
	Verzekeren	1	Informatie / Communicatie (1)

Juridische risico's

Risico	Classificatie	Aantal respondenten	Branches
Inbeslagname van data	Accepteren	1	Bouwnijverheid (1)

Risico	Classificatie	Aantal respondenten	Branches
	Vermijden	11	Financiële dienstverlening (2) Industrie (1) Informatie / Communicatie (2) Openbaar bestuur / Overheid (2) Zakelijke dienstverlening (3) Overig (1)
	Verminderen	2	Informatie / Communicatie (1) Openbaar bestuur / Overheid (1)
	Verzekeren	0	
Documentatie niet (tijdig) beschikbaar voor onderzoeken	Accepteren	4	Zakelijke dienstverlening (4)
	Vermijden	8	Financiële dienstverlening (1) Horeca (1) Industrie (1) Openbaar bestuur / Overheid (5)
	Verminderen	6	Bouwnijverheid (1) Financiële dienstverlening (2) Informatie / Communicatie (1) Openbaar bestuur / Overheid (1) Overig (1)
	Verzekeren	0	
Beperkingen door wet- en regelgeving	Accepteren	6	Bouwnijverheid (1) Informatie / Communicatie (2) Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (2)
	Vermijden	10	Financiële dienstverlening (2) Gezondheids- en welzijnszorg (1) Industrie (1) Openbaar bestuur / Overheid (4) Zakelijke dienstverlening (2)
	Verminderen	2	Informatie / Communicatie (1) Openbaar bestuur / Overheid (1)
	Verzekeren	1	Industrie (1)
Privacy van data is niet voldoende geborgd	Accepteren	4	Informatie / Communicatie (2) Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (1)

Risico	Classificatie	Aantal respondenten	Branches
	Vermijden	22	Financiële dienstverlening (4) Gezondheids- en welzijnszorg (1) Groot- en detailhandel (1) Industrie (2) Informatie / Communicatie (1) Openbaar bestuur / Overheid (8) Overige dienstverlening (1) Zakelijke dienstverlening (3) Overig (1)
	Verminderen	7	Bouwnijverheid (1) Gezondheids- en welzijnszorg (1) Informatie / Communicatie (1) Openbaar bestuur / Overheid (1) Zakelijke dienstverlening (2) Overig (1)
	Verzekeren	4	Industrie (1) Zakelijke dienstverlening (2) Onbekend (1)
Onvoldoende inzicht in naleving van de regels	Accepteren	4	Informatie / Communicatie (1) Zakelijke dienstverlening (3)
	Vermijden	9	Financiële dienstverlening (2) Industrie (1) Openbaar bestuur / Overheid (5) Zakelijke dienstverlening (1)
	Verminderen	5	Bouwnijverheid (1) Gezondheids- en welzijnszorg (1) Informatie / Communicatie (1) Openbaar bestuur / Overheid (2)
	Verzekeren	2	Openbaar bestuur / Overheid (1) Overig (1)

Bijlage 4b Relatie tussen risico, classificatie en doelgroep

Organisatorische risico's

Risico	Classificatie	Aantal respondenten	Doelgroep
Leveranciers lock-in	Accepteren	12	PvIB (3) CSA-N (1) CCN (1) ZN (3) Onbekend (4)
	Vermijden	11	PvIB (4) CSA-N (1) ZN (3) Onbekend (3)
	Verminderen	9	PvIB (2) ZN (6) Onbekend (1)
	Verzekeren	1	ZN (1)
Data lock-in	Accepteren	3	PvIB (2) ZN (1)
	Vermijden	11	PvIB (3) CCN (2) ZN (4) Onbekend (2)
	Verminderen	8	PvIB (2) CSA-N (2) ZN (1) Onbekend (3)
	Verzekeren	1	PvIB (1)
Governance niet goed geregeld	Accepteren	2	PvIB (1) ZN (1)
	Vermijden	8	PvIB (3) ZN (2) Onbekend (3)
	Verminderen	17	PvIB (4) CSA-N (1) ZN (8) Onbekend (4)
	Verzekeren	1	PvIB (1)

Risico	Classificatie	Aantal respondenten	Doelgroep
Imagoschade door toedoen van andere bedrijven	Accepteren	3	PvIB (1) ZN (1) Onbekend (1)
	Vermijden	13	PvIB (3) CCN (2) ZN (6) Onbekend (2)
	Verminderen	11	PvIB (2) ZN (6) Onbekend (3)
	Verzekeren	4	CSA-N (1) ZN (2) Onbekend (1)
Cloud leverancier stopt met leveren van diensten	Accepteren	4	PvIB (1) ZN (3)
	Vermijden	8	PvIB (1) CSA-N (1) ZN (4) Onbekend (2)
	Verminderen	10	PvIB (3) CSA-N (1) CCN (1) ZN (4) Onbekend (1)
	Verzekeren	4	PvIB (1) Onbekend (3)
Onbekendheid met nieuwe omgeving	Accepteren	9	PvIB (3) CCN (2) ZN (1) Onbekend (3)
	Vermijden	3	PvIB (1) ZN (2)
	Verminderen	10	PvIB (2) ZN (6) Onbekend (2)
	Verzekeren	1	ZN (1)

Juridische risico's

Risico	Classificatie	Aantal respondenten	Doelgroep
Inbeslagname van data	Accepteren	1	PvIB (1)
	Vermijden	11	PvIB (5) CCN (1) ZN (5)
	Verminderen	2	PvIB (1) ZN (1)
	Verzekeren	0	
Documentatie niet (tijdig) beschikbaar voor onderzoeken	Accepteren	4	PvIB (3) ZN (1)
	Vermijden	8	PvIB (3) CSA-N (1) ZN (4)
	Verminderen	6	PvIB (3) CSA-N (1) ZN (2)
	Verzekeren	0	
Beperkingen door wet- en regelgeving	Accepteren	6	PvIB (3) CCN (1) ZN (2)
	Vermijden	10	PvIB (5) ZN (5)
	Verminderen	2	ZN (2)
	Verzekeren	1	PvIB (1)
Privacy van data is niet voldoende geborgd	Accepteren	4	PvIB (1) ZN (3)
	Vermijden	22	PvIB (8) CSA-N (1) CCN (1) ZN (12)
	Verminderen	7	PvIB (3) CCN (1) ZN (3)

Risico	Classificatie	Aantal respondenten	Doelgroep
	Verzekeren	4	PvIB (2) ZN (1) Onbekend (1)
Onvoldoende inzicht in naleving van de regels	Accepteren	4	PvIB (1) ZN (3)
	Vermijden	9	PvIB (5) CCN (1) ZN (3)
	Verminderen	5	PvIB (2) CCN (1) ZN (2)
	Verzekeren	2	ZN (2)

Bijlage 5 Relatie tussen aantal respondenten, doelgroep en branche

Doelgroep	Aantal respondenten	Branches
Platform voor Informatie Beveiliging (PvIB)	15	Bouwnijverheid (1) Financiële dienstverlening (3) Industrie (2) Openbaar bestuur / Overheid (5) Zakelijke dienstverlening (4)
Cloud Security Alliance – Nederland (CSA-N)	2	Financiële dienstverlening (1) Horeca (1)
Cloud computing Nederland (CCN)	3	Informatie / Communicatie (2) Openbaar bestuur / Overheid (1)
Zakelijk netwerk	30	Gezondheids- en welzijnszorg (2) Groot- en detailhandel (1) Industrie (1) Informatie / Communicatie (6) Openbaar bestuur / Overheid (9) Overige dienstverlening (2) Zakelijke dienstverlening (7) Overig (2)
Onbekend	13	Onbekend