Cloud voor financiële instellingen

Iets nieuws onder de zon?

Auteur P. Heffels
In opdracht van Dhr. J.J.M. Nijland, Directeur Group Internal Audit, APG

Datum Juni 2016

Zuyd Hogeschool

Cloud voor financiële instellingen

Iets nieuws onder de zon?

Auteur	P. Heffels
Studentnummer	1236172
Onderwijsinstelling	Zuyd Hogeschool, faculteit Management & Recht
Studie	Hogere Juridische Opleiding
Profiel	Algemeen Juridisch uitstroomprofiel
Opdrachtgever	Dhr. J. Nijland, Directeur Group Internal Audit, APG
Opdrachtbegeleiding	Dhr. R. Ronken, Auditor 4, GIA/ICT& Diensten, APG
Afstudeermentor	Dhr. mr. M.J.P. Hennissen
Eerste afstudeerdocent	Dhr. mr. M.J.P. Hennissen
Tweede afstudeerdocent	Mevr. mr. L.L.C. Habets-Theunissen
Afstudeerperiode	Februari 2016 – juni 2016
Plaats	Oirsbeek
Datum	7 juni 2016

Inhoudsopgave

Dankwoord

Zo, het zit er bijna op. Na vier jaar studeren is het einde binnen handbereik. Het is nog niet allemaal klaar, maar het indienen van de scriptie voelt wel een beetje als het afronden van de studie.

Vier jaar geleden zag mijn wereld er heel anders uit: De economie was belabberd en ik had al zeker drie reorganisaties “overleefd” bij mijn toenmalige werkgever. Zou ik de volgende reorganisatie ook “overleven”? Wat als de nieuwe eigenaar van het bedrijf besluit om de hele vestiging te sluiten? Hoe sterk sta ik in de arbeidsmarkt als ik met mijn huidige collega’s in dezelfde vijver van werkgelegenheid zou moeten vissen? Ik had geen HBO diploma en als het laatste scenario werkelijkheid zou worden, dan schatte ik mijn kansen slecht in met mijn leeftijd en zonder diploma. Misschien was het verstandig om een “plan B” te hebben?

Eigenlijk had ik al langere tijd een studie willen volgen maar is het er nooit van gekomen. Huwelijk, verhuizing, kinderen, andere werkgever, verbouwing … noem maar op, er is altijd wel een goede reden om niet te kiezen voor een langdurig traject zoals een studie. Toen het studeren weer mijn aandacht had, was het natuurlijk de vraag welke studie ik dan zou willen gaan volgen. Weer “iets” in de IT? Nee, daar had ik geen zin meer in. Als ik dan zou gaan studeren dan moest het ook iets nieuws zijn; iets waar ik weinig van af wist en graag meer over zou willen weten.

Al zoekende kwam ik op het spoor van de Hogere Juridische Opleiding. Rechten? Op HBO niveau? Ik wist helemaal niet dat dat mogelijk was. Tot mijn stomme verbazing was het zelfs mogelijk om de studie in deeltijd te volgen bij een hogeschool dicht in de buurt. Heel erg lang heb ik niet meer hoeven nadenken over mijn keuze: Rechten, dat zou het worden!

De rest is bijna geschiedenis.

Ik heb een prachtige tijd achter de rug met een fantastische groep klasgenoten! We zijn met zestien personen begonnen aan de opleiding en de sfeer was vanaf de eerste dag erg goed! Helaas zijn er een aantal personen afgehaakt of overgestapt door de jaren heen waardoor de groep nog slechts zes personen telt, maar wat een hechte groep!

Je staat er niet direct bij stil maar door de jaren heen heb ik mijn klasgenoten vaker gezien dan mijn familie en vrienden. In het eerste jaar twee avonden per week en de jaren daarop minimaal één middag/avond kwam je bij elkaar voor het volgen van colleges, elkaar te coachen of aan groepsopdrachten samen te werken. Dat ga ik zeker missen. Wat ik eigenlijk wil zeggen: Mijn klasgenootjes, die ga ik missen!

