ACHMEA

Afstudeeronderzoek

Cloud Risk Assessment

Brinkhuis, S.W. (Stephan)
19-3-2018

Informatiepagina

Naam:	Stephan Willem Brinkhuis
Hogeschool:	Saxion University of Applied Sciences
Opleiding:	Security Management
Klas:	ASE5VA
Studentnummer:	354401
E-mail:	stephanbrinkhuis@outlook.com
Tel:	0657300895

Organisatie:	Achmea
Locatie:	Zeist Handelsweg 2
Praktijkcoach:	Willem van der Valk
E-mail	Willem.van.der.valk@achmea.nl
Tel.:	0653462182

1ste lezer:	René van den Nieuwenhoff
Opleiding:	Security Management
Locatie:	Apeldoorn
E-mail:	r.p.m.l.c.vandennieuwenhoff@saxion.nl
Tel.:	0629595194

2de lezer:	Marcel Paschedag
Opleiding:	Security Management
Locatie:	Apeldoorn
E-mail:	m.paschedag@saxion.nl

Inhoud

Begrippenlijst

Uitbestedingen
Het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf (art. 1:1 Wet financieel toezicht) (Nederlandse Encyclopedie 2017).

Cloud Risk Assessment
Om op een gestructureerde wijze inzicht te krijgen in de mogelijkheden en risico's van Cloud. Tevens geeft het risicoprofiel van de organisatie de wet- en regelgeving weer waaraan moet worden voldaan (Pinkelephant, 2017a).

Software As A Service (SAAS)
Het aanbieden en gebruiken van software via internet. Klanten betalen de software in een abonnementsvorm naar gebruik in plaats van het eenmalig kopen van software (Janssen, 2008).

BIV classificatie
BIV is een afkorting voor: Beschikbaarheid, Integriteit en Vertrouwelijkheid. De BIV helpt bij het classificeren van bepaalde bedrijfsprocessen of gegevens.

Efficiënt (doelmatig werken)
Sneller en zoveel mogelijk resultaat, met zo min mogelijk geld en of tijd.

Primaire bedrijfsprocessen
Achmea kent verschillende bedrijfsprocessen. Deze processen worden onderverdeeld in kritische bedrijfsprocessen en niet kritisch. Een kritisch bedrijfsproces is alles wat van invloed is op verzekerings- en herverzekeringsprocessen, bancaire dienstverlening en vermogens-beheer. Voorbeelden van niet kritische bedrijfsprocessen zijn bijvoorbeeld de loonadministratie of niet voldoende parkeergelegenheid (Kampen, 2017).

Enterprise Security Architect
Is iemand die informatiebeveiliging in brede zin aanpakt. Dit word gedaan door middel van het structureren van bedrijfsprocessen, beveiligingsprocessen en het personeel van een organisatie (Blokdyk, 2017).

Operational Risk Manager
Is verantwoordelijk voor interne gebeurtenissen, falende processen waardoor fouten ontstaan, frauderende werknemers, of het niet voldoen aan geldende wet- en regelgeving (Tijhaar, 2013).

1. Inleiding

Samen het risico dragen als iemand schade heeft. Zo begon het in Achlum (Friesland) in het jaar 1811. Ulbe Piers Draisma wilde het bezit van 39 boeren en notabelen verzekeren tegen brand. In ruim twee honderd jaar is Achmea gefuseerd met andere verzekeraars die de coöperatieve achtergrond delen (zie bijlage 1: Huidige merken van Achmea) (Achmea, 2017a).

De hulp bij het omgaan met risico's (bijvoorbeeld: wonen en werken) is een belangrijke behoefte van mensen. De manier waarop deze hulp moet worden geboden blijft zich echter ontwikkelen. Het ontwikkelt zich van 'schade vergoeden en voorkomen' naar 'mensen helpen om iets te behouden of te bereiken' (Achmeanet, 2017a). Naast de ontwikkelingen in de markt, ontwikkelt Achmea zich tot een verzekeraar die steeds digitaler is ingesteld. Als gevolg van de Achmea strategie wordt er meer samengewerkt met partners en externe partin, waarbij een toename van het aantal uitbestedingen en het gebruik van Cloud zichtbaar is (W. van der Valk, persoonlijke communicatie, 12 september 2017). Deze vernieuwingen gaan niet automatisch. Vernieuwen vergt mentaliteit en een houding om voorop te willen lopen en altijd naar betere oplossingen te zoeken (Achmeanet, 2017b).

Achmea is een organisatie van ongeveer 12.000 medewerkers in Nederland en 2500 in het buitenland bij dochterondernemingen. Er zijn negen verschillende vestigingen in Nederland, namelijk: Zeist, Amsterdam, Leeuwarden, Tilburg, Apeldoorn, De Meern, Leiden, Leusden en Zwolle.

Dit onderzoek richt zich op het onderwerp Cloud. Het begrip Cloud kent geen eenduidige definitie (Faber, 2017). Gedurende dit onderzoek zal er gebruik gemaakt worden van de definitie zoals die staat beschreven in de National Institute of Standards and Technology (NIST).

> Cloud Computing is een model voor het snel beschikbaar stellen van on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen (zoals netwerken, servers, opslag, applicaties en diensten), met een minimum aan management inspanning of interactie met de aanbieder. Dit cloudmodel legt de nadruk op beschikbaarheid en is samengesteld uit vijf essentiële kenmerken (zie hoofdstuk .2.2), drie delivery modellen (diensten) (zie hoofdstuk 2.3.1) en vier toepassingsmodellen (zie hoofdstuk 2.3.2 Cloud) (Pinkelephant, 2017a).

Het onderzoek wordt vanuit een Global Information Security Officer rol (GISO) uitgevoerd. De GISO maakt onderdeel uit van de afdeling Risk & Compliance in Zeist (zie bijlage 2: Organogram). Deze afdeling bestaat uit vier medewerkers die zich richten op het schrijven en up-to-date houden van het informatiebeveiligingsbeleid. Ook geven medewerkers van de GISO afdeling prioritering en een beoordeling aan risico's op het gebied van Cybersecurity en Business Continuity (Achmeanet, 2017b).

1.1 Aanleiding

Technologische ontwikkelingen maken het mogelijk om te blijven innoveren (Achmeanet, 2017). Deze innovaties doet Achmea met verschillende soorten partners. Denk hierbij aan startups, technologische bedrijven en kennisinstituten (Achmeanet, 2017b). Dit brengt tegelijkertijd nieuwe risico's met zich mee (Van der Valk, 2017). Een voorbeeld van een nieuw risico is ransomware[1]. Ransomware werkt door het sturen van e-mails naar willekeurige personen. Deze e-mails bevatten een link waarop geklikt moet worden, om bijvoorbeeld het account van de Hema te bevestigen. Achter de e-mail zit echter een crimineel die de computer overneemt en geld eist van de gebruiker als die zijn bestanden terug wil.

De doelstelling van Achmea is om met toonaangevende oplossingen dagelijks relevant voor klanten te zijn (Achmeanet, 2017). Om dit te kunnen realiseren, wordt door Achmea steeds meer gebruik gemaakt van Cloud (Van der Valk, 2017). Cloud zorgt voor dataverwerking via het internet. Waar vroeger applicaties en software op een fysieke computer of server in het gebouw moesten worden gedownload, is er nu toegang tot dezelfde soort toepassingen via het internet (Salesforce, 2017). Voordelen hiervan zijn de flexibiliteit, betere samenwerking en geen investeringen in de hardware (Salesforce, 2017). Echter, het werken in de Cloud resulteert in nieuwe (type) risico's (Van der Valk, 2017). Een voorbeeld van een nieuw type risico is het zeggenschapsrisico. Bij zeggenschap wordt er ingegaan op de mate waarin iemand toegang heeft tot bestanden en in hoeverre een organisatie vastzit aan een leverancier. Het risico van het vastzitten aan één leverancier is dat de organisatie die de dienst afneemt, geen invloed kan uitoefenen op de wijze waarop de dienst beveiligd wordt (Accountant, 2014).

De aanleiding voor dit onderzoek is dat steeds meer Cloud uitbestedingen worden gerealiseerd bij Achmea. Bij iedere Cloud uitbesteding wordt het gehele Cloud Risk Assessment uitgevoerd (zie hoofdstuk 2.5) (Van der Valk, 2017). Een gevolg van het uitvoeren van het gehele Cloud Risk Assessment is dat er veel tijd verloren gaat aan het identificeren van Cloud risico's, terwijl sommige Cloud risico's (uit het Cloud Risk Assessment) in mindere mate relevant kunnen zijn. Het kan ook voor komen dat Cloud risico's bij een uitbesteding van toepassing zijn, waarover onvoldoende informatie bekend is om het te kunnen mitigeren. De ervaring leert dat Cloud risico's bij de gecategoriseerde uitbestedingen (zie hoofdstuk 4.1) kunnen verschillen. Om deze reden wil Achmea een onderzoek laten uitvoeren naar de verschillende soorten uitbestedingen met bijbehorende Cloud risico's.

Door Achmea worden regelmatig Software As A Service (SAAS) uitbestedingen gerealiseerd (zie hoofdstuk 2.5). De SAAS is een Clouddienst die alle zorgen over beheer en de complete werkplek wegneemt (zie hoofdstuk 2.5) ongeacht de mate van kritiekheid van een bedrijfsproces. Deze mate van kritiekheid wordt gemeten op basis van de BIV classificatie (zie hoofdstuk 2.10). In de huidige situatie wordt door Achmea bij iedere uitbesteding het gehele Cloud Risk Assessment uitgevoerd (Van der Valk, 2017). Het gevolg hiervan kan zijn dat het realiseren van een SAAS uitbesteding efficiënter en/ of effectiever kan, omdat bijvoorbeeld bepaalde Cloud risico's minder relevant zijn.

[1] Ransomware: een gijzeling van de computer. De computer wordt geblokkeerd en je kunt er niks meer mee. Het is malware (schadelijke software) waarmee criminelen proberen om je 'losgeld' te betalen om er vanaf te komen (Vraaghetdepolitie.nl, 2017).

De vraag is: hoe kunnen de verschillende SAAS uitbestedingen worden afgestemd op het Cloud Risk Assessment, zodat deze zo efficiënt en/ of effectief mogelijk kunnen worden uitgevoerd?

1.2 Doelstelling onderzoek

Het doel van dit onderzoek is om aanbevelingen te doen aan de GISO afdeling van Achmea voor het afstemmen van verschillende SAAS uitbestedingen op het Cloud Risk Assessment, door de verschillende soorten uitbestedingen met bijbehorende Cloudrisico's vanuit de SAAS in kaart te brengen en deze af te stemmen op het Cloud Risk Assessment.
(Kernbegrippen zijn: SAAS uitbestedingen en Cloud Risk Assessment)

De reden dat ervoor is gekozen om het Cloud Risk Assessment af te stemmen op een SAAS uitbesteding, is omdat Achmea relatief veel SAAS uitbestedingen heeft waarbij er een oplossing moet komen om het Cloud Risk Assessment efficiënter en/of effectiever uit te voeren (Van der Valk, 2017). Een voorbeeld van een uitbesteding vanuit de SAAS die niet bedrijfskritisch is, kan loonadministratie zijn. Achmea kan bij het niet operationeel zijn van de loonadministratie nog steeds de primaire bedrijfsprocessen blijven uitvoeren.

1.2.1 Doelstelling beroepsproduct

Het beroepsproduct is een verslaglegging van de verschillende soorten SAAS uitbestedingen. Tevens worden er aanbevelingen gedaan over hoe en of het mogelijk is, om het Cloud Risk Assessment af te stemmen op bepaalde uitbestedingen die een SAAS component bevatten.

1.3 Probleemstelling

De hoofdvraag voor dit onderzoek is:
In hoeverre is er een categorisering aangebracht in de verschillende soorten uitbestedingen die Achmea kent en in hoeverre kan het Cloud Risk Assessment worden afgestemd op een uitbesteding die vanuit de SAAS Clouddienst wordt uitgevoerd?

1.3.1 Onderzoeksvragen

Onderzoeksvraag 1:
Welke uitbestedingen vanuit de SAAS zijn bekend binnen Achmea en op welke wijze verschillen deze van elkaar?
Toelichting
Onderzoeksvraag één is gericht op het verzamelen van informatie over de verschillende soorten uitbestedingen die Achmea onderkent en de verschillen tussen de uitbestedingen. Op het moment dat er verschillen zijn tussen de soorten uitbestedingen, kan hierin een categorisering worden aangebracht.

Onderzoeksvraag 2:
Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?
Toelichting
Onderzoeksvraag twee is gericht op het verzamelen van informatie over de structuur die het Cloud Risk Assessment hanteert. Naast de structuur wordt bij deze onderzoeksvraag onderzocht wat voor Cloud risico's het Assessment moet identificeren volgens de wet- en regelgeving en de norm die Achmea hanteert. Met de kennis op welke wijze het Cloud Risk Assessment is opgebouwd, kan vanuit de SAAS Clouddienst geanalyseerd worden welke Cloud risico's uit het Cloud Risk Assessment van toepassing zijn voor een bepaalde uitbesteding.

Onderzoeksvraag twee draagt bij aan het in kaart brengen van de wijze waarop het Cloud Risk Assessment is opgebouwd en welke factoren (zie hoofdstuk 2.9) een impact hebben op het Cloud Risk Assessment. Bijvoorbeeld bij een uitbesteding die persoonsgegevens verwerkt, zijn andere factoren van toepassing dan bij een uitbesteding waar computerschermen worden ingekocht.

Onderzoeksvraag 3:
Op welke wijze kan het Cloud Risk Assessment afgestemd worden op uitbestedingen die vanuit een SAAS Clouddienst worden uitgevoerd?
Toelichting
Onderzoeksvraag drie is gericht op het afstemmen van het Cloud Risk Assessment op een bepaalde uitbesteding vanuit de SAAS Clouddienst. Om te weten of het Cloud Risk Assessment afgestemd kan worden, is het belangrijk om te weten welke impact de verschillende factoren op het Cloud Risk Assessment hebben.

1.4 Afbakening

In samenspraak met de opdrachtgever wordt in deze paragraaf een afbakening van het onderzoek beschreven.

- Het uitgangspunt van dit onderzoek is het bestaande Cloud Risk Assessment van de Nederlandsche Bank (zie Bijlage 3 Het Cloud Risk Assessment).
- Het onderzoek zal zich richten op uitbestedingen die vanuit de SAAS worden gerealiseerd, omdat Achmea veel van dit soort uitbestedingen doet.
- Het resultaat van dit onderzoek zal zich beperken tot Cloud Assessments binnen Achmea.
- De aanbevelingen die door de student worden beschreven zullen alleen gaan over uitbestedingen voor de SAAS Clouddienst.
- De aanbevelingen worden beschreven op basis van feitelijke uitspraken door medewerkers van Achmea, wet- en regelgeving (zie hoofdstuk 2.8) en de vastgestelde normen (zie hoofdstuk 2.9).

1.5 Betrokkenen en belanghebbenden

Het onderzoek wordt uitgevoerd vanuit een GISO (Global Information Security Office) rol. De resultaten van dit onderzoek zijn bestemd voor medewerkers bij Achmea die het Cloud Risk Assessment moeten uitvoeren. De betrokkenen en belanghebbenden die te maken krijgen met het Cloud Risk Assessment worden in deze paragraaf beschreven.

1.5.1 Betrokkenen

De betrokkenen in dit onderzoek zijn:

- De Group Information Security Officer (GISO) als praktijkbegeleider

De GISO is werkzaam als manager van de GISO afdeling en is verantwoordelijk voor informatiebeveiliging en IT Risk Management. Tevens geeft de GISO adviezen op het gebied van IT risico's. Het belang bij dit onderzoek voor de GISO is om te analyseren welke ontwikkelingen Achmea doormaakt op het gebied van Cloud en welke effecten dit heeft op het informatiebeveiligingsbeleid.

- Enterprise Security Architect (ESA)

De ESA heeft het Cloudbeleid voor Achmea geschreven In de loop van dit jaar (2018) zal een vervolg komen op het beleid met daarin nieuwe doelstellingen en wet- en regelgeving. Het belang van de ESA bij dit onderzoek is de samenhang die kan worden gevonden tussen de verschillende typen Cloud, met de daaraan gekoppelde uitbestedingen. Met deze samenhang kunnen nieuwe inzichten ontstaan op het gebied van de privacy en security in een Cloud omgeving.

- Operational Risk Manager (ORM)

ORM houdt zich bezig met het uitbestedingsbeleid. In dit beleid wordt bepaald wat wel een uitbesteding is en wat niet. Het belang bij dit onderzoek voor de ORM is om te analyseren of het uitbestedingsbeleid moet worden aangepast, of dat er iets moet veranderen in de onderhandelingen met betrekking tot uitbestedingen.

1.5.2 Belanghebbenden

De belanghebbenden bij dit onderzoek zijn:

- Achmea (merken)

Het belang voor Achmea bij dit onderzoek is te analyseren welke Cloud ontwikkelingen er plaatsvinden en hoe het Cloud Risk Assessment moet worden afgestemd op een bepaalde uitbesteding vanuit de SAAS.

- De Nederlandsche Bank (DNB)

DNB heeft 44 Cloud risico's (zie bijlage 3 Het Cloud Risk Assessment) beschreven, die moeten worden gemitigeerd door Achmea op het gebied van Cloud. Op het moment dat uit dit onderzoek naar voren komt dat er nieuwe Cloud risico's zijn (door huidige ontwikkelingen) of Cloud risico's die zijn verouderd, moet dit worden gerapporteerd aan DNB.

1.6 Relevantie van het onderzoek

Het is voor Achmea belangrijk om te weten of het Cloud Risk Assessment kan worden afgestemd op specifieke kenmerken van uitbestedingen. Het belang hiervan is dat het tijdsbesparing kan opleveren bij het uitvoeren van het Cloud Risk Assessment, maar ook dat er bij een bepaalde uitbesteding meer aandacht kan worden besteed aan relevante Cloud risico's.

1.7 Leeswijzer

Deze scriptie gaat over de wijze waarop het Cloud Risk Assessment afgestemd kan worden op een SAAS uitbesteding. In hoofdstuk twee wordt het theoretisch kader beschreven. In dit hoofdstuk worden de relevante theorieën over SAAS uitbestedingen en het Cloud Risk Assessment beschreven. De methodologische verantwoording voor dit onderzoek wordt in hoofdstuk drie beschreven. Dit hoofdstuk geeft antwoord op de wijze waarop de onderzoeksvragen van dit onderzoek methodologisch worden verantwoord. In het vierde hoofdstuk worden de analyses beschreven van de verschillende interviews en documentaties die zijn gebruikt. Na de analyses in hoofdstuk vier, worden in hoofdstuk vijf de conclusies en de aanbevelingen op basis van de analyses beschreven. Tot slot wordt in hoofdstuk zes beschreven wat er eventueel aan vervolgonderzoek kan worden gedaan.