Ik had deze studie nooit kunnen afronden zonder de hulp van velen, die mij bewust of onbewust, geholpen hebben. Mijn buren bijvoorbeeld die onbewust geholpen hebben door pakketjes met studieboeken aan te nemen omdat er niemand thuis was. Zovelen onbewust, door hun waardering uit te spreken omdat ik het toch maar mooi volhield, die het een knap staaltje vonden wat ik deed of mijn studie gebruikten als voorbeeld tegenover hun schoolgaande kinderen die klaagden over hoe druk ze het hadden. Hun steun heeft mij zeker gesterkt om het vol te houden.

Die steun had ik ook nodig want volhouden was niet eenvoudig bij tijd en wijle. De rest van de wereld draait gewoon door en de studie komt daar bovenop. Het was zeker niet eenvoudig om ’s avonds en in weekenden motivatie en inspiratie te vinden om toch maar weer naar het studiekamertje te gaan en te lezen, opdrachten uit te werken, werkstukken te

maken of te leren voor tentamens. Zo'n studie is een trein die doordendert en het is zaak om aan boord te blijven want anders wordt het heel erg moeilijk.

Voor het mogelijk maken om al die jaren mijn stage binnen APG te kunnen lopen wil ik graag Arnold Dissel, Leo Bessems, Jeroen Spijkers, Harrie Alberti en Wil Scheijvens van harte bedanken! Ik zal vooral nooit vergeten hoe Harrie op een zondagochtend het beoordeelde competentiedossier op de fiets bij mij thuis kwam brengen!

Een bijzonder woord van dank dient uit te gaan naar Wil Scheijvens. Aan de start van de studie was ik ingehuurd door Wil en nu aan het einde is hij mijn manager. Dank voor al die jaren waarin je mij hebt gesteund, dank voor je instemming dat ik mijn stage kon combineren met mijn inzet bij APG, maar vooral dank voor het vertrouwen dat je in mij hebt gesteld om geen misbruik te maken van de uitzonderlijke situatie dat een inhuurkracht tegelijk stage loopt bij zijn opdrachtgever!

Dank voor Roel Ronken die mij heeft begeleidt bij het uitvoeren van het afstudeeronderzoek. Roel wist precies waar ik tegenaan liep bij het zoeken naar een onderwerp en heeft mij meteen met raad en daad bijgestaan. Het was Roel die mij op het juiste spoor heeft gezet, een opdrachtgever is gaan zoeken en contacten heeft gelegd voor het uitvoeren van de interviews. Als ik niet meer vooruit kwam dan kon ik altijd terecht bij Roel en na een begripvol en stimulerend gesprek kon ik gemotiveerd weer verder.

Toch zijn de echte helden in dit verhaal mijn vrouw Elsie en dochter Dennise! Zij zijn de huisgenoten die de echte offers hebben opgebracht. Offers van een partner of een vader die nauwelijks tijd voor ze had, die alsmaar in zijn kamertje zat te studeren, voor wie de planning aangepast moest worden omdat het weer tentamentijd was, of die zaken uitstelde totdat de studie het toeliet. Ondanks alles waren zij het die mij stimuleerden op momenten waar ik het zelf niet meer zag zitten, waar ik het zat was om iedere avond te studeren en waar ik liever andere dingen deed waardoor ik uiteindelijk in tijdnood zou komen. Op die momenten was het vooral Elsie die me een beetje uitdagend vroeg of ik al klaar was met studeren, die mij met een empathische blik en een begripvol knikje naar het studeerkamertje stuurde en die werkelijk nooit, maar dan ook nooit geklaagd heeft over mijn afwezigheid! Schat, ik hou van je! Zonder jou was het me niet gelukt!