2. Theoretisch kader

In hoofdstuk één is de context van het onderzoek beschreven, die de basis vormt van de theoretische uitwerking in dit hoofdstuk. In dit hoofdstuk wordt beschreven wat Cloud is en welke kenmerken het heeft. Vervolgens wordt de relatie tussen de kernbegrippen die staan beschreven in de doelstelling van dit onderzoek (zie Hoofdstuk 1.2) uitgewerkt in een globaal conceptueel model (zie hoofdstuk 2.3). Het model wordt vervolgens in dit hoofdstuk vanuit de theorie per kernbegrip beschreven.

Het beschrijven van een theoretisch kader draagt bij aan de benodigde informatie om de probleemstelling en onderzoeksvragen te beantwoorden. Tevens heeft het theoretisch kader een positieve invloed op de betrouwbaarheid en validiteit van het onderzoek.

2.1 Wat is Cloud?

Het verwerken van informatie is aan het veranderen. Waar eerst gebruik werd gemaakt van de traditionele IT[2], is nu het gebruik van Cloud in opkomst. Bij het gebruik van Cloud wordt er gebruik gemaakt van internetverbindingen met daaraan gekoppelde internetsystemen die staan opgeslagen in een datacenter. Het datacenter kan zich overal ter wereld bevinden (Nobel, 2015).

Zoals beschreven in de inleiding, is er geen eenduidige definitie voor het woord Cloud en zal (voor dit onderzoek) de definitie van de NIST worden gebruikt. Er is voor de definitie van NIST gekozen, omdat de NIST kort en bondig beschrijft wat Cloud is en waar het uit bestaat.

> Cloud Computing is een model voor het snel beschikbaar stellen van on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen (zoals netwerken, servers, opslag, applicaties en diensten), met een minimum aan management inspanning of interactie met de aanbieder. Dit cloudmodel legt de nadruk op beschikbaarheid en is samengesteld uit vijf essentiële kenmerken (zie hoofdstuk 2.2), drie delivery modellen (diensten) (zie hoofdstuk 2.3.1) en vier toepassingsmodellen (zie hoofdstuk 2.3.2) (Nobel, 2015).

2.1.1 Het begrijpen van Cloud

Cloud bestaat uit drie lagen namelijk uit de applicaties waarmee wordt gewerkt, het platform dat wordt gebruikt om in te werken en de IT-infrastructuur (zie afbeelding1). Iedere laag bestaat, zoals beschreven in afbeelding één, uit een aantal componenten, namelijk:

De bedrijfsapplicaties:

- Portaal (bijvoorbeeld BlackBoard)
- Bedrijfsapplicaties (een app voor werktijden)

[2] Traditionele IT: Organisaties hebben een aangelegde (fysieke) infrastructuur met een datacenter binnen de organisatie (WINXX ICT, 2017).

Het platform:

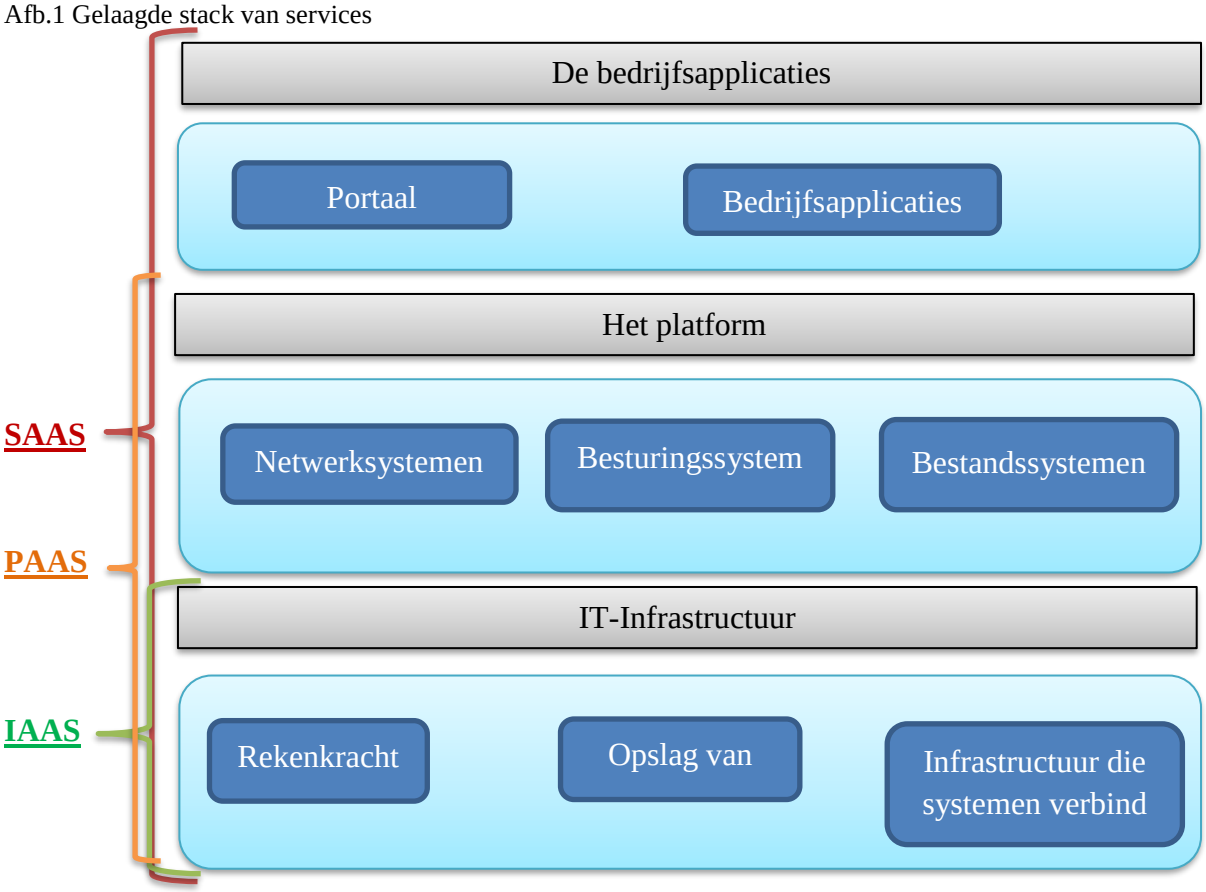
- Netwerksystemen: een centrale computer die ervoor zorgt dat individueel gebruik van computersystemen voor organisaties mogelijk is (Pelckmans, 2014).
    - LAN (Local Area Network) is een lokaal netwerk binnen een gebouw. Denk hierbij aan een thuisnetwerk of schoolnetwerk.
    - WAN (Wide Area Network) is een wereldwijd netwerk waarin geen beperking is tussen de afstand van computers.
- Besturingssystemen (Van der Toolen & Wang, 2017) zijn programma's die na het opstarten van de computer, in het geheugen worden geladen. Denk hierbij aan Windows, IOS of Linux.
- Bestandssystemen zijn systemen waarin data op een harde schijf zijn georganiseerd (Computable, 2017).

De IT-infrastructuur:

- Rekenkracht (levering van de service)
- Opslag van data
- Infrastructuur die de systemen onderling en met de gebruikers verbindt

Door middel van deze lagen wordt een virtuele omgeving gecreëerd waarbij gebruikers vanuit iedere plaats en op elk moment applicaties kunnen gebruiken en bij de data kunnen komen.

Afb.1 Gelaagde stack van services



Bij groei van de organisatie die gebruik maakt van traditionele IT, moet er extra dataopslag gehuurd of gekocht worden op de vraag van het aantal gebruikers. Mocht het aantal gebruikers of de vraag na een drukke periode dalen, dan heeft de organisatie een dataopslag waar niks mee wordt gedaan. Cloud zorgt voor extra IT capaciteit wanneer de organisatie het nodig heeft. Op het moment dat de organisatie het niet meer nodig heeft, kan de dataopslag worden teruggegeven aan de Cloudprovider (Van Hoof, 2017). Het nadeel van Cloud is dat de organisatie niet alles in eigen beheer heeft. Om dit te kunnen ondervangen, wordt onderscheid gemaakt tussen verschillende typen Clouds (zie hoofdstuk 2.3).

2.2 Kenmerken van Cloud

Er wordt gesproken over Cloud als het voldoet aan een vijftal kenmerken. Deze kenmerken zijn (Van Hoof, 2017):

- **On demand service:**

Een afnemer kan op ieder willekeurig moment zelf servertijd, verwerkingscapaciteit, opslagcapaciteit en netwerkcapaciteit aanvragen zonder menselijke interactie met de aanbieder (Van Hoof, 2017).

- **Toegang via netwerk**

De computerfaciliteiten zijn via het netwerk toegankelijk en kunnen benaderd worden via standaard mechanismen waardoor een diversiteit aan toegangsapparatuur gebruikt kan worden, zoals cliënt platformen (bijvoorbeeld PC, mobiele telefoons, laptops en PDA's) (Van Hoof, 2017).

- **Gedeeld gebruik van middelen (resource pooling)**

De gebruikte fysieke IT-middelen worden via virtualisatie gedeeld over vele afnemers door middel van een multi-tenant[3] model en dynamisch gealloceerd geheugen[4] (Van Hoof, 2017).
Bij het gebruik van gedeelde middelen bestaat er een mate van locatie onafhankelijkheid zodat een afnemer geen controle heeft over of kennis van de exacte locatie van de voorzieningen. Echter, op het niveau van land of staat kan de afnemer in staat worden gesteld keuzes te maken in verband met wettelijke beperkingen (Van Hoof, 2017).

- **Hoge mate van elasticiteit**

IT-middelen kunnen snel (minuten, uren) en flexibel (tijdvensters, capaciteit) beschikbaar worden gesteld en kunnen naar behoefte worden opgeschaald en weer terug geschaald. Hierdoor lijken de voorzieningen een onbeperkte capaciteit te hebben zodat de afnemer dynamisch op ieder moment over iedere gewenste capaciteit kan beschikken (Van Hoof, 2017).

- **Measured services**

Cloud systemen beheren de middelen automatisch voor optimaal gebruik. Het gebruik van de middelen wordt voor de afnemer transparant inzichtelijk gemaakt op het niveau van het type dienst (bijvoorbeeld inzicht in tijd, opslag, verwerkingscapaciteit, bandbreedte en actieve gebruikersaccounts) (Van Hoof, 2017).

[3] Multi-tenant: de software draait op een server. Meerdere klanten maken gebruik van dezelfde toepassing en delen één enkele database (Unit4, z.d.).
[4] Dynamisch gealloceerd geheugen: dit is geheugen voor objecten zonder dat expliciet door het programma wordt aangevraagd en weer wordt vrijgegeven als het niet meer nodig is (Stroustrup, 2017).

2.3 Cloud types

Om te kunnen analyseren met wat voor soort Cloud risico's Achmea te maken krijgt bij een bepaalde uitbesteding vanuit de SAAS, is het belangrijk om te weten wat SAAS is en in welk opzicht deze verschilt met overige Cloud types. In deze paragraaf wordt een onderscheid gemaakt tussen Clouddiensten en Cloud toepassingsmodellen.

2.3.1 Clouddiensten

Als een organisatie bedrijfsprocessen wil laten uitvoeren door gespecialiseerde bedrijven, dan kan uit drie verschillende soorten (platformen) diensten gekozen worden, namelijk: Infrastructure As A Service (IAAS), Platform As A Service (PAAS) en Software As A Service (SAAS). Deze diensten bepalen de mate waarin een organisatie de verantwoordelijkheden en controle bij de leverancier neerlegt (Bazuin, 2016). Zoals beschreven in de aanleiding, zal dit onderzoek zich richten op de SAAS Clouddienst.

Infrastructure As A Service (IAAS)

IAAS is een minimale laag van outsourcing. Deze optie is geschikt als de organisatie zelf de omgeving beheert, maar niet de fysieke (zoals hardware, verbindingen en het datacenter) inkoop doet. De organisatie blijft in eigen beheer van 'de managementlaag, de software en alle applicaties', maar regelt niet zelf de fysieke infrastructuur (Bazuin, 2016). In afbeelding 1 wordt weergegeven welk beheer over een proces wordt uitbesteed aan de Cloud leverancier.

Platform As A Service (PAAS)

Met de PAAS ligt er meer controle bij de leverancier van de Clouddienst dan bij IAAS. De leverancier regelt namelijk naast de IAAS ook alles wat te maken heeft met het besturingssysteem (denk hierbij bijvoorbeeld aan Windows). De organisatie behoudt het beheer over de eigen data en ontwikkeling van applicaties (Bazuin, 2016). Het voordeel van de PAAS is dat de provider zorgt voor het Operational System en zorgt dat alles up-to-date is. Dit betekent dat de organisatie direct een omgeving heeft om applicaties in te ontwikkelen en te testen. In afbeelding 1 wordt weergegeven welke processen bij een PAAS worden uitbesteed aan de Cloud leverancier.

Software As A Service (SAAS)

SAAS is een dienst die alle zorgen over beheer en de complete werkplek wegneemt. Het beheer van de servers, netwerk, opslag en applicaties wordt door de Cloud leverancier verzorgd. Een reden voor een organisatie om gebruik te maken van deze dienst, is om zich volledig te kunnen richten op de eigen processen (zie hoofdstuk 2.4) (Bazuin, 2016). In afbeelding 1 weergegeven welk beheer over een proces wordt uitbesteed aan de Cloud leverancier.

2.3.2 Cloud toepassingsmodellen

Er zijn verschillende soorten Cloud toepassingsmodellen te onderscheiden namelijk: Private Cloud, Public Cloud, Hybrid Cloud en Community Cloud (deitauditor, 2017). Ieder Cloud toepassingsmodel heeft zijn voor- en nadelen. In deze paragraaf worden de verschillende soorten Cloud toepassingsmodellen beschreven.

Private Cloud:
Een Private Cloud is een Cloud infrastructuur die uitsluitend wordt geëxploiteerd voor bijvoorbeeld Achmea. Een private Cloud kan worden beheerd door een derde partij of door Achmea zelf. Beide partijen kunnen eigenaar van de middelen zijn (Van Hoof, 2017).

Voordelen:
Bij een Private Cloud liggen de controle en ontwikkeling van cloudapplicaties volledig bij de organisatie, met als voordeel dat er met de eigen ICT-omgeving gewerkt kan worden. Private Cloud biedt de mogelijkheid om bestaande applicaties te gebruiken, waardoor derde partijen in de Cloudomgeving kunnen werken. Naast de applicaties kiest de organisatie zelf de hardware met de bijbehorende capaciteit.

Bij een Private Cloud bepaalt de organisatie wanneer backups[5] worden gemaakt. Bij het maken van backups is het vanuit veiligheidsoverwegingen belangrijk om dit op twee verschillende locaties te realiseren (Cloudscanner, 2017). Dit wordt ook wel een Dual Data Center genoemd. Het hebben van een Dual Data Center kan ervoor zorgen dat er bij uitval taken kunnen worden overgenomen, waardoor bedrijfsprocessen niet worden onderbroken (Cloudscanner, 2017).

Tot slot heeft de Private Cloud als voordeel dat de organisatie zelf bepaalt wie toegang verkrijgt tot gegevens. Dit kan worden beheerd door een autorisatiebeleid op te stellen (Cloudscanner, 2017).

Nadelen:
Als een organisatie kiest voor een Private Cloud, dan moeten er veel investeringen worden gedaan. Denk hierbij aan de hardware die snel kan verouderen en gevoelig is voor storingen en uitval. Het gevolg hiervan is dat de hardware om de zoveel tijd vervangen moet worden. Tevens kost het onderhoud van de servers en applicaties veel tijd, geld en energie (Cloudscanner, 2017).

Public Cloud
Bij een Public Cloud maakt de organisatie gebruik van de technische infrastructuur van een aanbieder. Dit betekent dat de organisatie betaalt om de diensten via het internet te gebruiken. De aanbieders van de Public Cloud hebben de beschikking over een eigen serverpark en daar worden de online applicaties (waar organisaties gebruik van maken) op gedraaid (Cloudscanner, 2017).

[5] Backups: een kopie van gegevens die zich op een gegevensdrager of binnen een applicatie bevinden (Cloudshape, 2017)).

Voordelen:
Bij een Public Cloud hoeft een organisatie niet de eigen hardware aan te schaffen of online applicaties te ontwikkelen. Omdat publieke Clouddiensten vaak veel gebruikers hebben, zijn de kinderziektes al uit de online applicatie gehaald, waardoor de organisatie weinig tot geen last heeft van storingen of andere soorten fouten (Cloudscanner, 2017).

Publieke Clouddiensten richten zich vooral op grote groepen gebruikers, waardoor aanbieders profiteren van schaalvoordelen. Het gevolg voor de gebruikers is dan dat de prijzen zullen dalen voor een bepaalde dienst. Ook is het voordeel bij een online aanbieder dat als de gebruiker te weinig capaciteit heeft, deze binnen een paar minuten kan worden uitgebreid.

Nadelen:
Een van de belangrijkste nadelen van Public Cloud voor een organisatie is dat er geen volledige controle is over de eigen bedrijfsdata. Ook is het voor de organisatie moeilijk te achterhalen waar de bedrijfsdata zijn opgeslagen (Cloudscanner, 2017). Naast de opslag van bedrijfsdata, heeft de organisatie weinig tot geen invloed op de beveiliging van de servers waarop de data staan (Cloudscanner, 2017). Hackers zijn wereldwijd actief en zoeken naar zwakke plekken in servers van publieke clouddiensten. Het gevolg voor de organisatie kan zijn dat er een datalek wordt gevonden. Dit kan leiden tot een boete of reputatieschade voor de organisatie (Cloudscanner, 2017).

Bij een Public Cloud maken meerdere organisaties gebruik van dezelfde hardware en processorcapaciteit. Een gevolg hiervan kan zijn dat als meerdere organisaties tegelijkertijd gebruik maken van deze dienst, de snelheid zal afnemen en een verminderende performance kan optreden (Cloudscanner, 2017).

Hybrid Cloud
Een Hybrid Cloud is een combinatie van de Public Cloud en Private Cloud. Afhankelijk van het doel realiseren organisaties een mix van de clouddiensten. Over het algemeen maken organisaties gebruik van Public Clouds die betrekking hebben op algemene kantoorapplicaties. De vertrouwelijke gegevens worden vaak ondergebracht in een Private Cloud (Cloudscanner, 2017). De voor- en de nadelen zijn beschreven onder de koppen Private Cloud en Public Cloud.

Community Cloud
Bij dit toepassingsmodel maken organisaties gebruik van een gedeelde omgeving om informatie en kennis met elkaar uit te kunnen wisselen. De Community Cloud voldoet aan de specifieke eisen die door de deelnemende organisaties worden gesteld (Pinkelephant, 2017b). Denk hierbij aan locatie, beveiliging, beleid, architectuur enz. Het gebruik van dit toepassingsmodel wordt steeds vaker een onderdeel van een Hybrid Cloud (Pinkelephant, 2017b). Voorbeelden van organisaties die een gemeenschappelijk belang hebben zijn: onderwijsorganisaties, onderzoeksorganisaties, overheidsinstellingen en zorginstellingen.