1 Introductie

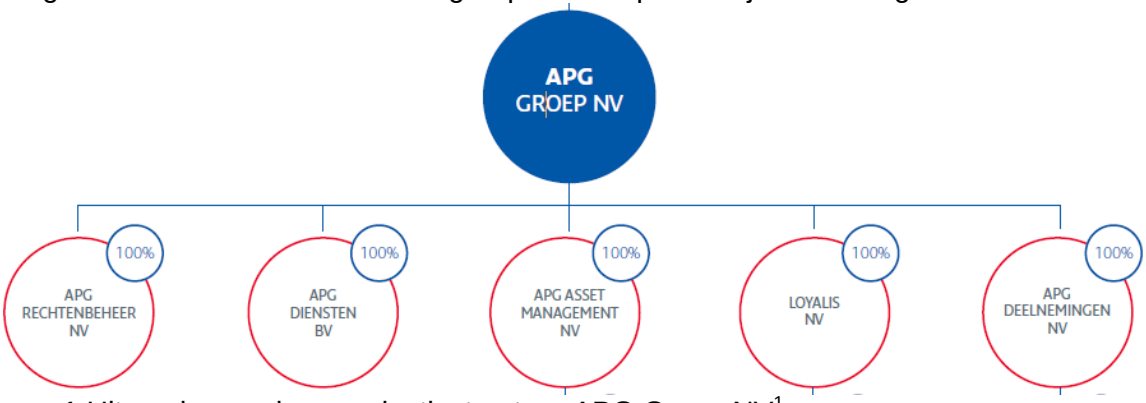
De reden voor het uitvoeren van dit onderzoek is gelegen in de opgedane ervaringen met betrekking tot het afnemen van Cloud-diensten en de verschillende manieren waarop daarnaar wordt gekeken. Die verschillen komen met name naar voren tijdens het uitvoeren van het beoordelingstraject (de zogenaamde “risicoanalyse”) naar de geschiktheid van de Cloud-aanbieder.

Door die verschillende interpretaties van hetgeen daadwerkelijk uitgevoerd moet worden is de indruk ontstaan dat er onnodig zware trajecten worden doorlopen. Tijd dus om te onderzoeken wat er nu echt gedaan moet worden zodat iedereen weet wat er wordt verwacht.

De opdrachtgever voor dit onderzoek is de heer J. Nijland, Directeur Group Internal Audit en de dagelijkse begeleiding is verzorgt door de heer R. Ronken, Auditor 4 GIA/ICT&Diensten, beiden vanuit APG. Het onderzoek is specifiek gericht op de situatie van APG maar feitelijk van toepassing op alle direct en/of indirect onder toezicht staande financiële instellingen.

APG Groep NV verricht binnen het bedrijfsonderdeel APG Rechtenbeheer NV voor verschillende pensioenfondsen een mix van pensioenadministratie, vermogensbeheer, bestuursadvisering, pensioencommunicatie en werkgeversdiensten. Voor deze werkzaamheden is APG de partij waaraan het betreffende pensioenfonds haar uitvoeringswerkzaamheden heeft uitbesteed. Daarnaast is APG een beleggingsinstelling (APG Asset Management NV), premiepensioeninstelling en verzekeraar (Loyalis NV).

De organisatiestructuur van de APG groep ziet er op hoofdlijnen als volgt uit:



Figuur 1 Uitsnede van de organisatiestructuur APG Groep NV[1]

1.1 Probleembeschrijving

Vanuit wettelijk oogpunt is het een onder toezicht staande onderneming toegestaan om werkzaamheden uit te besteden aan derden, zolang wordt voldaan aan de verplichtingen die de toezichthouders opleggen[2].

[1] APG Groep NV 2016, p. 11
[2] Zie hoofdstuk 3 (Wettelijke basis, toezicht en uitbesteding).

De sancties die een toezichthouder kan opleggen bij het niet nakomen van deze verplichtingen zijn divers en graderen van een normoverdragend gesprek of waarschuwing (mogelijk zelfs openbaar gepubliceerd) en het opleggen van boetes[3] tot het intrekken van de vergunning en zelfs aangifte bij het Openbaar Ministerie[4].