Voordelen:
De Community Cloud kan zowel lokaal als door derde partijen worden geregeld. Een voordeel van Community Cloud is het pay-per-use[6] model (Pinkelephant, 2017b). Wat vooral een groot voordeel is van de Community Cloud is dat het niveau van beveiliging, de privacy, het toezicht en de naleving op beleid worden geassocieerd met die van een Private Cloud (Rouse, 2017).

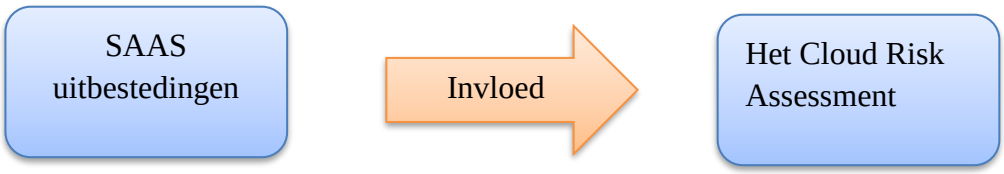
Nadelen:
Het nadeel van een Community Cloud is dat organisaties gezamenlijk de voorwaarden van de dienstverlening bepalen. Dit betekent dat er altijd een mate van afhankelijkheid is met een medegebruiker. Ook moet de samenwerking tussen de verschillende organisaties goed verlopen om tegenstrijdige belangen te voorkomen (Fundaments Cloud Infrastructure, 2017).

2.4 Het globaal conceptueel model

Voordat beschreven kan worden wat de verschillende invloeden van SAAS uitbestedingen op het Cloud Risk Assessment zijn, wordt er dieper ingegaan op de definitie en kenmerken van een SAAS en wat het Cloud Risk Assessment is met bijbehorende wet- en regelgeving, normen en factoren.

Zoals beschreven in de doelstelling van dit onderzoek (zie hoofdstuk 1.2), zijn de kernbegrippen ‘SAAS uitbestedingen’ en ‘Cloud Risk Assessment’. Dit betekent dat het onderzoek zo is opgezet dat er wordt onderzocht wat de invloed van SAAS uitbestedingen is op het Cloud Risk Assessment (zie hoofdstuk 4).

Afbeelding.2: Globaal conceptueel model



2.5 Software As A Service (SAAS)

In paragraaf 2.3.1 Clouddiensten werd beschreven wat voor soort Clouddienst de SAAS is. Omdat Achmea relatief veel SAAS uitbestedingen realiseert en daarbij het gehele Cloud Risk Assessment uitvoert, zal dit onderzoek zich richten op de mogelijkheden om een SAAS uitbesteding af te stemmen op het Cloud Riks Assessment. Om deze reden wordt in deze paragraaf dieper ingegaan op de definitie en de architectuur van de SAAS.

[6] Pay-per-use: een manier van een betalingsstructuur die zo werkt dat de klant toegang heeft tot alle resources, maar alleen betaalt voor wat er daadwerkelijk gebruikt wordt (Rouse, 2017).

2.5.1 SAAS

Er is geen eenduidige definitie van SAAS. De onderstaande definitie is afkomstig van een scriptie van A. Jessurun en N. Mirkovic (Jessurun & Mirkovic, 2017).

Software As A Service is online toegang (ongeacht tijd en locatie) tot een op afstand beheerde applicatie. SAAS staat parallel gebruik toe van eenzelfde applicatie door een groot aantal onafhankelijke gebruikers (klanten), biedt een aantrekkelijke betalingsstructuur vergeleken met de toegevoegde waarde voor de klant en het maakt nieuwe en innovatieve software mogelijk (Jessurun & Mirkovic, 2017).

Omdat er geen eenduidige definitie van het woord SAAS is, worden er een aantal kenmerken beschreven om de SAAS uit te leggen, zoals die gebruikt zal worden tijdens dit onderzoek. Deze kenmerken zijn (Jessurun & Mirkovic, 2017):

- SAAS applicaties zijn webapplicaties. Dit betekent dat er geen software vanuit de klant nodig is om de applicatie te gebruiken.
- Voor SAAS is een internetverbinding vereist.
- SAAS leverancier is de eigenaar en licentiehouder van de SAAS applicatie.
- Een SAAS applicatie wordt beheerd door één leverancier.
- De SAAS leverancier biedt meerdere klanten dezelfde applicatiesoftware, infrastructuur en fysieke database.
- Het betaalmodel is op basis van gebruik (pay per use) of abonnementsstructuur.

De beschreven kenmerken zijn niet alle kenmerken van de SAAS, maar bieden wel een referentiekader voor het begrip.

2.5.2 Architectuur

De basis voor de SAAS is de multi-tenant architectuur. In het multi-tenant model heeft de leverancier alle software en data van klanten op één locatie opgeslagen en kan er via gescheiden kanalen gebruik gemaakt worden van de verschillende soorten softwarefunctionaliteiten en data. De SAAS leverancier heeft alles volledig in eigen beheer en draagt de verantwoordelijkheid voor het aanleveren en transporteren van webdiensten (Jessurun & Mirkovic, 2017).

In het geval dat afnemers de bedrijfsdata verspreid hebben over meerdere SAAS leveranciers en locaties, wordt er gesproken over een multi-vendor model (Jessurun & Mirkovic, 2017). Er is dan geen sprake meer van een één op één relatie, maar van een netwerk met samenwerkende organisaties (Computable, 2017).

2.6 Cloud Risk Assessment

De Nederlandsche Bank (DNB) heeft als initiatiefnemer in Europa ervoor gezorgd dat het wettelijk mogelijk is voor financiële instellingen om te outsourcen in de Cloud (DNB, 2017). De guidance die door DNB is ontwikkeld, bestaat uit onder andere 44 Cloud risico's (Cloud Risk Assessment) die moeten worden gerapporteerd aan DNB (zie bijlage 3 Het Cloud Risk Assessment).

Het Cloud Risk Assessment (zie bijlage 3 Het Cloud Risk Assessment) is een framework om potentiele Cloud risico's bij een uitbesteding te identificeren. Dit framework is gebaseerd op het risicoprofiel van een financiële instelling en de geldende wet- en regelgeving (zie hoofdstuk 2.9) (Hillenaar, 2017). Het doel van het Cloud Risk Assessment voor dit onderzoek is om structuur aan te brengen in het identificeren van potentiële Cloud risico's en het beoordelen van nieuw Cloud aanbieders (Vohradsky, 2017).

Structuur:
Het Cloud Risk Assessment is onderverdeeld in vier risicogebieden namelijk (zie bijlage 3):

- **Operational Risks**

De risico's één tot en met negen van DNB hebben betrekking op het operationeel houden van het bedrijfsproces dat is uitbesteed in een Cloud. Denk bijvoorbeeld aan het risico Lock-in.

- **Technical Risks**

Technische risico's zijn specifieke risico's die kunnen optreden tijdens het uitbesteden van een bedrijfsproces in een Cloud. Een voorbeeld hiervan is een DDOS aanval.

- **Compliance Risks**

Deze risico's zijn gericht op het gebied Compliance, en kunnen van invloed zijn op een Cloud uitbesteding.

- **General Not Cloud Specific Risks**

De risico's die worden beschreven zijn niet specifiek gericht op Cloud. Wel kunnen deze algemene risico's invloed uitoefenen op het gebruik van Cloud.

2.7 Compliance

Zoals beschreven in paragraaf 2.6, helpt het Cloud Risk Assessment bij het identificeren van potentiele Cloud risico's. Omdat uitbestedingen van elkaar kunnen verschillen, zijn er verschillende soorten wet- en regelgevingen (zie hoofdstuk 2.8) en normen (zie hoofdstuk 2.9) van toepassing. Een voorbeeld van twee verschillende soorten uitbestedingen is het uitbesteden van persoonsgegevens en een uitbesteding van hardware. Bij het uitbesteden van persoonsgegevens moet er rekening gehouden worden met de Wet bescherming persoonsgegevens (Wbp). Bij een hardware uitbesteding hoeft er geen rekening gehouden te worden met wetten en normen die te maken hebben met persoonsgegevens. Wel moet rekening worden gehouden met wetten en normen die eisen stellen aan bijvoorbeeld de kwaliteit van hardware.

Omdat er meerdere definities zijn voor het woord 'compliance', is het belangrijk om een definitie zo praktisch mogelijk te vertalen. De meest gebruikte definitie is het toezien op en voldoen aan geldende wet- en regelgeving (De complianceofficer, 2017). Een definitie die bruikbaarder is gaat over de vertaling van wetten en (interne) regels naar de gewenste norm (organisatiegedrag). Bij het uitvoeren van het Cloud Risk Assessment zijn er op het gebied van compliance een aantal wetten en regels waarop men zich kan richten, namelijk (De complianceofficer, 2017):

- Gedragsregels uitgevaardigd door de organisatie zelf.
- Regels ter voorkoming van belangenverstrengeling.
- Bevorderen van compliance gericht gedrag.

2.8 Wet- en regelgeving

Als data of processen worden gemitigeerd naar Cloud, dan kan dit gevolgen hebben voor de mate waarin er wordt voldaan aan de geldende wet- en regelgeving. Dit heeft te maken met het soort uitbesteding dat wordt gerealiseerd (bijvoorbeeld persoonsgegevens of hardware). Bij het gebruik van Cloud, zijn beperkende eisen opgesteld door DNB voor financiële instellingen. Naast de wet- en regelgeving hanteert Achmea een normenkader. De eisen en normen die gehanteerd worden zijn (Faber, 2017):

- Export of opslaan van data
- Eisen gesteld aan beveiligingsmaatregelen
- Eisen in relatie tot compliance en het uitvoeren van audits

De wet- en regelgeving op het gebied van Cloud is onder te verdelen in twee gebieden.
Het eerste gebied stelt eisen voor de beveiliging en controle van data (Faber, 2017). Dit houdt in dat er wordt gestuurd op de mate waarin de organisatie controle heeft over de eigen data. Het tweede gebied is data en persoonsgegevens in de Cloud (Faber, 2017). Dit richt zich op de verwerking van persoonsgegevens (Faber, 2017).

Beveiliging en controle:
Financiële instellingen staan onder toezicht van DNB. Dit is bepaald op grond van de Wet financieel toezicht (Wft) en het Besluit prudentiële regels[7]. Deze wetten moeten ervoor zorgen dat een Cloudprovider voldoet aan de toezichtwetgeving[8] (Faber, 2017).

Vanuit DNB is vastgesteld dat Cloud te vertalen is naar een vorm van uitbesteding. DNB dient te worden geïnformeerd als een organisatie het voornemen heeft om over te gaan op Cloud (Faber, 2017). DNB en Achmea hebben de afspraak dat bij iedere Cloud uitbesteding er minimaal een Cloud Risk Assessment wordt uitgevoerd op basis van de 44 Cloud risico's (Zie bijlage 3 DNB Cloud risico's) (Faber, 2017).

Bij het gebruik van de Cloud is Achmea sterk afhankelijk van de Cloudprovider. Deze afhankelijkheid zorgt voor vragen over de risico's en de mate waarin controle en regie zoveel mogelijk kunnen worden behouden. Vanuit het bedrijfsjuridisch oogpunt van Achmea moeten de volgende vragen worden beantwoord (Faber, 2017):

- Hoe wordt gewaarborgd dat data en software altijd toegankelijk en beschikbaar zijn?
- Hoe kan afdoende beveiliging worden afgedwongen en gecontroleerd?
- Hoe wordt gezorgd dat bij een beëindiging van de overeenkomst een naadloze overgang naar de nieuwe provider plaatsvindt en geen data achterblijven?

Data en persoonsgegevens in de Cloud
Kenmerkend voor de Cloud is dat er vaak gebruik wordt gemaakt van meerdere datacentra en dat data worden opgeslagen op meerdere locaties. In veel gevallen zullen diensten die via de Cloud worden geleverd persoonsgegevens verwerken. Het kan zo zijn dat op die verwerking de Wbp van toepassing is (Faber, 2017).

[7] Besluit prudentiële regels: deze regels zijn van toepassing op vergunning houdende en onder toezicht staande financiële ondernemingen die werkzaam zijn op de financiële markten (DNB, 2017).
[8] Zie de artikelen 27 t/m 32a van het besluit prudentiële regels, die art. 3:18 van de Wet financieel toezicht uitvoert.

Eisen aan doorgifte

De Autoriteit Persoonsgegevens (AP) stelt eisen aan de doorgifte van persoonsgegevens naar landen buiten de EER[9]. In beginsel mogen de persoonsgegevens alleen worden doorgegeven aan landen die een passend beschermingsniveau bieden. De Europese Commissie wijst de landen aan die een passend beschermingsniveau kunnen bieden (Faber, 2017).

Huidige wetgeving

Op iedere verwerking van persoonsgegevens is de Wbp van toepassing. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon (Faber, 2017). Verschillende partijen zijn betrokken bij de toetsing of Achmea voldoet aan de huidige wet- en regelgeving op het gebied van de Cloud, namelijk: De Nederlandsche Bank, College Bescherming Persoonsgegevens (CBP)[10] en auditors (Faber, 2017).

2.9 Normenkader

Voor het uitbesteden van bedrijfsprocessen is er een normenkader waaraan moet worden voldaan. De uitbestedingen verlopen volgens een vastgesteld proces dat bestaat uit vier fases, namelijk (Outsourcing Policy, 2017):

1. Analyse: bepalen of een uitbestede functie of activiteit een kritieke of belangrijke functie is.
2. Initiatie: contracteren van een geschikte partij resulterend in een ondertekend contract en/of Security Agreement (SA).
3. Overdracht: overdragen van de uit te besteden werkzaamheden aan de gecontracteerde dienstverlener en de inrichting van de vastgelegde processen, rollen en verantwoordelijkheden.
4. Levering en Beheer: beheren, bewaken en bijsturen van het proces dat is uitbesteed tot het einde der looptijd. Dit betekent de overeenkomst inclusief het beheren van de risicoanalyse en het tijdig opstarten van verlenging of initiatie nieuwe uitbesteding.

2.10 Geldende wet- en regelgeving en normenkader

Op het identificeren van Cloud risico's en laten voldoen aan de geldende wet- en regelgeving bij een uitbesteding, zijn verschillende factoren van toepassing. Deze factoren zijn onderverdeeld in kenmerken en documenten (zie afbeelding 2).

2.10.1 Identificatie met behulp van de verschillende kenmerken

De kenmerken die helpen bij het identificeren van Cloud risico's bij een bepaalde uitbesteding zijn (zie afbeelding 3):

- **Soort Clouddienst**

Deze diensten bepalen de mate waarin Achmea de verantwoordelijkheden en controle bij de leverancier legt (Bazuin, 2016).

[9] EER= De Europese Economische Ruimte is de Europese Unie plus IJsland, Noorwegen en Liechtenstein.
[10] Het College Bescherming Persoonsgegevens: Houdt toezicht op de naleving van de Wet Bescherming Persoonsgegevens (SBIFormaat, 2017).

- **Type uitbesteding**

Het verlenen van een opdracht aan een derde tot het verrichten van werkzaamheden (Kampen, 2017).

- **BIV classificatie**

BIV is een afkorting voor 'Beschikbaarheid, Integriteit en Vertrouwelijkheid'. De BIV helpt bij het classificeren van bedrijfsprocessen of gegevens. Om waardes te geven aan de BIV, heeft het classificatiemodel betrekking op een aantal punten (Taskforce, 2014):

  - Beheer gegevensverzameling
  - Informatiesystemen
  - Servers
  - Netwerkcomponenten

Per classificatieniveau (beschikbaarheid, integriteit en vertrouwelijkheid) worden beveiligingseisen beschreven. In de komende paragrafen wordt de definitie van de verschillende classificatieniveaus beschreven met voorbeelden van bijbehorende beveiligingsnormen.

Beschikbaarheid

Beschikbaarheid is gedefinieerd als eigenschappen van het geheel van ICT diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of dienst beschikbaar is voor de geautoriseerde gebruiker, op het moment dat het beschikbaar moet zijn (VNG, 2017).

Voorbeeld beveiligingsnorm: moeten de systemen tijdens werktijd beschikbaar zijn van 8:00 tot 17:00 uur of moeten de systemen 24 uur lang geraadpleegd kunnen worden.

Integriteit

Integriteit geeft de mate aan waarin informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en tijdigheid van transacties.

Het onderwerp integriteit valt onder twee delen uiteen, namelijk de integriteit van datacommunicatie en -opslag enerzijds en de integriteit van de informatie in de applicaties of fysiek anderzijds. Integriteit is gekoppeld aan de applicatie en is altijd situatie afhankelijk en afhankelijk van de eisen van een proces (VNG, 2017). Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en of applicatie nadere afspraken gemaakt kunnen worden. De beveiligingseisen die betrekking hebben op integriteit zijn authenticatie, autorisatie, monitoring en beveiliging. De bewaartermijnen zijn indicatief (VNG, 2017).

Voorbeeld beveiligingsnorm: het authenticatieniveau moet gebaseerd zijn op iets wat men weet en iets wat men heeft (bijvoorbeeld een token of certificaat).

Vertrouwelijkheid

Vertrouwelijkheid is het kwaliteitsbegrip waaronder privacybescherming, maar ook de exclusiviteit van informatie gevangen kunnen worden (VNG, 2017). Het geeft de mate aan waarin informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en geautoriseerdheid van de transacties (VNG, 2017).

Voorbeeld beveiligingsnorm: een autorisatie tot een systeem vereist dat de medewerker deze kennis nodig heeft voor het uitvoeren van zijn taken.

2.10.2 Identificatie met behulp van de verschillende documenten

De documenten die helpen bij het identificeren en specificeren van Cloud risico's bij een bepaalde uitbesteding zijn:

- **Algemene Inkoopvoorwaarden Achmea (AIV)**

In dit document zijn de inkoopvoorwaarden vastgesteld die van toepassing zijn op alle leveranciers die aan Achmea diensten, goederen, software en Clouddiensten leveren (AIV, 2017).

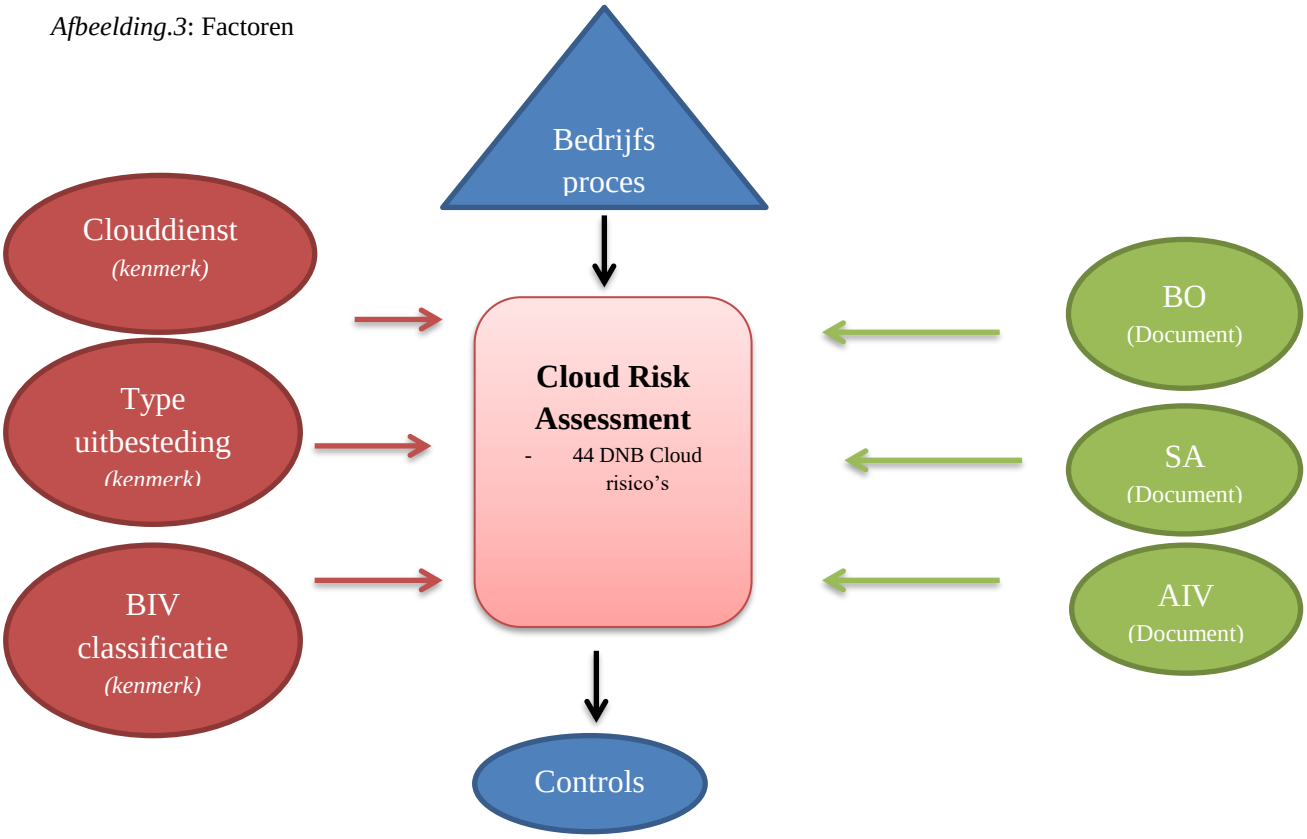
- **Security Agreement (SA)**

In dit document zijn eisen opgesteld waaraan een leverancier minimaal moet voldoen. Naast de afspraken die zijn gemaakt in het Service Agreement, dient de leverancier minimaal in het bezit te zijn van de beveiligingstandaard NEN-ISO/IEC 27001:2013 of een hieraan gelijkwaardige norm (Security Agreement, 2017). De afspraken die tussen de leverancier en Achmea zijn gemaakt, dienen vastgelegd te worden in de vorm van een contract of Security Agreement (SA).

- **Bewerkingsovereenkomst Achmea (BO)**

Dit is een document dat wordt gebruikt als een leverancier persoonsgegevens verwerkt voor Achmea. Mochten bij een uitbesteding persoonsgegevens worden verwerkt in de vorm van namen of foto's, dan dient een verwerkingsovereenkomst ingevuld te worden.

Afbeelding.3: Factoren



2.11 Conclusie

Zoals beschreven, wordt er een onderscheid gemaakt tussen verschillende typen Clouds. Doordat deze in kaart zijn gebracht, kan worden geconcludeerd dat de SAAS de meest verregaande uitbesteding is (zie afbeelding 1). Dit betekent dat de organisatie het minst in eigen beheer heeft. Bij het realiseren van een uitbesteding, is het belangrijk om te voldoen aan de geldende wet- en regelgeving en de norm die door Achmea is opgesteld. Om hieraan te kunnen voldoen, zijn er een aantal factoren van invloed die helpen bij het identificeren en specificeren van Cloud risico's. Deze factoren worden visueel weergegeven in afbeelding 3.

3. Methodologische verantwoording

In dit hoofdstuk worden de dataverzamelingsmethoden beschreven, die bij de onderzoeksvragen (zie hoofdstuk 1.3.1) worden gebruikt om ze te kunnen beantwoorden. Om de juiste methoden te kiezen voor dit onderzoek, is onderzocht welke methode van dataverzameling het beste tot zijn recht komt bij de onderzoeksvragen.

Dit onderzoek is kwalitatief van aard. Het doel van dit onderzoek is niet om theorieën te testen, maar om inzichten te verkrijgen in verschillende percepties van mensen (Swaen, 2017a). Voor het verzamelen van de data is gebruik gemaakt van interviews en documentaties.

Om een antwoord te kunnen definiëren op de onderzoeksvragen (zie hoofdstuk 1.3.1), zijn interviews gehouden met specialisten die werkzaam zijn bij Achmea (kenmerk kwalitatief onderzoek). Om te achterhalen of een uitbesteding voldoet aan de wet- en regelgeving (zie hoofdstuk 2.8) en de norm (zie hoofdstuk 2.9) die Achmea hanteert, wordt onderzocht welke impact de verschillende factoren (zie afbeelding 3) hebben op het Cloud Risk Assessment en welke documentaties daarvoor worden gebruikt.

3.1 Bronverantwoording

De documentaties die zijn gebruikt in het kader van dit onderzoek, zijn gecontroleerd op betrouwbaarheid, volledigheid en actualiteit (Losse, 2017):

Kenmerken bron

- Is de auteur van de publicatie bekend?
- Is het jaar van publicatie/uitgave bekend?
- Is in de publicatie aan bronvermelding gedaan?

Doel auteur

- Wat zijn de belangen van de auteur?
- Is er sprake van een opiniestuk?

Inhoud bron

- Kloppen de gegevens met wat andere bronnen melden?
- Hoe worden de uitspraken door de auteur onderbouwd?

3.2 Methodologische verantwoording onderzoeksvragen

In deze paragraaf wordt de methodologische verantwoording van de onderzoeksvragen beschreven. Eerst wordt beschreven op welke wijze de interviews en documentaties voldoen aan de methodologische verantwoording.

3.2.1 Interview

Omdat Cloud uitbestedingen een nieuwe ontwikkeling is binnen de financiële sector, is het belangrijk om respondenten te vinden die zijn gespecialiseerd op het gebied van Cloud. Om dit te realiseren is er een selecte steekproef[11] uitgevoerd, waarbij de respondent aan minimaal één van de onderstaande kenmerken moet voldoen (Verhoeven, 2017):

[11] Selecte steekproef: interviews die worden georganiseerd met deskundigen of betrokkenen over een bepaald onderwerp (Verhoeven, 2017).

- De respondent dient werkzaam te zijn bij Achmea, omdat de onderzoeksresultaten zich richten op Achmea (zie hoofdstuk 1.4).
- De respondent is bekend met Cloud uitbestedingen waarmee Achmea te maken heeft.
- De respondent weet welk Cloud beleid er binnen Achmea wordt gehanteerd.
- De respondent weet wat het Cloud Risk Assessment is en hoe het uitgevoerd moet worden.

Met de bovenstaande beschreven kenmerken is de onderzoeker door de opdrachtgever in contact gebracht met een tweetal respondenten namelijk:

- Enterprise Security Architect (ESA)

Met de ESA heeft er een interview plaatsgevonden over de normen en de eisen die door zowel Achmea als DNB (het Cloud Risk Assessment) worden gesteld aan een bepaalde uitbesteding. Bij het uitbesteden van persoonsgegevens worden bijvoorbeeld andere eisen en normen gesteld, dan bij het uitbesteden van inkoop van printers.

- Operational Risk Manager (ORM)

Met de ORM is een interview gehouden waarin de categorisering van de verschillende soorten uitbestedingen is besproken en de invloeden ervan op een SAAS Clouddienst.

Afbeelding.4: Respondenten

Respondent	Functie	specialisatie
Respondent 1	Enterprise security architect	Cloud beleid
Respondent 2	Operational Risk Manager	Uitbestedingsbeleid

De specialisten zijn gekozen op basis van relevante kennis voor dit onderzoek (zie de hiervoor beschreven kenmerken). De reden dat er is gekozen voor het interviewen van de ESA is dat diegene het Cloud beleid heeft geschreven en dat up to date houdt. De ESA heeft toegelicht welke wetten en normen van toepassing zijn bij een bepaalde uitbesteding en hoe deze tot stand zijn gekomen. Deze informatie is belangrijk voor het in kaart brengen van de verschillende kenmerken en documentaties die een impact kunnen hebben op een bepaalde uitbesteding (zie hoofdstuk.1.3.1). De ORM is geïnterviewd om zijn specifieke kennis op het gebied van uitbestedingen. Het uitbestedingsbeleid van Achmea is door de ORM geschreven en wordt door de ORM gehanteerd. De ORM hanteert dit beleid in zijn dagelijkse werkzaamheden door risico's bij uitbestedingen te beoordelen. Deze informatie draagt bij aan de beantwoording van de verschillende soorten uitbestedingen die Achmea doet.

Afgezien van de twee specialisten zijn er binnen Achmea geen werknemers die specifieke kennis hebben op het gebied van Cloud. Wel zijn er binnen Achmea werknemers die Cloud risico's moeten identificeren en specificeren met behulp van het Cloud Risk Assessment. Deze personen zijn niet geïnterviewd omdat dit wordt ingevuld als een checklist die vervolgens gecontroleerd wordt (op inhoud) door de ORM (Kampen, 2017). De mensen die het Cloud Risk Assessment invullen zijn daarom niet relevant voor dit onderzoek.

Om de interviews te kunnen controleren op betrouwbaarheid, zijn bij beide interviews geen suggestieve vragen gesteld (zie afbeelding 5). Vervolgens is dieper ingegaan op de specialisatie van de respondent (zie bijlagen 4 en 5).

De opzet van de interviews is als volgt: eerst zijn algemene vragen gesteld over wat het probleem en de oorzaak zijn (zie afbeelding 5). Vervolgens zijn de vragen afgestemd op het specialisatiegebied van de respondenten (zie bijlagen 4 en 5) (zie afbeelding 4). Tot slot is naar de mening van de respondenten gevraagd over de wijze waarop het Cloud Risk Assessment afgestemd kan worden (zie het document getranscribeerde interviews) (Scribbr, 2017).

Afbeelding.5: Algemene vragen

Algemeen	***Wat is uw functie binnen Achmea?***
Houdingen en meningen	*In welke mate krijgt u met Cloud te maken?*
	Waarom is het hebben van Cloud beleid belangrijk?
	Wat is uw visie op het huidige beleid met betrekking tot Cloud?
Feiten	*Biedt het Cloudbeleid voldoende kaders om de risico's te kunnen mitigeren?*
	Wat zijn uw werkzaamheden op het gebied van Cloud?
	Wordt de Cloud Risk Assessment aangepast aan de normen die Achmea stelt, of alleen aan de wet- en regelgeving?
Motivatie	*Wordt het beleid afgestemd met de wijze waarop dit in de praktijk gebeurt?*
	Wat zou u willen veranderen aan het beleid?
	Op welke wijze worden de medewerkers begeleid om een Cloud Risk Assessment uit te voeren?

De interviews zijn opgenomen en volledig getranscribeerd. Vervolgens zijn ze uitgewerkt en gecontroleerd bij de respondenten. Dit vergroot de betrouwbaarheid van dit onderzoek.

3.2.2 Data- analyse

Dit betreft een inductief onderzoek, wat betekent dat de data die is gevonden een theorie vaststelt (Dingemanse, 2017). Omdat de onderzoeker nog niet precies wist waar die naar op zoek was, is het belangrijk om een structuur in de verzamelde data aan te brengen (Van Lanen, 2017). De structuur in de afgenomen interviews is aangebracht op basis van verschillende stappen die zijn doorlopen (Scribbr, 2017):

- Transcriberen

De interviews zijn volledig getranscribeerd. Dit betekent dat letterlijk is opgeschreven wat er in de interviews werd gezegd (Dingemanse, 2017).

- Oriënteren op coderen

In deze fase zijn de verschillende stappen van coderen doorgenomen.

- Open coderen

Het verbinden van labels aan tekstfragmenten. Deze codes geven per fragment aan wat het hoofdthema is.

- Axiaal coderen

Na het open coderen zijn er vergelijkingen gemaakt tussen de verschillende soorten tekstfragmenten. De overeenkomende codes zijn met elkaar samengevoegd.

Na het structureren van de wijze waarop er wordt gecodeerd, worden de gegevens uit de dataverzameling samengevat en in verschillende categorieën ingedeeld. De definitie van analyseren is:

> *Uiteenrafeling van de gegevens over een bepaald onderwerp in categorieën, het benoemen van deze categorieën met begrippen en het aanbrengen en toetsen van relaties tussen de begrippen in het licht van de probleemstelling (Boeije & Boeije, 2014).*

De interviews zijn met de computer en het softwareprogramma Atlas.ti[12] uiteengerafeld in codes die bij de kernbegrippen horen. Voor de analyse is een thematische codelijst opgesteld op basis van de vragen uit het interview. Tevens zijn er codes toegevoegd over onderwerpen die niet vooraf in het interview zijn opgenomen, zoals het bewustzijn van de medewerkers. De output van de gecodeerde data is geanalyseerd en als tekst vastgelegd (zie hoofdstuk 4). De gecodeerde data zijn in tabellen weergegeven en is niet bedoeld als kwantitatieve analyse. De tabellen geven uitsluitend inzicht in de geanalyseerde transcripten (zie afbeelding 6 en 7). In deze tabellen wordt de frequentie weergegeven. De frequentie geeft aan hoe vaak de gecodeerde data zijn genoemd. In dit onderzoek wordt verondersteld dat de factor (frequentie ten opzichte van kernbegrippen) een indicatie is van het belang van het kernbegrip.

3.2.3 Documentatie

Bij dit onderzoek is gebruik gemaakt van bestaande documentatie die is aangeleverd door de Operational Risk Manager van de afdeling Risk & Compliance. Door informatie uit de verschillende documentaties te analyseren, is een beeld gecreëerd van de Cloud risico's die geïdentificeerd moeten worden volgens de wet- en regelgeving en de norm die Achmea hanteert bij een bepaalde uitbesteding. Met behulp van deze informatie is geanalyseerd welke impact de verschillende factoren hebben op het Cloud Risk Assessment bij een uitbesteding die vanuit de SAAS wordt gerealiseerd.

3.3 Methodologische verantwoording per onderzoeksvraag

In deze paragraaf wordt beschreven op welke methodologische wijze de onderzoeksvragen zijn onderzocht.

Onderzoeksvraag één

Welke uitbestedingen vanuit de SAAS zijn bekend binnen Achmea en op welke wijze verschillende deze van elkaar?

Om te weten welke uitbestedingen bekend zijn binnen Achmea, is het Outsourcing Policy document (waarin het uitbestedingsbeleid staat beschreven) geanalyseerd. Dit document is

[12] Atlas.ti is een softwareprogramma die helpt bie een kwalitatieve data analyse. Dit is voor dit onderzoek gebruikt om de interviews te analyseren.

geanalyseerd op het beleid dat Achmea voert op het gebied van uitbestedingen en welke uitbestedingen Achmea kent. De vragen die naar voren kwamen en die zijn behandeld tijdens het interview met de Operational Risk Manager, zijn:

- Op welke wijze verschillen de uitbestedingen van elkaar?
- Welke uitbestedingen worden er gehanteerd binnen de SAAS Clouddienst?
- In hoeverre heeft de Nederlandsche Bank een rol gespeeld in de categorisering van de verschillende soorten uitbestedingen?

Deze vragen zijn behandeld met de Operational Risk Manager in de vorm van een diepte interview (document getranscribeerde interviews). De vragen zijn gericht op het verzamelen van informatie. Het is daarom belangrijk om de specialist de ruimte te geven om te kunnen antwoorden. Dit is de reden dat er is gekozen voor een half-gestructureerd interview[13].

Onderzoeksvraag twee

Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?

Om te weten welke factoren een impact hebben op het Cloud Risk Assessment, zijn verschillende documentaties geanalyseerd:

- Het Cloud Risk Assessment van DNB
- Bewerkersovereenkomst (BO)
- Algemene Inkoopvoorwaarden Achmea (AIV)
- Security Agreement (SA)
- Outsourcing Policy

De documentaties zijn geanalyseerd op basis van de verschillende invloeden die ze hebben op het Cloud Risk Assessment. Ook is geanalyseerd welk beleid er wordt gevoerd door Achmea en/of dit invloed heeft op de Cloud risico's uit het Cloud Risk Assessment. Naar aanleiding hiervan is een aantal vragen naar voren gekomen die tijdens het interview met de Enterprise Security Architect zijn behandeld:

- Wat zegt DNB over de Cloud risico identificatie?
- Is de norm afgestemd op andere organisaties van Achmea, zo ja met wie en hoe?
- Waarop is het Cloud beleid van Achmea gebaseerd?
- Waarom zijn deze factoren gekozen voor het identificeren van Cloud risico's?

Om deze informatie over het Cloud beleid en de wijze waarop het is opgesteld te vergaren, is een diepte interview gehouden met de ESA op het gebied van Cloud beleid binnen Achmea. Omdat er informatie vergaard moest worden over specifieke onderwerpen, is gebruik gemaakt van het half-gestructureerde interview.

Onderzoeksvraag drie

Op welke wijze kan het Cloud Risk Assessment afgestemd worden op uitbestedingen die vanuit een SAAS Clouddienst worden uitgevoerd?

[13] Halfgestructureerd interview: er is hier sprake van een vragenlijst of een lijst met onderwerpen, maar de respondent heeft alle ruimte voor eigen inbreng (Verhoeven, 2017).

Om onderzoeksvraag drie te kunnen beantwoorden, is het belangrijk om het Outsourcing Policy te hebben geanalyseerd. Het doel is te achterhalen op welke wijze het Cloud Risk Assessment afgestemd kan worden op uitbestedingen vanuit een SAAS Clouddienst. De vragen die naar aanleiding van deze analyse naar voren zijn gekomen, zijn besproken met zowel de ORM als de ESA. De vragen zijn:

- Op welke wijze kan het Cloud Risk Assessment afgestemd worden?
- Is de SAAS Clouddienst van invloed op de afstemming van het Cloud Risk Assessment?
- Welke factoren spelen een rol bij de afstemming van het Cloud Risk Assessment?