Het niet voldoen aan de wettelijke eisen bij uitbesteding kan dus leiden tot (hoge) boetes en zelfs intrekking van de vergunning. Het opleggen van dergelijke maatregelen kan niet alleen leiden tot financiële problemen maar ook tot imagoschade en voortzettingsrisico's voor de onderneming. Vooral in een onzekere pensioenmarkt, waarbij de conjuncturele ontwikkelingen en een mogelijke herziening van de regierol van de overheid kan leiden tot verdere commercialisering van de pensioenmarkt[5], dienen dergelijke risico's voorkomen te worden.

Figuur 1: Overzicht scenario's uit Kaal & Koomans, PBM 2016/2, p. 25-28

Met het uitbrengen van de circulaire Cloud computing in 2011[6] heeft De Nederlandse Bank (DNB) nader aangegeven wat hij verwacht van onder toezicht staande organisaties op het gebied van uitbesteding naar Cloud-diensten en heeft inmiddels diverse richtlijnen en hulpmiddelen ter beschikking gesteld om een risicoanalyse uit te kunnen voeren. DNB hanteert daarbinnen echter open normen en laat de invulling c.q. uitwerking daarvan over aan de onder toezicht staande organisaties.

Deze open normen zorgen voor onzekerheid bij uitbesteding waardoor het risico bestaat dat onnodig zware eisen worden gesteld aan aanbieders om te voorkomen dat non-conformiteit optreedt. Hierdoor wordt wellicht een voor alle partijen onnodig belastend inkooptraject doorlopen en beperkt een onder toezicht staande onderneming zichzelf in de mogelijkheden die Cloud-diensten bieden.

Naast de onzekerheid over het correct invullen van open normen speelt ook de vraag hoe hiermee moet worden omgegaan wanneer partijen waaraan werkzaamheden zijn uitbesteed zelf ook weer gebruik maken van onderaannemers? Het hogere doel blijft een beheerste en integere bedrijfsvoering, ongeacht hoeveel onderaannemers betrokken zijn bij de uitbesteding van IT diensten.

[3] Voor een voorbeeld van de hoogte van dergelijke boetes zie ECLI:NL:RBROT:2015:5635 waarin veroordeelde werd veroordeeld tot betaling van een boete van € 22.680.000.
[4] Stcrt. 2008, nr. 132, p. 30
[5] Kaal & Koomans, PBM 2016/2, p. 25-28
[6] Chilvers-van der Kruk & Koning, 2011

1.2 Centrale vraag

Op basis van het gestelde in de probleemomschrijving zal dit onderzoek antwoord geven op de volgende centrale vraag:

"Welke eisen worden door DNB en AFM opgelegd aan onder toezicht staande organisaties bij het afnemen van Cloud-diensten en welke risicomitigerende maatregelen moeten worden genomen om te voldoen aan deze eisen in het algemeen en specifiek wanneer sprake is van onderaanneming bij de aanbieder van de Cloud-dienst?"

1.3 Deelvragen

Om de centrale vraag te kunnen beantwoorden zijn een aantal deelvragen geformuleerd die tezamen het antwoord vormen.

1. Wat zijn Cloud-diensten?
2. Wat is de wettelijke basis waarop eisen worden gesteld aan het gebruik van Cloud-diensten?
3. Welke eisen worden gesteld door toezichthouders bij het gebruik van Cloud-diensten?
4. Welke risicomitigerende maatregelen moeten worden genomen in het algemeen?
5. Welke risicomitigerende maatregelen moeten worden genomen wanneer sprake is van onderaanneming?

1.4 Onderzoeksmethode

Het onderwerp Cloud heeft betrekking op een hele keten van wetgever, toezichthouders, onder toezicht staande organisaties en Cloud-aanbieders. Ieder aspect in die keten is betrokken geworden in het onderzoek. Gelet op aard van het onderwerp en de relatieve korte beschikbaarheid daarvan is gekozen voor een kwalitatief onderzoek.