Om deze vragen te kunnen beantwoorden, zijn de verschillende factoren (met behulp van de AIV, SA, bewerkersovereenkomst etc.)) geanalyseerd op basis van de mogelijke impact die ze kunnen hebben op het Cloud Risk Assessment. Tevens is onderzocht welke invloeden het document Outsourcing Policy heeft op een SAAS uitbesteding. Naast de documentaties, is door middel van een half-gestructureerd interview aan beide specialisten gevraagd op welke wijze het Cloud Risk Assessment efficiënter en/ of effectiever uitgevoerd kan worden (zie document getranscribeerde interviews).

Betrouwbaarheid en validiteit

Twee belangrijke indicatoren voor het bepalen van de kwaliteit van een onderzoek, zijn de betrouwbaarheid en validiteit. Om de betrouwbaarheid van de geanalyseerde documentaties te garanderen, is het boek *Wat is onderzoek* van Nel Verhoeven geraadpleegd. Hierin wordt een aantal regels gehanteerd om de betrouwbaarheid van het onderzoek te garanderen (Verhoeven, 2017):

- Onderhoud nauw contact met de opdrachtgever over de opzet en de uitvoering van het onderzoek.
- Maak eventueel gebruik van triangulatie.
- Peer evaluation- en peer consulatiemethoden.

Daarnaast is gebruik gemaakt van de interne consistentie[14]. Er zijn verscheidene onderwerpen behandeld (het Cloud Risk Assessment, beleid) die hetzelfde beogen te meten, namelijk het efficiënter en/ of effectiever uitvoeren van het Cloud Risk Assessment.

Validiteit is de mate waarin wordt gemeten wat daadwerkelijk gemeten moet worden (Tubbing, 2016). Aan dit onderzoek hebben respondenten deelgenomen die een eigen specialisatiegebied hebben. Het is daarom lastig om precies te meten wat gemeten moet worden. De informatie uit de interviews is namelijk niet te valideren met overige organisaties (ABN Amro, Rabobank). In dit onderzoek is de interne validiteit[15] gewaarborgd. Het onderzoek is zo opgezet in de vorm van interviews en bijpassende documentaties dat de conclusies (van de twee specialisten) voor waar kunnen worden aangenomen (Swaen, 2017a).

Om ervoor te zorgen dat de structuur, taal, verwijzingen en lay out van dit scriptie methodologisch verantwoord is, is er door een externe nakijkdienst naar gekeken.

[14] Interne consistentie: homogeniteit tussen items, ofwel de mate waarin binnen een meetinstrument verschillende items die hetzelfde beogen te meten gelijkwaardige resultaten opleveren (Tubbing, 2016).

[15] Interne validiteit: wordt ook wel methodologische validiteit genoemd. Het zet iets over de kwaliteit van de methode, dataverzameling en analyse

4. Analyse

In hoofdstuk drie is de methodologische verantwoording van dit onderzoek beschreven. In dit hoofdstuk worden de analyses van de verschillende onderzoeksvragen behandeld. Met behulp van deze analyses en het empirisch onderzoek dat is uitgevoerd, kan een antwoord worden geformuleerd op de probleemstelling. De probleemstelling is als volgt gedefinieerd:
In hoeverre is er een categorisering aangebracht in de verschillende soorten uitbestedingen die Achmea kent en in hoeverre kan het Cloud Risk Assessment worden afgestemd op een uitbesteding die vanuit de SAAS Clouddienst wordt gerealiseerd?
Om deze vraag te beantwoorden zullen de volgende deelvragen geanalyseerd worden:

1. *Welke uitbestedingen vanuit de SAAS zijn er bekend binnen Achmea en op welke wijze verschillende deze van elkaar?*
2. *Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?*
3. *Op welke wijze kan het Cloud Risk Assessment afgestemd worden op uitbestedingen die vanuit een SAAS Clouddienst worden uitgevoerd?*

4.1 Analyse onderzoeksvraag één

In deze paragraaf wordt onderzoeksvraag één geanalyseerd. De onderzoeksvraag is als volgt gedefinieerd:
Welke uitbestedingen vanuit de SAAS zijn er bekend binnen Achmea en op welke wijze verschillende deze van elkaar?

De waarnemingen zijn hier gericht op hetgeen in de documentatie Outsourcing Policy wordt beschreven en de vragen die zijn gesteld tijdens de interviews met de specialisten over de uitbestedingen die vanuit de SAAS bekend zijn bij Achmea. Bij het stellen van deze vraag wordt een antwoord beschreven in het document Outsourcing Policy over de verschillende soorten uitbestedingen. Tijdens de interviews zijn vragen gesteld die zijn gericht op het specialisatiegebied van de desbetreffende respondent. Zoals beschreven in hoofdstuk 2.4, is een van de kernbegrippen van dit onderzoek SAAS uitbestedingen. Hier is een splitsing gemaakt in verschillende soorten dimensies. Dimensies hebben invloed op kernbegrippen. Als er wordt gesproken over een Inkoop uitbesteding (zie afbeelding 6) dan heeft dit invloed op een SAAS uitbesteding. Als er over een Kob uitbesteding wordt gesproken dan heeft dit ook invloed op een SAAS uitbesteding, maar dan kent het een andere impact. Daarom is er een verschil aangebracht in verschillende dimensies. Onder het kopje 'Aspect' in afbeelding 6 staat beschreven waarover is gesproken binnen die dimensie. De frequentie geeft aan hoe vaak er is gesproken over de verschillende dimensies en aspecten.

Afbeelding 6: SAAS uitbestedingen
Freq. = hoe vaak een code is genoemd

SAAS uitbestedingen				
Dimensie	**Aspect**	**Freq. Interview ESA**	**Freq. Interview ORM**	**Freq. Totaal**
Inkoop uitbesteding		7	10	17
	Mate van kritiekheid	6	7	
	Toelichting Inkoop uitbesteding	1	3	
Standaard uitbesteding		7	9	16
	Mate van kritiekheid	6	8	
	Toelichting Standaard uitbesteding	1	1	
Kob uitbesteding		8	9	17
	Mate van kritiekheid	7	7	
	Toelichting Kob uitbesteding	1	2	
SAAS uitbestedingen		**Freq. 22**	**Freq. 28**	**Freq. 50**

Uit de tabel blijkt dat bij iedere SAAS uitbesteding ongeveer evenveel opmerkingen zijn gemaakt over de verschillende uitbestedingen en de aspecten die daarmee gepaard gaan. Met name tijdens het interview met de ORM werden de verschillende soorten uitbestedingen frequent genoemd. Dit is logisch, omdat de ORM verantwoordelijk is voor uitbestedingen die worden gerealiseerd binnen Achmea.

Om risico's te kunnen identificeren, is er een categorisering aangebracht in de verschillende soorten uitbestedingen, namelijk: inkoop, standaard en Kob (kritisch of belangrijke) uitbestedingen. Voor een inkoop uitbesteding gelden andere richtlijnen dan voor een standaard of Kob uitbesteding. Deze richtlijnen zijn gecategoriseerd op basis van de mate waarin een functie of activiteit kritiek of belangrijk wordt bevonden (Kampen, 2017).

4.1.1 SAAS uitbestedingen volgens de ESA

Inkoop uitbestedingen

Toen er nog geen Cloud beleid was, werd gesproken over grote en kleine Cloud uitbestedingen. Dit leverde miscommunicatie op, omdat een kleine uitbesteding (zoals dat werd genoemd) even kritisch kan zijn voor een bedrijfsproces als een grote uitbesteding. Nu is er een categorisering in uitbestedingen binnen Achmea, die richtlijnen geeft voor het classificeren en identificeren van risico's (dus ook de Cloud risico's). Bij het uitvoeren van een inkoop uitbesteding, wordt gesproken over uitbestedingen die geen direct gevaar vormen voor de primaire bedrijfsprocessen. Een voorbeeld van zo'n proces is een parkeerapp. Bij het uitvoeren van een inkoop uitbesteding, kan het zijn dat niet alle Cloud risico's (uit het Cloud Risk Assessment) even relevant zijn. Wel moeten deze Cloud risico's geïdentificeerd worden, omdat het belangrijk is om in kaart te hebben welke Cloud risico's er worden gelopen. Deze informatie is nodig om te kunnen overwegen of bepaalde Cloud risico's worden geaccepteerd of niet.

Standaard uitbestedingen

De standaard uitbesteding is een uitbesteding die indirect gevaar oplevert voor de primaire bedrijfsprocessen of reputatie van Achmea. Bij deze uitbesteding is het belangrijk om de Cloud risico's te identificeren en te mitigeren. Bij het accepteren van deze risico's worden er wellicht Cloud risico's gelopen die niet kunnen worden geaccepteerd zoals bij de inkoop uitbesteding wel kan. Het Cloud beleid helpt bij de wijze waarop Cloud risico's (uit het Cloud Risk

Assessment) geïdentificeerd moeten worden en bij het beoordelen van de betrouwbaarheid van de Cloud provider. Het beoordelen van de Cloud provider gebeurt met behulp van een vragenlijst. Deze vragenlijst dient vooraf ingevuld te worden door de werknemer die een proces wil uitbesteden. Naast het identificeren van de verschillende Cloud risico's, is in het Cloud beleid een lijst opgenomen met Cloud controls. Stel dat een Cloud provider niet SOCII of ISO 27001 gecertificeerd is (dit zijn documenten die ondersteuning bieden bij het mitigeren van IT-risico's), dan moet de full control lijst worden uitgevoerd. Deze lijst bestaat uit 190 Cloud maatregelen. Deze maatregelen moeten worden voorgelegd aan de Cloud provider met de vraag of deze maatregelen zijn geïmplementeerd.
Een voorbeeld van een standaard uitbesteding is het uitbesteden van de loonadministratie.

Kob uitbestedingen
Voor de Kob uitbesteding dienen dezelfde stappen doorlopen te worden als bij een standaard uitbesteding. Bij een Kob uitbesteding dienen de Cloud risico's die uit het Cloud Risk Assessment komen, te worden gespecificeerd. Met deze specificaties kunnen er beheersmaatregelen worden getroffen die passen bij het desbetreffende Cloud risico. Als de risico's zijn geïdentificeerd, moeten deze worden gespecificeerd met behulp van een aantal factoren. Deze factoren staan beschreven in afbeelding 3. Bij het controleren op betrouwbaarheid en kennis van de Cloud provider, dienen dezelfde stappen te worden doorlopen als bij een standaard uitbesteding.
Een voorbeeld van een Kob uitbesteding is het afhandelen van schadeclaims.

4.1.2 Inkoop uitbesteding volgens de ORM
Inkoop uitbestedingen
Het uitbesteden van een bedrijfsproces dat niet de primaire processen van Achmea in gevaar brengt, is een inkoop uitbesteding. Bij dit soort uitbestedingen is het identificeren van Cloud risico's in mindere mate relevant. Stel dat het bedrijfsproces loonadministratie een week lang uit de lucht is, dan kan Achmea nog steeds door met de primaire bedrijfsvoering namelijk schadeclaims afhandelen. Het onderscheid tussen de verschillende uitbestedingen is gemaakt, omdat er niet gesproken wordt over grote of kleine uitbestedingen, maar de mate van kritiekheid van een bedrijfsproces dat wordt uitbesteed. Het identificeren van Cloud risico's bij een uitbesteding van loonadministratie is veel minder relevant dan bij een uitbesteding van een meldpunt waar de schadeclaims binnenkomen.

Standaard uitbestedingen
Een standaard uitbesteding is van niet kritieke of minder belangrijke operationele functie of activiteit. Zonder deze activiteiten lopen de primaire processen van Achmea geen direct gevaar. Bij het uitvoeren van een standaard uitbesteding, is het belangrijk om te beschrijven welk bedrijfsproces er wordt uitbesteed. Bij een uitbesteding van persoonsgegevens is het belangrijk om te weten welke gegevens verwerkt worden en welke Cloud risico's (uit het Cloud Risk Assessment) daarmee gepaard gaan. Deze risico's moeten worden gespecificeerd door middel van een Bewerkersovereenkomst.

Kob uitbesteding
Bij een Kob uitbesteding is het belangrijk om alle mogelijk risico's te identificeren en specificeren. Het is belangrijk dat de personen die deze uitbestedingen doen, nadenken over wat er uitbesteed wordt en welke Cloud risico's er worden gelopen. In de praktijk komt naar voren dat mensen die deze uitbestedingen realiseren het moeilijk vinden om de risico's te specificeren.

4.1.3 SAAS uitbestedingen vanuit de documentatie

De definitie van uitbestedingen is in het document Outsourcing Policy als volgt gedefinieerd:
Het verlenen van opdrachten aan derde tot het verrichten van werkzaamheden (Kampen, 2017):

a. die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of dienstverlening; of
b. die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan.

Inkoop uitbesteding
In het document Outsourcing Policy wordt beschreven dat het specifiek inkopen van producten of diensten valt onder een inkoop uitbesteding. Een voorbeeld van een inkoop uitbesteding is het vragen om advies van een externe partij.

Standaard uitbesteding
Het uitbestedingsbeleid beschrijft dat er bij een standaard uitbesteding sprake is van niet kritieke en minder belangrijke operationele functies en activiteiten. Zonder deze functies en activiteiten lopen de primaire bedrijfsprocessen geen direct gevaar. Een voorbeeld van een standaard uitbesteding is de loonadministratie.

Kob uitbesteding
De Kob uitbesteding is een uitbesteding die kritieke of belangrijke operationele functies of activiteiten uitvoert. Zonder deze activiteit of functie kan Achmea niet functioneren. Een voorbeeld van zo'n primair proces is het herverzekeringsproces.

Verschillen
Het verschil tussen de gecategoriseerde uitbestedingen is de mate van kritiekheid voor een primair bedrijfsproces of reputatie. Bij een inkoop uitbesteding levert uitval of misbruik geen direct gevaar op voor de bedrijfsprocessen of reputatie van Achmea. Een standaard uitbesteding levert indirect gevaar op en een Kob uitbesteding is direct gevaarlijk voor de bedrijfsprocessen of reputatie van Achmea.

4.2 Analyse onderzoeksvraag twee

In deze paragraaf wordt onderzoeksvraag twee geanalyseerd. De onderzoeksvraag is als volgt gedefinieerd: Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?

De waarnemingen zijn hier gericht op hetgeen in de verschillende documentaties wordt beschreven en de vragen die zijn gesteld tijdens de interviews met de specialisten over het Cloud Risk Assessment. Bij het stellen van deze vraag worden in documentaties antwoorden beschreven over de verschillende factoren. Gedurende de interviews zijn vragen aan de specialisten gesteld, over hetgeen voor hen van belang is. Zoals beschreven in hoofdstuk 2.4, is een van de kernbegrippen het Cloud Risk Assessment. Net als in onderzoeksvraag één zijn er ook hier dimensies die over het onderwerp het Cloud Risk Assessment gaan. De dimensies die staan beschreven in afbeelding 7 hebben invloed op het Cloud Risk Assessment. De Compliance Risks (bijvoorbeeld waar staat de data) zijn Cloud risico's op het gebied van beleid. Terwijl Operational Risks (bijvoorbeeld logging) gespecificeerd zijn op de operationele risico's. Deze verschillende soorten Cloud risico's zijn onderdeel van het Cloud Risk Assessment maar hebben verschillende invloeden op het Cloud Risk Assessment. De frequentie geeft aan hoe vaak er is gesproken over de verschillende dimensies en aspecten door de respondenten.

Afbeelding 7: Het Cloud Risk Assessment
Freq. = hoe vaak een code is genoemd

Het Cloud Risk Assessment Dimensie	Aspect	Freq. Interview ESA	Freq. Interview ORM	Freq. Totaal
Compliance Risks		10	8	18
	Cloud beleid	4	5	
	Identificeren Cloud risico's	4	2	
	Maatregelen Cloud risico's	2	1	
Technical Risks		10	8	18
	Cloud beleid	4	5	
	Identificeren Cloud risico's	5	2	
	Maatregelen Cloud risico's	1	1	
Operational Risks		8	8	16
	Cloud beleid	6	4	
	Identificeren Cloud risico's	2	3	
	Maatregelen Cloud risico's	0	1	
General Not Cloud Specific Risks		8	8	16
	Cloud beleid	5	4	
	Identificeren Cloud risico's	2	3	
	Maatregelen Cloud risico's	1	1	
Het Cloud Risk Assessment		**Freq. 36**	**Freq. 32**	**Freq. 68**

Uit deze tabel blijkt dat ongeveer evenveel opmerkingen zijn gemaakt over de verschillende dimensies van het Cloud Risk Assessment en over de aspecten. Met name tijdens het interview met de ESA is te zien dat de verschillende risicogebieden uit het Cloud Riks Assessment frequent worden genoemd. Dit is logisch, omdat de ESA een lijst van Cloud controls heeft opgesteld om Cloud risico's te kunnen mitigeren.

Om het Cloud Risk Assessment af te kunnen afstemmen op de identificatie en classificatie van de Cloud risico's, is een categorisering aangebracht in de verschillende soorten risicogebieden, namelijk: Compliance Risks, Technical Risks, Operational Risks en General Not Cloud Specific Risks (zie hoofdstuk 2.6). Deze richtlijnen zijn gecategoriseerd op basis van risicogebieden op het gebied van Cloud.

4.2.1 Het Cloud Risk Assessment volgens de ESA

Er worden verschillende soorten Cloud risico's beschreven, die zijn onderverdeeld in vier soorten risicogebieden (zie hierboven dimensies). Echter, door de ESA wordt geen onderscheid gemaakt tussen de verschillende dimensies die zijn beschreven in afbeelding 7. Dit onderscheid wordt niet gemaakt, omdat de ESA het belangrijk vindt dat bij iedere uitbesteding het volledige Cloud Risk Assessment wordt uitgevoerd. Dit betekent dat de ESA het uitvoeren van het Cloud Risk Assessment bij een uitbesteding die persoonsgegevens verwerkt, even belangrijk vindt als een uitbesteding die te maken heeft met het faciliteren van een parkeerapp. Dit heeft te maken met de relevantie van Cloud risico's. De risico's zijn namelijk op te delen in een lage relevantie en een hoge relevantie. Het kan niet zijn dat een Cloud risico helemaal niet van toepassing is.

4.2.2 Het Cloud Risk Assessment volgens de ORM

Het aantal opmerkingen van de ORM over het Cloud Risk Assessment is wat lager, omdat de ORM zich met name bezighoudt met het uitbestedingsbeleid. Echter, door de ORM wordt geen onderscheid gemaakt tussen de verschillende soorten dimensies. Iedere Cloud risicogroep is even belangrijk. Dit betekent dat de ORM het net als de ESA belangrijk vindt dat indien een uitbesteding wordt gedaan, ongeacht de soort uitbesteding, het gehele Cloud Risk Assessment uitgevoerd wordt. De ORM geeft aan dat dit te maken heeft met de relevantie van het Cloud risico. Een risico kan in mindere mate relevant zijn, maar het blijft nog steeds een risico.

4.2.3 Het Cloud Risk Assessment volgens de documentaties

De kenmerken die zijn geanalyseerd:

Clouddienst

De soort Clouddienst bepaalt in welke mate de organisatie het bedrijfsproces in eigen beheer houdt. Bij een SAAS uitbesteding is het belangrijker om een Cloud Risk Assessment uit te voeren, dan bij een IAAS dienst. Dit heeft te maken met het feit dat een SAAS het volledige beheer bij de Cloud provider legt.

Type uitbesteding

De wijze van analyseren van de verschillende soorten typen uitbestedingen is gedaan door middel van het uitbestedingsbeleid. Dit beleid is opgenomen in het document Outsourcing Policy. Voor de wijze waarop dit is geanalyseerd wordt er verwezen naar hoofdstuk 4.1.3.

BIV classificatie

De BIV classificatie staat voor: beschikbaarheid, integriteit en vertrouwelijkheid (zie hoofdstuk 2.9). Dit zijn verschillende soorten beschermingsniveaus beschreven in de vorm van classificaties. Deze beschermingsniveaus zijn geanalyseerd op de mogelijke impact van het Cloud Risk Assessment. Het beschikbaarheidsniveau stelt geen eisen aan de inhoud van de data. Een voorbeeld van het classificeren van een uitbesteding op het gebied van beschikbaarheid is het te allen tijde kunnen raadplegen van de e-mail. Bij het classificatieniveau 'integriteit' is het

belangrijk dat de informatie actueel is. Een voorbeeld van integriteit is dat de klant moet kunnen inzien voor welk zorgpakket er is betaald. Bij het classificatieniveau 'vertrouwelijkheid' is het belangrijk om te weten wat de vertrouwelijkheidsrisico's zijn bij een bepaalde uitbesteding. Worden er bijvoorbeeld persoonsgegevens uitbesteed en wat zijn de mogelijke risico's als deze worden gestolen?

De documenten die zijn geanalyseerd:

Algemene Inkoopvoorwaarden Achmea (AIV)

Zoals beschreven in hoofdstuk 2.9, bevat het AIV algemene richtlijnen voor uitbestedingen die worden gedaan. De voorwaarden gaan over goederen, diensten, software en Clouddiensten (AIV, 2017). De relevantie van de AIV op een SAAS uitbesteding, is dat iedere host waarbij Achmea een dienst afneemt, moet voldoen aan de scheiding tussen de programmatuur[16] en dataserver[17] (AIV, 2017). Dit betekent dat een programma niet op een centrale computer mag draaien.

Security Agreement (SA)

Het Security Agreement helpt bij het identificeren van de Cloud risicogebieden waarmee Achmea te maken kan krijgen bij een uitbesteding. Tevens is het een document om afspraken vast te leggen met de leverancier. Deze afspraken zijn belangrijk voor de manier waarop er wordt omgegaan met een bedrijfsproces dat is uitbesteed. Op deze wijze ontstaat er een vertrouwensband met de leverancier en Achmea.

De Cloud risico's die zijn opgenomen in het Cloud Risk Assessment, worden geïdentificeerd in verschillende artikelen die zijn opgenomen in het Security Agreement. *Bijvoorbeeld:* er heeft een datalek plaatsgevonden bij de leverancier. In het Security Agreement worden richtlijnen beschreven om afspraken vast te leggen tussen de leverancier en de afnemer. Deze afspraken bepalen (in het voorbeeld van een datalek) wanneer er wordt gerapporteerd aan de afnemer en op welke wijze dit gebeurt.

Bewerkersovereenkomst (BO)

De BO is een verplichte bijlage op het moment dat persoonsgegevens worden uitbesteed. Het document helpt bij het specificeren van Cloud risico's op het gebied van:

- Persoonsgegevens buiten de EU
- Geheimhouding en bijzondere persoonsgegevens
- Beveiliging
- Melden datalekken
- Inschakelen derden
- Medewerking bij klachten en verzoeken
- Vrijwaring
- Retourneren en vernietigen persoonsgegevens
- Audits
- Verwerkingsgegevens

[16] Programmatuur: programma's van een computer
[17] Dataserver: een centrale computer in een netwerk die opgeslagen data beschikbaar stelt aan gebruikers

Naast het identificeren van Cloud risico's, helpt de BO bij het afstemmen van het Cloud Risk Assessment. Is bijvoorbeeld bij een uitbesteding geen sprake van persoonsgegevens die worden verwerkt, dan hoeft de BO niet uitgevoerd te worden.

Kortom, de BO is een verplicht document voor aanvullende richtlijnen, die helpen bij het identificeren en specificeren van risico's op het gebied van persoonsgegevens.

4.3 Analyse onderzoeksvraag drie

Op welke wijze kan het Cloud Risk Assessment afgestemd worden op uitbestedingen die vanuit een SAAS Clouddienst worden uitgevoerd?

De waarnemingen zijn hier gericht op hetgeen is geanalyseerd in de onderzoeksvragen één en twee. Om een antwoord te formuleren op deze onderzoeksvraag, is tijdens de interviews gesproken over de kernbegrippen met bijbehorende dimensies die staan beschreven in hoofdstuk 4.1 en hoofdstuk 4.2. Met deze informatie is er geanalyseerd wat voor invloed de verschillende soorten SAAS uitbestedingen op het Cloud Risk Assessment hebben. Tevens worden hier de analyses van de verschillende kenmerken en documentaties (zie afbeelding 3) meegenomen.

5. Resultaten

In hoofdstuk vier zijn de analyses beschreven. In dit hoofdstuk komen de resultaten aan bod.

5.1 Resultaten onderzoeksvraag één

Welke uitbestedingen vanuit de SAAS zijn er bekend binnen Achmea en op welke wijze verschillen deze van elkaar?

Uit de analyse van onderzoeksvraag één (zie hoofdstuk 4.1.1) kan worden geconcludeerd dat drie verschillende soorten uitbestedingen van toepassing zijn, namelijk:

- *Inkoop uitbesteding*

Een inkoop uitbesteding is een uitbesteding die geen gevaar vormt voor de primaire bedrijfsprocessen en/of reputatie. Een voorbeeld van zo'n bedrijfsproces is een parkeerapp die bijhoudt hoeveel plaatsen er nog vrij zijn op het parkeerterrein.

- *Standaard uitbesteding*

De standaard uitbesteding is een uitbesteding die indirect gevaar vormt voor de primaire bedrijfsprocessen en/of reputatie. Een voorbeeld van een standaard uitbesteding is de loonadministratie. Bij de uitval van dit proces loopt de organisatie geen direct gevaar. Wel kan na verloop van tijd onrust ontstaan omdat de organisatie iedere keer te laat is met het uitbetalen van het loon, met als gevolg dat bijvoorbeeld een staking plaatsvindt.

- *Kob uitbesteding*

Een Kob uitbesteding is een uitbesteding die direct gevaar oplevert voor de primaire bedrijfsprocessen en/of reputatie. Bijvoorbeeld bij de uitval van bijvoorbeeld een herverzekeringsproces. Het herverzekeren van klanten is namelijk een primair proces van Achmea.

De categorisering is gebaseerd op de mate van kritiekheid voor de primaire bedrijfsprocessen en/of reputatie van Achmea.

5.2 Resultaten onderzoeksvraag twee

Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?

Zoals beschreven in de analyse van onderzoeksvraag twee (zie hoofdstuk 4.2) zijn er verschillende factoren die impact hebben op het identificeren en classificeren van Cloud risico's. Deze factoren worden onderverdeeld in kenmerken en documenten (zie afbeelding 3). De kenmerken die impact hebben op het Cloud Risk Assessment zijn (zie hoofdstuk 2.10.1):

- **Soort Clouddienst**

Een Clouddienst bepaalt de mate waarin Achmea de verantwoordelijkheden en controle bij de leverancier neerlegt.

- **Type uitbesteding**

Het verlenen van een opdracht aan een derde tot het verrichten van werkzaamheden.

- **BIV classificatie**

De BIV helpt bij het classificeren van bedrijfsprocessen of gegevens.

Naast de kenmerken zijn er ook verschillende soorten documenten die impact hebben op het Cloud Risk Assessment. Deze documenten zijn (zie hoofdstuk):

- **Algemene Inkoopvoorwaarden Achmea (AIV)**

In dit document zijn de inkoopvoorwaarden vastgesteld die van toepassing zijn op alle leveranciers die aan Achmea diensten, goederen, software en Clouddiensten leveren.

- **Security Agreement (SA)**

In dit document zijn eisen opgesteld waaraan een leverancier minimaal moet voldoen.

- **Bewerkingsovereenkomst Achmea (BO)**

Dit is een document dat wordt gebruikt als een leverancier persoonsgegevens verwerkt voor Achmea.

5.3 Resultaten onderzoeksvraag drie

Om een afstemming te realiseren, kan worden geconcludeerd dat de factoren (zie afbeelding 3) die bij onderzoekvraag twee zijn beschreven, invloed hebben op de afstemming van het Cloud Risk Assessment. De wijze waarop het Cloud Risk Assessment is afgestemd, is afhankelijk van de relevantie van een Cloud risico bij een bepaalde factor. De factoren zijn onderverdeeld in kenmerken en documenten.

In de volgende paragraaf wordt beschreven wat voor impact de verschillende kenmerken en documenten hebben op het Cloud Risk Assessment. De risico's die worden beschreven zijn in mindere mate relevant. Dit betekent niet dat het geen Cloud risico's zijn, maar wel dat ze geaccepteerd kunnen worden als restrisico (zie bijlage 6. Excel sheet Afstemming):

- ***Soort Clouddienst***

Een SAAS uitbesteding is de meest verregaande uitbesteding die er is. Dit heeft gevolgen voor de mate van relevantie van een aantal Cloud risico's uit het Cloud Risk Assessment. Deze risico's zijn:

  - DNB Cloud risico 20: Undertaking of malicious probs or scans

Het verzamelen van de informatie in de context van een hackpoging, zal niet door de organisatie gebeuren. Bij een SAAS uitbesteding bevinden de data zich namelijk bij een host. De organisatie die de SAAS uitbesteding heeft gedaan, moet ervoor zorgen dat een meldingsplicht is vastgelegd, maar niet over het verzamelen van de informatie over de hackpoging.

  - DNB Cloud risico 21: Compromise service engine

Dit Cloud risico wordt afgehandeld door de host. Deze afspraken staan vast in het AIV van Achmea.

  - DNB Cloud risico 39: Backups lost, stolen

De ontoereikende fysieke procedure is wel een Cloud risico, maar dit hoeft geen gevolgen te hebben voor de werking van de Cloud. Bij verlies van een backup, kan de Cloud alsnog worden benaderd.

  - DNB Cloud risico 41 Theft of computer equipment

Het stelen van bijvoorbeeld een computer heeft geen invloed op Clouddiensten. Mensen kunnen een andere computer gebruiken. Tevens is er geen toegang tot de Clouddienst voor de dief, omdat autorisatiemaatregelen bestaan voor het gebruik maken van een Clouddienst.

  - DNB risico 42 Natural disaster

Een natuurramp hoeft geen risico te zijn voor het gebruik van Cloud. De Cloud is een virtuele omgeving waardoor het niet uitmaakt vanuit welke locatie of welke computer het wordt benaderd.

- ***Type uitbesteding***

  Er is een categorisering aangebracht in uitbestedingen (zie hoofdstuk 5.1) namelijk: inkoop, standaard, en Kob uitbesteding. In deze paragraaf wordt beschreven wat de impact van de verschillende soorten uitbestedingen op de Cloud risico's uit het Cloud Risk Assessment is (zie Excel sheet Afstemming).

  - **Inkoop uitbesteding**

Een inkoop uitbesteding vormt geen gevaar voor de primaire bedrijfsprocessen of reputatie van een organisatie. Het gevolg hiervan is dat de 44 Cloud risico's uit het Cloud Risk Assessment een lage relevantie hebben. Mocht het een uitbesteding zijn waarbij belangrijke gegevens of primaire processen van Achmea direct of indirect in gevaar komen, dan wordt het minimaal een standaard uitbesteding.

Bijvoorbeeld: er wordt een SAAS uitbesteding gedaan om bij te houden hoeveel mensen een zorgverzekering afsluiten bij Zilveren Kruis, zonder gegevens van de desbetreffende personen op te slaan. Dit heeft geen gevolgen voor de primaire processen of reputatie van Achmea.

  - **Standaard uitbesteding**

  De standaard uitbesteding levert geen direct gevaar op voor de primaire bedrijfsprocessen of reputatie van een organisatie, maar een langdurige uitval van deze uitbesteding wel. Het is daarom van belang om het gehele Cloud Risk Assessment uit te voeren. Om het Cloud Risk Assessment in te vullen, is het van belang om alle factoren (zie afbeelding 3) die impact hebben op de uitbesteding, te definiëren en specificeren.

Bijvoorbeeld: de SAAS uitbesteding bij het voorbeeld van de inkoop uitbesteding wordt uitgebreid met namen van mensen die een verzekering hebben afgesloten bij Achmea. Een gevolg hiervan is dat persoonsgegevens verwerkt worden zoals namen van klanten. Het verlies of de diefstal van deze gegevens levert geen direct gevaar op voor de reputatie of de bedrijfscontinuïteit van Achmea. Wel kan het naar verloop van tijd gevolgen hebben voor de reputatie, omdat mensen geen vertrouwen meer hebben in de wijze waarop er wordt omgegaan met de persoonlijke gegevens.

  - **Kob uitbesteding**

De Kob uitbesteding is de meest kritieke (zie hoofdstuk 4.1). Bij een Kob uitbesteding is het belangrijk om de Cloud risico's zoveel mogelijk te identificeren en specificeren. Hiervoor dienen alle mogelijke documenten en kenmerken (zie afbeelding 5) uitgevoerd te worden, die helpen bij het specificeren van mogelijke Cloud risico's die gepaard gaan met de desbetreffende uitbesteding.

Bijvoorbeeld: niet alleen de namen van klanten worden aan de verzekering gelinkt, maar ook wat voor soort verzekering er is afgesloten. Bij diefstal of misbruik heeft dit directe gevolgen voor Achmea.

- ***BIV classificatie***

In hoofdstuk 2.10.1 wordt beschreven wat de BIV classificatie inhoudt. Vanuit de beschikbaarheid, integriteit en vertrouwelijkheid is gekeken naar de relevantie van Cloud risico's.

De volgende resultaten zijn hieruit gekomen:

- **Beschikbaarheid**

Als het Cloud Risk Assessment vanuit het classificatieniveau beschikbaarheid wordt geanalyseerd, dan zijn er achttien Cloud risico's van toepassing (zie Excel sheet Afstemming). Dit geringe aantal Cloud risico's heeft te maken met het feit dat er geen eisen worden gesteld aan de inhoud van data.

- **Integriteit**

De kenmerken van integriteit zijn de mate waarin informatie actueel is, geen fouten bevat en volledig is. Als vanuit de integriteit naar het Cloud Risk Assessment wordt gekeken, dan resulteert dit in dertig relevante Cloud risico's (zie Excel sheet Afstemming). De reden dat integriteit meer Cloud risico's bevat dan beschikbaarheid, is omdat integriteit eisen stelt aan de inhoud van data. Het feit dat vanuit integriteit minder risico's relevant zijn dan vanuit vertrouwelijkheid, is omdat er vanuit integriteit vooral wordt gekeken naar het organisatieproces (werkt het naar behoren).

- **Vertrouwelijkheid**

Op basis van het Cloud Risk Assessment zijn de meeste Cloud risico's van toepassing op het classificatietype vertrouwelijkheid. Op dit classificatieniveau zijn 35 Cloud risico's uit het Cloud Risk Assessment van toepassing (zie Excel sheet Afstemming). De reden dat het classificatieniveau vertrouwelijkheid meer Cloud risico's met zich mee brengt dan de andere twee classificatieniveaus, is omdat bij een SAAS uitbesteding geen tot weinig sprake is van eigen beheer over gegevens.

Naast de kenmerken zijn er documenten die een impact hebben op het Cloud Risk Assessment. De documenten helpen met name bij het specificeren van de Cloud risico's.

- ***Algemene Inkoopvoorwaarden Achmea (AIV)***

De impact die de AIV heeft op het Cloud Risk Assessment is lastig te bepalen, omdat dit document niet specifiek gericht is op het onderwerp Cloud. Het gevolg hiervan is dat (voordat er kan worden voldaan aan de algemene voorwaarden) de Cloud risico's al geïdentificeerd moeten zijn. Deze Cloud risico's kunnen door middel van de kenmerken en overige documenten (zie afbeelding 3) worden beschreven. Geheel op zichzelf staand heeft de AIV een te generieke invloed op het Cloud Risk Assessment, die niet kan worden afgestemd. Zie ook het Excel document Afstemming voor de generieke afstemming op de 44 Cloud risico's van het Cloud Risk Assessment.

- ***Security Agreement (SA)***

De SA helpt bij het identificeren van de Cloud risicogebieden waarmee de organisatie te maken kan krijgen bij een uitbesteding. Tevens is het een document om afspraken vast te leggen met de leverancier. Deze afspraken zijn belangrijk voor de omgangswijze met het bedrijfsproces dat is uitbesteed. Op deze manier ontstaat een vertrouwensband met de leverancier en de organisatie. De Cloud risico's die zijn opgenomen in het Cloud Risk Assessment worden geïdentificeerd in verschillende artikelen die zijn opgenomen in de SA. *Bijvoorbeeld:* er heeft een datalek plaatsgevonden bij de leverancier. In de SA worden richtlijnen gegeven om afspraken vast te leggen tussen de leverancier en de afnemer. Deze afspraken bepalen (in het voorbeeld van een datalek) wanneer er wordt gerapporteerd aan de afnemer en op welke wijze

dit gebeurt. De Cloud risico's uit het Cloud Risk Assessment zijn te specifiek voor de SA om bepaalde Cloud risico's als minder relevant aan te wijzen (zie het Excel sheet Afstemming).

- **Bewerkersovereenkomst (BO)**

Naast het identificeren van Cloud risico's, helpt de BO bij het afstemmen van het Cloud Risk Assessment. Is er bijvoorbeeld bij een uitbesteding geen sprake van persoonsgegevens die worden verwerkt, dan hoeft de BO niet uitgevoerd te worden. Op het moment dat er wel persoonsgegevens worden uitbesteed, zijn acht Cloud risico's niet van toepassing (zie bijlage 6 Excelsheet Afstemming). Deze Cloud risico's zijn niet van toepassing, omdat ze een lage relevantie hebben met betrekking tot het uitbesteden van persoonsgegevens. Kortom, de BO is een verplicht document voor aanvullende richtlijnen, die helpen bij het identificeren en specificeren van Cloud risico's op het gebied van de verwerking van persoonsgegevens.