Om de deelvragen te kunnen beantwoorden is een combinatie van methodes nodig geweest. De eerste twee vragen zijn door een literatuurstudie onderzocht.

Voor het beantwoorden van vraag 3 is een combinatie van literatuuronderzoek en interviews gebruikt. Het onderzoek heeft plaatsgevonden door het afnemen van een semigestructureerd interview met een toezichthouder. Het interview moest zorgen voor het verhogen van de kwaliteit van het literatuuronderzoek door bevestiging te krijgen over de compleetheid of zelfs aanvullingen daarop. Die kwalitatieve slag was nodig om inzichtelijk te maken of de toezichthouders hun beleid en eisen daaromtrent hebben uitgevoerd naar de bedoelingen daarover van de wetgever.

Voor het beantwoorden van de deelvragen 4 en 5 zijn voornamelijk semigestructureerde interviews met partijen in de keten van toezicht gevoerd, gebaseerd op vooraf uitgevoerd literatuuronderzoek.

De interviews zijn samenvattend getranscribeerd zodat de inhoud direct bruikbaar is in het rapport en daarmee een duidelijke link ontstaat tussen het interview en de resultaten. De uitwerkingen zijn toegevoegd als bijlagen.

De volgende interviews zijn uitgevoerd:

Naam	Functie	Organisatie	Perspectief
Mevr. I. Talsma	Toezichthouder ICT	DNB	Organisatie belast met het toezicht op financiële instellingen en pensioenfondsen
Dhr. F. Toebosch	Hoofd Interne Beheersing	ABP	a) Onder toezicht staande organisatie b) Uitbesteder van uitvoeringswerkzaamheden c) Uitbesteder aan Cloud-diensten
Dhr. M. Boerekamp	Lid Raad van Bestuur	APG	a) Onder toezicht staande organisatie b) Aannemer van uitvoeringswerkzaamheden c) Uitbesteder aan Cloud-diensten
X	Directeur Global Compliance & Integrity	XYZ	a) Onder toezicht staande organisatie b) Uitbesteder aan Cloud-diensten

Na het afnemen van het interview is gevraagd of de naam van geïnterviewde en/of de naam van de instelling gebruikt mochten worden in het rapport. Daarbij is afgesproken dat ze eerst voorzien werden van de uitwerking van het interview voordat ze definitief akkoord gaven. In één geval is dat akkoord, door oorzaken buiten het interview of de inhoud van de uitwerking daarvan om uitgebleven, waardoor deze geanonimiseerd is opgenomen in dit rapport.

De beantwoording van de onderzoeksvraag is voor een groot deel gebaseerd op antwoorden uit de interviews. Daarom zal in het rapport regelmatig verwezen worden naar antwoorden daaruit. Voor de leesbaarheid zal voor het verwijzen naar de interviews gebruik worden gemaakt van een verkorte aanduiding volgens het formaat “<Instelling>, <Vraagnummer>”, wat vervolgens verwijst naar het gegeven antwoord op de desbetreffende vraag behorend tot het interview dat is afgenomen bij betreffende instelling.

1.5 Leeswijzer

Dit rapport volgt qua indeling de structuur van de deelvragen. In hoofdstuk 2 wordt een uitleg gegeven over Cloud-diensten en de relevantie met uitbesteden besproken.

In hoofdstuk 3 worden de resultaten van het onderzoek naar de wettelijke basis voor toezicht op het gebruik van Cloud-diensten weergegeven.

In hoofdstuk 4 staan de eisen die worden gesteld aan uitbesteding, gekeken vanaf de wetgever en zoals die zijn uitgewerkt door de toezichthouders.

Hoofdstuk 5 geeft een overzicht van maatregelen die een financiële instelling moet nemen bij uitbesteding aan Cloud-diensten in het algemeen.

In hoofdstuk 6 worden eventuele additionele maatregelen besproken in het geval dat de aannemende partij zelf ook weer (delen van) zijn dienstverlening heeft uitbesteedt en de effecten daarvan voor het financiële stelsel.