6. Conclusie & Aanbevelingen

In hoofdstuk vijf zijn de resultaten beschreven. In dit hoofdstuk zullen de conclusies en aanbevelingen worden behandeld.

6.1 Conclusie onderzoeksvraag één

Welke uitbestedingen vanuit de SAAS zijn er bekend binnen Achmea en op welke wijze verschillen deze van elkaar?

Er zijn drie verschillende soorten uitbestedingen namelijk: Inkoop, Standaard en de Kob uitbesteding. Deze verschillen van elkaar op basis van de mate van kritiekheid.

Toelichting:

Er kan worden geconcludeerd dat de uitbestedingen niet specifiek gericht zijn op SAAS. Wel is er een categorisering aangebracht in de uitbestedingen op basis van de mate van kritiekheid. Door de mate van kritiekheid van een SAAS uitbesteding te duiden, valt de uitbesteding onder een van de drie gecategoriseerde uitbestedingen.

6.2 Conclusie onderzoeksvraag twee

Welke factoren hebben impact op het Cloud Risk Assessment voor het identificeren en classificeren van Cloud risico's?

Alle kenmerken en documenten die zijn opgenomen in afbeelding drie hebben impact op het Cloud Risk Assessment.

Toelichting:

Er kan geconcludeerd worden dat verschillende soorten factoren impact hebben op het Cloud Risk Assessment. Deze factoren zijn onderverdeeld in kenmerken en documenten. Deze informatie vormt de basis voor de beantwoording van onderzoeksvraag drie, omdat hierin wordt beschreven wat de impact van de verschillende factoren is om deze te kunnen afstemmen op het Cloud Risk Assessment.

6.3 Conclusie onderzoeksvraag drie

Op welke wijze kan het Cloud Risk Assessment afgestemd worden op uitbestedingen die vanuit een SAAS Clouddienst worden uitgevoerd?

Het Cloud Risk Assessment moet worden afgestemd op basis van factoren.

Toelichting:

Geconcludeerd kan worden dat de afstemming moet plaatsvinden op basis van de factoren (zie afbeelding 3) en mate van relevantie van een bepaald Cloud risico uit het Cloud Risk Assessment.

6.4 Conclusie probleemstelling

In hoeverre is er een categorisering aangebracht in de verschillende soorten uitbestedingen die Achmea kent en kan het Cloud Risk Assessment worden afgestemd op een uitbesteding die vanuit de SAAS wordt gerealiseerd?

Er is een categorisering aangebracht in uitbestedingen op basis van de mate van kritiekheid (zie conclusie onderzoeksvraag een). De afstemming van het Cloud Risk Assessment op een SAAS uitbesteding is mogelijk door de verschillende factoren in afbeelding drie te identificeren en classificeren.

Toelichting:

De categorisering bestaat uit een inkoop uitbesteding die geen impact heeft op de primaire bedrijfsprocessen en reputatie van de organisatie. De standaard uitbesteding die indirecte gevolgen heeft voor de primaire bedrijfsprocessen en reputatie van de organisatie. En tot slot de Kob uitbesteding die directe gevolgen heeft voor de primaire bedrijfsprocessen of reputatie van de organisatie.

De afstemming van het Cloud Risk Assessment op een SAAS uitbesteding is mogelijk door de mate van relevantie van de verschillende factoren uit onderzoeksvraag twee en drie te identificeren en classificeren. Met deze informatie kan er worden gekeken naar de mate van relevantie van bepaalde Cloud risico's uit het Cloud Risk Assessment bij een bepaalde uitbesteding. Voor de afstemming van het Cloud Risk Assessment wordt er verwezen naar bijlage 6 Excel sheet Afstemming.

6.5 Aanbevelingen

In deze paragraaf worden aanbevelingen beschreven voor de afstemming en efficiënter uitvoeren van het Cloud Risk Assessment op een uitbesteding die vanuit de SAAS wordt gerealiseerd.

De volgende aanbevelingen zijn geformuleerd naar aanleiding van het onderzoek:

De belangrijkste aanbeveling naar aanleiding van dit onderzoek is om te zorgen dat in de praktijk het Cloud Risk Assessment afgestemd gaat worden op de specifieke eigenschappen van de SAAS uitbesteding.

Toelichting:

In de huidige situatie wordt het gehele Cloud Risk Assessment uitgevoerd als een checklist. In de conclusie van onderzoeksvraag drie is geschreven dat bepaalde Cloud risico's in mindere mate relevant zijn voor een SAAS uitbesteding. Het is daarom de bedoeling dat in de praktijk gekeken gaat worden naar de kenmerken van een SAAS uitbesteding met de bijbehorende Cloud risico's uit het Cloud Risk Assessment. Als dit in de praktijk kan worden verwezenlijkt, dan levert dit tijdsbesparing op bij de identificatie en classificatie van Cloud risico's.

De tweede aanbeveling is dat het bewustzijn van het personeel vergroot moet worden.

Toelichting:
In de huidige situatie is niet iedereen zich bewust van de factoren die van invloed zijn bij een bepaalde uitbesteding. Op het moment dat dit wel het geval is, wordt het veiligheidsbewustzijn op het gebied van het realiseren van uitbestedingen vergroot. Zoals staat beschreven in de analyse van het interview met de ORM, is het bewustzijn van het personeel op het gebied van uitbestedingen met identificatie en classificatie van relevante Cloud risico's laag (Getranscribeerde interviews). Het is daarom aan te bevelen om het bewustzijn van de medewerkers die uitbestedingen realiseren te vergroten.

De derde aanbeveling is bij het realiseren van een uitbesteding die valt onder de inkoop uitbesteding om het Cloud Risk Assessment niet uit te voeren.

Toelichting:
Zoals beschreven in de conclusie van onderzoeksvraag twee vormt de inkoop uitbesteding geen gevaar voor de primaire bedrijfsprocessen of reputatie van de organisatie. Het is daarom niet nodig om Cloud risico's te identificeren die naar alle waarschijnlijkheid worden geaccepteerd als restrisico.

7. Vervolgonderzoek

Naar aanleiding van dit onderzoek zou een aantal vervolgonderzoeken relevant kunnen zijn voor het verder definiëren en specificeren het Cloud Risk Assessment.

1. IAAS en PAAS

Dit onderzoek heeft zich gericht op de Clouddienst SAAS en de afstemming op het Cloud Risk Assessment. Om te weten met welke Clouddienst Achmea minder relevante Cloud risico's loopt, moet worden onderzocht wat de impact van de PAAS en IAAS op het Cloud Risk Assessment is.

2. Bewustzijn personeel

Uit het interview met de ORM is naar voren gekomen dat de mensen die Cloud uitbestedingen realiseren, niet altijd weten wat voor impact deze hebben op het bedrijfsproces of de reputatie van Achmea. Voor het effectiever werken met het Cloud Risk Assessment, is een onderzoek naar het huidige bewustzijn van personen van belang.

3. Analyseren

Dit uitgevoerde onderzoek valideren met reeds uitgevoerde Cloud Risk Assessments. Als dit onderzoek kan worden vergeleken met Cloud Risk Assessments die in de praktijk zijn uitgevoerd, kan worden onderzocht of er Cloud risico's zijn die bij bepaalde uitbestedingen een lage relevantie hebben.

Bronnenlijst

Accountant. (2014, 4 april). Negen risico's cloud computing. Geraadpleegd op 9 oktober 2017, van https://www.accountant.nl/nieuws/2014/4/negen-risicos-cloud-computing/#

Achmea. (2017a). Geschiedenis. Geraadpleegd op 6 september 2017, van https://www.achmea.nl/over-ons/geschiedenis/Paginas/default.aspx

Achmea. (2017b). Versie 1.0. Geraadpleegd op 9 oktober 2017, van https://zoeken.achmeanet.nl/Paginas/Documenten.aspx?k=GISO

Achmea (2017c). Onze merken. Geraadpleegd op 6 september 2017, van https://www.achmea.nl/merken/Paginas/default.aspx

Achmea. (2017d). Organisatie. Geraadpleegd op 6 september 2017, van https://www.achmea.nl/over-ons/organisatie/paginas/default.aspx

Achmeanet.nl. (2017a). Gewaagd doel. Geraadpleegd op 8 september 2017, van https://nieuws.achmeanet.nl/organisatie/000/Paginas/Klantrelevant-en-toonaangevend.aspx

Achmeanet.nl. (2017b). [Tabel Organizational Risks]. Geraadpleegd op 8 september 2017, van http://www.toezicht.dnb.nl/binaries/50-228202.pdf

Avero Achmea. (2017). Consument, zakelijk & adviseurs. Geraadpleegd op 6 september 2017, van https://www.averoachmea.nl/

Bazuin, I. (2016, 8 november). Cloudoplossingen: de verschillen tussen IaaS, PaaS en SaaS. Geraadpleegd op 12 september 2017, van https://www.ogd.nl/blog/post/2016/11/cloudoplossingen-de-verschillen-tussen-iaas-paas-en-saas/

Bel, H. (2006, 3 december). Veel organisaties worstelen. Geraadpleegd op 15 februari 2018, van file:///C:/Users/steph/Downloads/expert-brief-security-architectuur.pdf

Boeije, H., & Boeije, H. (2014). *Analyseren in kwalitatief onderzoek*. Amsterdam, Nederland: Boom Lemma.

Centraal Beheer. (2017). Onze verzekeringen op een rij. Geraadpleegd op 6 september 2017, van https://www.centraalbeheer.nl/verzekeringen/Paginas/overzicht.aspx?categorie=meest-gekozen

Cloudscanner (2017, 26 januari). Wat zijn de verschillen tussen publieke, private en hybride cloud? Geraadpleegd op 13 september 2017, van http://cloudscanner.nl/wat-zijn-de-verschillen-tussen-de-publieke-private-en-hybride-cloud/

Cloudshape. (2017). Herken het verschil tussen Cloud en Cloud. Geraadpleegd op 12 februari 2018, van http://partner.ictmedia.nl/images/uploads/documenten/Whitepaper_realcloud_LR.pdf

De Nederlandsche Bank. (2017) Besluit prudentiële regels Wft (Bpr). Geraadpleegd op 26 september 2017, van http://www.toezicht.dnb.nl/4/4/2/50-204104.jsp

Diddens, M. (2017). Operational Risk Management. Geraadpleegd op 15 februari 2018, van www.infosecurity.nl/accentadvies/operational-risk-management

Dingemanse, K. (2017, 16 mei). Ultiem stappenplan voor het coderen van interviews. Geraadpleegd op 19 september 2017, van https://www.scribbr.nl/onderzoeksmethoden/coderen-interview/

deitauditor. (2017). Taken, bevoegdheden en verantwoordelijkheden van de Compliance Officer. Geraadpleegd op 7 september 2017, van http://www.decomplianceofficer.nl/content/2011/11/Taken-bevoegdheden-en-verantwoordelijkheden-van-de-Compliance-Officer

Faber, R. (2015, 10 december). Geraadpleegd op 15 oktober 2017 Computing Privacy & Security.

FBTO. (2017). De verzekeringen van FBTO. Geraadpleegd op 6 september 2017 van https://www.fbto.nl/hulp-en-contact/Paginas/alle-verzekeringen.aspx

Fundaments Cloud Infrastructure. (2017). Verschillende soorten cloud. Geraadpleegd op 13 september 2017, van https://www.fundaments.nl/verschillende-soorten-cloud

Hagelunie. (2017). Onze verzekeringen. Geraadpleegd op 6 september 2017, van http://www.hagelunie.nl/onze-verzekeringen/Paginas/default.aspx

Hillenaar, Y. (2017). Cloud Risk Assessment. Problematiek: waarom een Cloud Risk Assessment? Geraadpleegd op 16 oktober 2017, van https://www.pinkelephant.nl/it-management-consulting/process/cloud-risk-assessment/

Inshared. (2017). Alle verzekeringen van Inshared. Geraadpleegd op 6 september 2017, van https://www.inshared.nl/verzekeringen

Interpolis. (2017). Alle verzekeringen. Geraadpleegd op 6 september 2017, van https://www.interpolis.nl/verzekeren

Janssen, M. (2008, 5 december). Wat is SAAS? Geraadpleegd op 5 oktober 2017, van http://computerworld.nl/cloud/62599-wat-is-saas

Jessurun, A., & Mirkovic, N. (2015, 23 september). Hoewel de bovenstaande omschrijvingen. Geraadpleegd op 17 oktober 2017, van Software As A Service

Kampen, A. (2017, 1 oktober). Achmea definieert het proces van uitbesteden. Geraadpleegd op 30 december 2017, van het document Outsourcing Policy

Losse, M. (2012). Syllabus Probleemanalyse. Enschede Nederland geraadpleegd op 12-9-2017 van Enschede: Saxion University of Applied Sciences

Nationaal Cyber Security Centrum. (2017). NIST. Geraadpleegd op 11 september 2017, van https://www.ncsc.nl/zoeken?query=Cloudcomputing+%26+Security

Nederlandse encyclopedie. (2017). Uitbesteden. Geraadpleegd op 19 september 2017, van http://www.encyclo.nl/begrip/uitbesteden

Outsourcing Policy. (2017, 1 oktober). Outsourcing Policy Achmea. Geraadpleegd op 31 oktober 2017, van www.achmea.nl/ Outsourcing Policy

Pelckmans, B. (2014). Soorten LAN versus WAN. Geraadpleegd op 12 februari 2018, van http://methodes.pelckmans.be

Pinkelephant. (2017a). De Cloud Risk Assessment. Geraadpleegd op 20 september 2017, van https://www.pinkelephant.nl/it-management-consulting/process/cloud-risk-assessment/

Pinkelephant. (2017b). Wat is een Community Cloud? Geraadpleegd op 13 september 2017, van https://www.pinkelephant.nl/cloud/cloud-computing/typen-cloud-computing/community-cloud/

Rouse, M. (2012). Browse definitions by topic [Community Cloud]. Geraadpleegd op 4 oktober 2017, van http://searchcloudstorage.techtarget.com/definition/community-cloud

Rouse, M. (2017). Metered services (pay-per-use). Geraadpleegd op 13 september 2017, van http://searchcio.techtarget.com/definition/metered-services

Salesforce. (2017). Waarom overstappen op de cloud. Geraadpleegd op 19 september 2017, van https://www.salesforce.com/nl/blog/2015/12/waarom-overstappen-op-de-cloud---10-voordelen-van-cloud-computin.html

SBIFormaat. (2015). Het CBP houdt toezicht op de naleving. Geraadpleegd op 6 oktober 2017, van https://www.sbiformaat.nl/kennisbank/college-bescherming-persoonsgegevens

Syntrus Achmea. (2017a). Syntrus Achmea Pensioenbeheer vanaf 1 januari 2018. Geraadpleegd op 6 september 2017, van https://www.syntrusachmea.nl/nl/Default.aspx

Syntrus Achmea. (2017b). Gespecialiseerde vermogensbeheerder in vastgoed en hypotheken. Geraadpleegd op 6 september 2017 van http://www.achmeavastgoed.nl

Swaen, B. (2017a, 10 juni). Kwalitatief vs kwantitatief onderzoek. Geraadpleegd op 27 september 2017, van https://www.scribbr.nl/onderzoeksmethoden/kwalitatief-vs-kwantitatief-onderzoek/

Swaen, B. (2017b, 3 augustus). Validiteit in je scriptie. Geraadpleegd op 19 september 2017, van https://www.scribbr.nl/onderzoeksmethoden/validiteit-van-scriptieonderzoek/

Taskforce. (2014, 13 november). Taskforce dataclassificatie. Geraadpleegd op 21 januari 2018, van https://www.cip-overheid.nl/wp-content/uploads/2015/03/BID-Operationale-producten-BIR-010-Dataclassificatie-1.0.pdf

Tubbing, L. (2016, 12 juni). Validiteit en betrouwbaarheid. Geraadpleegd op 19 september 2017, van https://deafstudeerconsultant.nl/afstudeertips/onderzoeksmethoden/validiteit-en-betrouwbaarheid/

Unit4. (z.d.). Cloud computing – betekenis van de belangrijkste termen. Geraadpleegd op 20 september 2017, van http://www.unit4.com/nl/betekenis-cloud

Van der Toolen, H., & Wang, W. (2015). *Programmeren voor Dummies.* Amsterdam, Nederland: Pearson Education Benelux.

Van der Valk, W. (2017). Opdrachtomschrijving Zeist Nederland geraadpleegd op 21-9-2017

Van Hoof, J. (2010, 9 september). Cloud Computing: Het concept ontrafeld. Geraadpleegd op 12 september 2017, van http://www.xr-magazine.nl/artikelen/536/cloud-computing/cloud-computing-het-concept-ontrafeld

Van Lanen, M. (2017, 2 juni). Inductief én deductief analyseren bij kwalitatief onderzoek: het geheel is meer dan de delen. Geraadpleegd op 27 september 2017, van https://www.tijdschriftkwalon.nl/inhoud/tijdschrift_artikel/KW-15-1-8/Inductief-n-deductief-analyseren-bij-kwalitatief-onderzoek-het-geheel-is-meer-dan-de-delen

Verhoeven, N. (2011). *Wat is onderzoek?* (4de druk). Amsterdam, Nederland: Boom Lemma.

Vohradsky, D. (2017). Cloud Risk. 10 principles for a Framework for Assessment. Geraadpleegd op 18 oktober 2017, van https://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx

Vraaghetdepolitie.nl. (2017). Wat is Ransomware? Geraadpleegd op 18 december 2017, van https://www.vraaghetdepolitie.nl/pesten-en-geweld/chantage/wat-is-ransomware.html

WINX ICT. (2012, 22 juni). Cloud Computing. Geraadpleegd op 12 februari 2018, van http://winxx.nl/cloudcomputing

Woonfonds. (2017). Verzekeringen. Geraadpleegd op 6 september 2017, van https://www.woonfonds.nl/verzekeringen#

Zilveren Kruis. (2017). De zorgverzekering van Zilveren Kruis. Geraadpleegd op 6 september 2017, van https://www.zilverenkruis.nl/consumenten/zorgverzekering/Paginas/default.aspx

Zorgverzekeraar OZF. (2017). Onze zorgverzekeringen op een rij geraadpleegd op 6 september 2017 van https://www.ozf.nl/consumenten/zorgverzekering/Paginas/default.aspx

Blokdyk, G. (september 2017) Enterprise Information Security Architecture. London Engeland. Createspace Independent Publishing Platform

Tijhaar, W. (augustus 2013) Finance en risk management. Amsterdam. Noordhoff Uitgevers B.V.

Bijlage

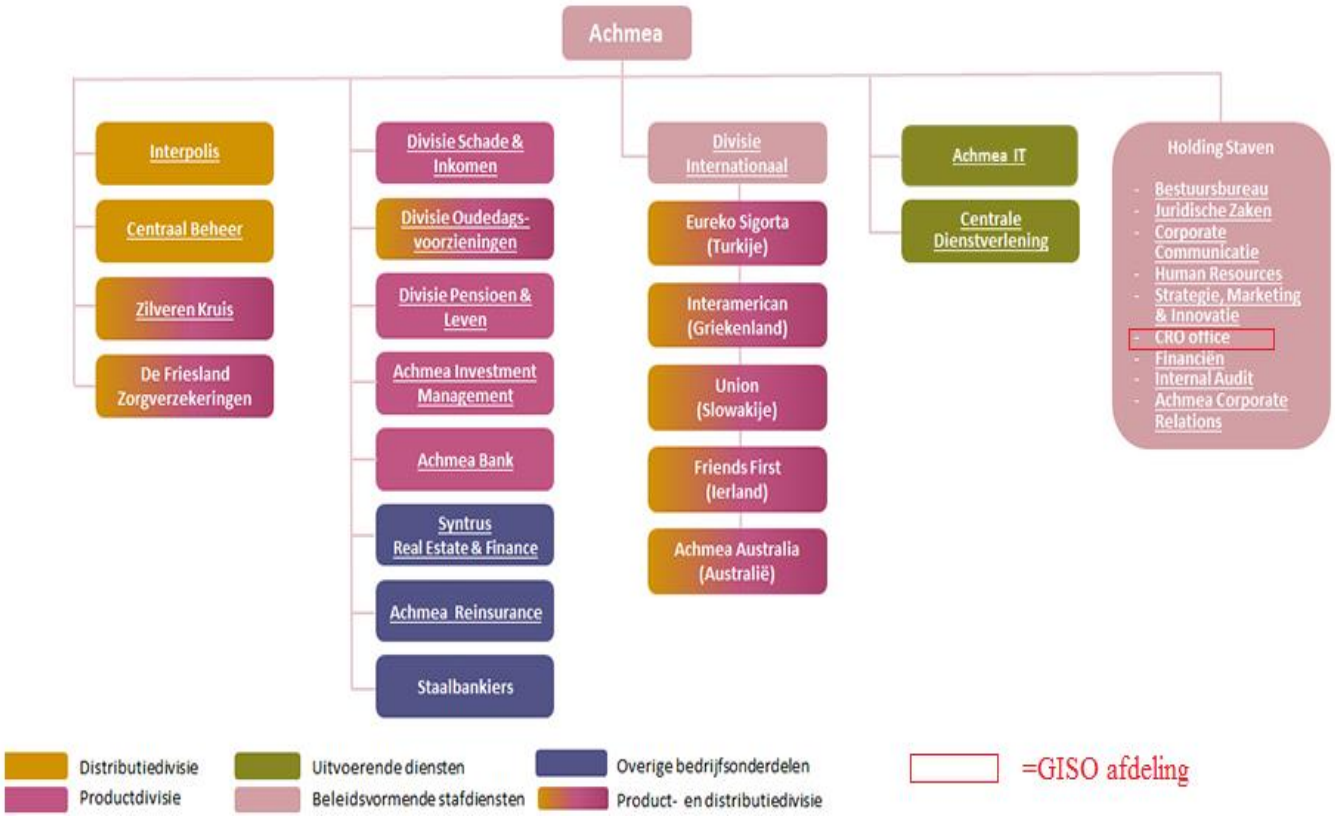
Voor de bijlage 4: Interview Enterprise Security Architect en bijlage 5 Interview Operational Risk Manager wordt er doorverwezen naar het document getranscribeerde interviews.

Bijlage 1: Huidige merken van Achmea

De huidige merken waarbij mensen en ondernemers terecht kunnen voor verzekeringen op het gebied van zorg en schade of het inkomen veilig te stellen zijn(Achmea 2017):

- Zilveren Kruis
  - Een zorgverzekeraar (Zilveren Kruis, 2017).
- Centraal Beheer
  - Particulieren en bedrijven kunnen hier terecht voor financiële producten en diensten zoals; schade- en inkomensverzekeringen, pensioenen, hypotheken, spaar- en beleggingsproducten(Centraal Beheer, 2017).
- Interpolis
  - De Interpolis is een verzekeraar voor vervoer, reizen, toekomst, zorg en gezin, wonen en zakelijk (Interpolis, 2017).
- FBTO
  - FBTO biedt verzekeringen aan voor vervoer, wonen, zorg, rechtsbijstand en overlijden (FBTO, 2017).
- Avéro Achmea
  - Avéro Achmea bieden verzekeringen voor zorg, Vervoer & vrije tijd, Wonen & gezin en inkomen (Avero Achmea, 2017).
- Inshared
  - Inshared biedt verzekeringen voor vervoer, wonen, dieren, reizen, rechtsbijstand en ongevallen (Inshared, 2017).
- Syntrus Achmea
  - Syntrus Achmea voeren pensioenregelingen uit voor een bedrijfstak, beroepsgroep of onderneming. Ook zijn ze gespecialiseerd in vermogensbeheer (vastgoed en hypotheken) (Syntrus Achmea 2017b).
- Hagelunie
  - Hagelunie is een organisatie die zich specialiseert in verzekeringen voor de glastuinbouwspecialisten. Een aantal voorbeelden van objecten die verzekerd kunnen worden zijn; kassen, gewassen, gebouwen en bedrijfsmiddelen. Tevens geeft de organisatie preventietips voor de glastuinbouwindustrie (Hagelunie, 2017).
- Zorgverzekeraar OZF
  - Een zorgverzekeraar (Zorgverzekeraar OZF, 2017).
- Woonfonds
  - Woonfonds verstrekt verzekeringen voor overlijden en beleggen. Tevens geeft het adviezen/ informatie over hypotheken en woongenot(Woonfonds, 2017).

Bijlage 2 Organogram



Bijlage 3 Het Cloud Risk Assessment

referentie	Operational Risks
DNB01	Lock-in
DNB02	Loss of Governance
DNB03	Compliance challenges (i.e. right tovexamine, exit clause, privacy acy etc.)
DNB04	Loss of business reputation due to cotenant activities
DNB05	Cloud service termination or failure
DNB06	Cloud provider acquisition
DNB07	Supply chain failure
DNB08	Changing regulations
DNB09	Insufficient skills and knowledge to identify risks related to Outsourcing / Cloud computing
	Technical Risks
DNB10	Resource exhaustion; under or over provisioning
DNB11	Isolation failure
DNB12	Cloud provider malicious insider — abuse of high privilege roles
DNB13	Management interface compromise
DNB14	Intercepting data in transit
DNB15	Data leakage on up/download, intra-cloud
DNB16	Insecure or ineffective deletion of data
DNB17	DDOS
DNB18	EDOS
DNB19	Loss of encryption keys
DNB20	Undertaking of malicious probes or scans
DNB21	Compromise service engine
DNB22	Conflicts between customer hardening procedures and cloud environment
	Compliance Risks
DNB23	Right to audit for supervisors
DNB24	Subpoena and e-Discovery
DNB25	Where is the data
DNB26	Risk from changes of jurisdiction
DNB27	Data protection risks
DNB28	Specific local data privacy
DNB29	Risk of conflicting regulations
DNB30	Exit clausule in contract
DNB31	Licensing risks
	General NOT Cloud Specific Risks
DNB32	Network breaks
DNB33	Network management
DNB34	Modifying network traffic
DNB35	Privilege escalation
DNB36	Social engineering attacks
DNB37	Loss or compromise of operational logs
DNB38	Loss or compromise of security logs
DNB39	Backups lost, stolen
DNB40	Unauthorized access to premises
DNB41	Theft of computer equipment
DNB42	Natural disasters
DNB43	Conflict of interest
DNB44	Bandwidth limitations

Bijlage 4 Interview Enterprise Security Architect

Vragen interview Enterprise security architect	
Algemeen	Bent u met een nieuw Cloud beleid bezig?
	Op welke wijze is het Cloud beleid opgesteld?
	Wordt er vanuit het risico naar de maatregel geredeneerd (zoals in de DNB 44 risico's)?
	Wat doet u als de organisatie geen certificering heeft?
	Wie doet de Cloud uitbesteding auditen?
	Is de Cloud checklist met de risico's ook bedoelt voor mensen die de Cloud Risk Assessment daadwerkelijk gaan uitvoeren (of gebeurt dit door de audit)?
Probleem	Wat is de onderverdeling in de verschillende soorten risico's?
	Wat is het belang van een Cloud security beleid?
	Kan het zo zijn dat de Clouddienst wordt afgenomen terwijl de beleidsdocumenten niet overeenkomen?
	Op basis van wat is de norm vastgesteld?
Oorzaak	Wordt de Cloud checklist door iedereen binnen Achmea op dezelfde wijze gebruikt?
	Op welke wijze wordt er bepaalt dat iets vanuit de SAAS wordt uitbesteed?
	Op welke wijze worden de risico's geïdentificeerd?
	Vindt u dat de Cloud Risk Assessment en de checklist de risico's voldoende identificeren?
Oplossingen	Op welke wijze kan ervoor gezorgd worden dat er meer duidelijkheid komt over het gebruik van de Cloud checklist?
	Wat zou u veranderen aan de Cloud checklist?
	Is het mogelijk om de Cloud risico's (uit het Cloud Risk Assessment) af te stemmen op een bepaalde uitbesteding?

Bijlage 5 Interview Operational Risk Manager

Vragen Operational Risk Manager	
Algemeen	De Enterprise security Architect heeft een beleid vastgesteld, in hoeverre heeft dit invloed op de uitbestedingen?
	Heeft de checklist invloed op het uitbestedingsbeleid?
	Kan er een onderscheid worden gemaakt in uitbestedingen?
	Is er een beleid beschreven over hoe risico's te kwalificeren?
Probleem	Wanneer is een uitbesteding een Cloud?
	Kan een risicochecklist worden aangepast op een uitbesteding?
	Hoe wordt de mate van de kritiekheid van een risico bepaald?
	Is er voldoende kennis bij de mensen die de checklist moeten invullen?
Oorzaak	Hoe wordt er in de praktijk omgegaan met uitbestedingen?
	Wat is de reden dat er verschillende soorten checklist in omloop zijn?
	Wat zijn de verantwoordelijkheden van de persoon die de uitbesteding wil gaan doen?
	Op welke wijze wordt een uitbesteding met de bijbehorende risico's beoordeeld?
Oplossingen	Op welke wijze kan ervoor gezorgd worden dat er meer duidelijkheid komt op welke wijze de Cloud checklist gebruikt moet worden?
	Wat zou u veranderen aan de Cloud checklist?
	Is het mogelijk om de risico's af te stemmen op een bepaalde uitbesteding?

Bijlage 6 Excel sheet Afstemming

referentie	Operational Risks		Geen invloed op Cloud	Beschikbaarheid	Integriteit	Vertrouwelijkheid	SAAS	AIV (ART. 40)	SA	BO
DNB01	Lock-in	Risk of not being able to migrate easily from one provider to another		X	X	X	X	x	x	x
DNB02	Loss of Governance	Control and influence on the cloud providers, and conflicts between customer hardening procedures and the cloud environment.		X	X	X	X	x	x	x
DNB03	Compliance challenges (i.e. right tovexamine, exit clause, privacy acy etc.)	The risk of Cloud Providers which cannot provide evidence of compliancy to all relevant requirements, policies, laws etc.			X	X	X	x	x	x
DNB04	Loss of business reputation due to contenant activities	Risk of malicious activities carrie dout by one tenant affecting the reputation of another tenant			X	X	X	x	x	
DNB05	Cloud service termination or failure	Ths risk of providers going out of business. The risk of unclear data ownership.		X	X	X	X	x	x	x
DNB06	Cloud provider acquisition	Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk.		X			X	x	x	
DNB07	Supply chain failure	A cloud provider can outsource certain specialized tasks of its 'production' chain to third parties. The risk of non-compliancy of those subcontractors.		X	X	X	X	x	x	x
DNB08	Changing regulations	The risk of changes in laws and regulations could impact the requirements for both the financial institution and the cloud provider. Changes in regulations could aslo impact the risks for the Otso.			X	X	X	x	x	
DNB09	Insufficient skills and knowledge to identify risks related to Outsourcing / Cloud computing	If the financial institution has insufficient knowledge to identify the risks involved or to assess the operational effectiveness of the controls at the Cloud SP outsourcing is not allowed. Monitoring outsourcing requires specific skills and knowledge.			X	X	X	x	x	x
	Technical Risks								x	
DNB10	Resource exhaustion; under or over provisioning	There is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections.		X	X	X	X		x	
DNB11	Isolation failure	This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure.		X	X	X	X	x	x	x
DNB12	Cloud provider malicious insider – abuse of high privilege roles	The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees.		X	X	X	X	x	x	x
DNB13	Management interface compromise	The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.			X	X	X	x	x	x
DNB14	Intercepting data in transit	Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be con-sidered as possible threat sources.			X		X	x	x	x
DNB15	Data leakage on up/download, intra-cloud	Data leakage from inside or outside the cloud provider is a major reputational risk for the financial institution. The contract must contain a section in which the financial institution is informed by the cloud provider in case of any relevant data leakage.			X	X	X	x	x	x
DNB16	Insecure or ineffective deletion of data	The risk of data being available beyond the lifetime specified in the security policy. (i.e. not wiped/deleted securely enough).		X			X	x	x	x
DNB17	DDOS	Distributed denial of service attacks could lead to: unavailability, identity theft, integrity failures etc. Contract should contain a section in which the financial institution is informed in case of a DDOS		X	X	X	X	x	x	x
DNB18	EDOS	as 17, but with the effect of Cloud customer going bankrupt or stolen from.		X	X	X	X	x	x	x
DNB19	Loss of encryption keys	Loss or disclosure of secret keys (SSL, file encryption, customer private keys, etc) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorised use for authentication and nonrepudiation (digital signature).			X	X	X	x	x	x
DNB20	Undertaking of malicious probes or scans	Collect information in the context of a hacking attempt. A possible impact could be a loss of confidentiality, integrity and availability of service and data.		X	X	X		x	x	x
DNB21	Compromise service engine	Risk of compromise the highly specialized platform, the service engine located above the physical hardware resources and manages customer resources.				X		x	x	x
DNB22	Conflicts between customer hardening procedures and cloud environment	Risk of not being able to comply to the hardening procedures of the client, as well as differences between or unclear segregation of responsibilities.			X		X	x	x	x

	Compliance Risks									
DNB23	Right to audit for supervisors	Risk of not being compliant to regulation; In the contract the right to examine/audit for DNB must be granted without any limitations to this right. The right also applies for sub- contractors in the chain. If there is an adjustment (new sub contractor) in the chain, the institution needs to be informed.					**X**	**x**	**x**	**x**
DNB24	Subpoena and e-Discovery	The risk of disclosure of centralized storage as well as shared physical hardware, to unwanted parties.			**X**	**X**	**X**	**x**	**x**	**x**
DNB25	Where is the data	It should be clear where data is stored. This applies also for backup data in a vault locaction and replicated data in a secundary or third datacenter. Also an financial institution needs to know whether the data is traveling between data centers or if the data stays in one datacenter.			**X**	**X**	**X**	**x**	**x**	**x**
DNB26	Risk from changes of jurisdiction	Change in location of data could lead to different jurisdiction, laws and regulations.				**X**	**X**	**x**	**x**	**x**
DNB27	Data protection risks	The risk of not being able to validate if data is handled in a lawfull way. Compliant to regulations like privacy laws, as well as encryption standards apply.				**X**	**X**	**x**	**x**	**x**
DNB28	Specific local data privacy	The risk that other law and regulations apply at the location where the datacenter is situated compared to where the contract party is situated; http://www.cbpweb.nl/Pages/med_20120703_europeseopinie-cloudcomputing.aspx				**X**	**X**	**x**	**x**	**x**
DNB29	Risk of conflicting regulations	Laws and regulations due change on a regular basis. The risks exist the cloud provider cannot to comply to both regulations.				**X**	**X**	**x**	**x**	**x**
DNB30	Exit clausule in contract	The contract must contain an exit-clause. The exit clause should contain f.i. the way data is threated, time lines, etc.				**X**	**X**	**x**	**x**	**x**
DNB31	Licensing risks	Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment.		**X**	**X**	**X**	**X**	**x**	**x**	
	General NOT Cloud Specific Risks							x	x	
DNB32	Network breaks	Due to misconfiguration, system or OS vulnerabilities, lack of resource isolation or lack of, or a poor and untested, business continuity and disaster recovery plan.		**X**			**X**	**x**	**x**	**x**
DNB33	Network management	This could dramatically effect network uptime, experience, up-time and service delivery.		**X**		**X**	**X**	**x**	**x**	**x**
DNB34	Modifying network traffic	This could affect data integrity, loss and alteration of sensitive information. Eventually this will evolve as a reputational risk.			**X**	**X**	**X**	**x**	**x**	**x**
DNB35	Privilege escalation	This could lead to access to information or parts of the system normally not accessible to these users.			**X**	**X**	**X**	**x**	**x**	**x**
DNB36	Social engineering attacks	Due to lack of security awareness, user provisioning vulnerabilities, lack of resource isolation, communication encryption vulnerabilities, inadequate physical security procedures.			**X**	**X**	**X**	**x**	**x**	**x**
DNB37	Loss or compromise of operational logs	Due to lack of policy or poor procedures for logs collection and retention, vulnerabilities, lack of forensic readiness, system or OS vulnerabilities.		**X**	**X**	**X**	**X**	**x**	**x**	**x**
DNB38	Loss or compromise of security logs	Due to lack of policy or poor procedures for logs collection and retention, vulnerabili-ties, user provisioning vulnerabilities, user de-provisioning vulnerabilities, lack of forensic readiness, system or OS vulnerabilities.		**X**	**X**	**X**	**X**	**x**	**x**	**x**
DNB39	Backups lost, stolen	Due to inadequate physical security procedures, vulnerabilities, user provisioning vul-nerabilities, user de-provisioning vulnerabilities.			**X**	**X**		**x**	**x**	**x**
DNB40	Unauthorized access to premises	Due to inadequate physical security procedures. Since cloud providers concentrate resources in large data centres, and although the physical perimeter controls are likely to be stronger, the impact of a breach of those controls is higher.			**X**	**X**	**X**	**x**	**x**	**x**
DNB41	Theft of computer equipment	Due to inadequate physical security procedures.	**Minst relevant**					**x**	**x**	
DNB42	Natural disasters	Generally speaking, this risk from natural disasters is lower compared to traditional infrastructures because cloud providers usually offer multiple redundant sites and network paths by default.	**Minst relevant**					**x**	**x**	
DNB43	Conflict of interest	Large cloud providers could use their resources as well as all the data stored on centralized storage, for other purposes.			**X**	**X**	**X**	**x**	**x**	**x**
DNB44	Bandwidth limitations	The number of intercontinental data lines is limited. A break in one or more of these lines could impact the availability and the performance.		**X**			**X**	**x**	**x**	