Tenslotte worden in hoofdstuk 7 de conclusies getrokken en aanbevelingen gedaan.

2 Cloud-diensten

Alvorens een beschrijving te geven van Cloud-diensten is het belangrijk om de relatie met uitbesteding duidelijk te maken.

2.1 Uitbesteding

In dit onderzoek wordt de definitie van “uitbesteding” gehanteerd uit artikel 1 van de Beleidsregel uitvoering pensioenwet en Wet verplichte beroepspensioenregeling (Bupw):

Uitbesteden: Het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:
a. die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of
b. die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan;

Mr. Drs. P. Laaper zet in zijn proefschrift[7] uiteen welke drie cumulatieve criteria zijn te onderkennen die de reikwijdte van de uitbestedingsregels bepalen:
1. De dienstverlener is “een derde”.
2. De uitbesteding betreft “eigen werkzaamheden” van het pensioenfonds. Dat kunnen ook ondersteunende werkzaamheden zijn.
3. De uitbesteding betreft “wezenlijke werkzaamheden”. Daarbij gelden kernactiviteiten zonder meer als “wezenlijk”. De afbakening is vooral van belang bij ondersteunende werkzaamheden.

Daaruit blijkt dat niet alle uitbesteding gemeld moet worden aan de toezichthouders, zoals bijvoorbeeld het uitbesteden van de catering. Dit soort uitbestedingen moeten uiteraard wel degelijk uitgevoerd worden zodat de uitbestedende partij geen risico’s loopt. Een voorbeeld daarvan kan het eisen van een verklaring omtrent gedrag (VOG) zijn van iedere werknemer van de leverende partij.

2.2 Cloud

DNB hanteert de definitie voor Cloud-diensten[8] zoals vastgelegd in de standaard[9] van het “National Institute of Standards and Technology” (NIST):
“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”

De drie service modellen waarover gesproken wordt in de definitie zijn: Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). De vier implementatiemodellen zijn: Private -, Community -, Public - en Hybrid Clouds[10].

[7] Laaper 2015, p. 33
[8] DNB, Open Boek Toezicht, http://www.toezicht.dnb.nl/2/5/50-230433.jsp
[9] NIST SP 800-145, p. 2
[10] NIST SP 800-145 beschrijft ook nog vijf essentiële karakteristieken maar die zijn, wegens hun technische karakter, voor dit onderzoek niet van belang.

In het kort zeggen de service modellen iets over de manier waarop de functionaliteit ter beschikking wordt gesteld en de mate van invloed op c.q. verantwoordelijkheid over de infrastructuur en zeggen de implementatiemodellen iets over het gebruik en de locatie van de dienst.

In dit onderzoek wordt onder infrastructuur verstaan: Het geheel van hardware (server, opslag en netwerk componenten) en software (applicaties of programmeerbare interfaces) die tezamen de Cloud-dienst vormen.

2.2.1 Cloud service modellen

Software as a Service (SaaS) houdt in dat de Cloud-aanbieder applicatiefunctionaliteit beschikbaar stelt aan de eindgebruiker. De gebruiker heeft geen weet van (of enige beheertaken op) de onderliggende infrastructuur en zal hoogstens enkele specifieke configuratie instellingen moeten beheren. Daartegenover staat dat de geboden applicatie doorgaans weinig ruimte biedt voor klantspecifieke functionaliteit (maatwerk).

Voorbeelden van SaaS diensten zijn: Microsoft Office 365 (Office 2016, Sharepoint, Skype for Business, etc.), Google Apps (Gmail, Agenda, Drive, etc.) en Salesforce.

Bij **Platform as a Service (PaaS)** krijgt de klant de beschikking over een set hulpmiddelen om zelf applicaties te ontwikkelen op de infrastructuur van de Cloud-aanbieder, of eigen verworven applicaties te draaien. De klant hoeft de onderliggende infrastructuur niet te kennen of te beheren maar heeft wel controle over de applicaties en de omgeving waarin deze zich bevindt.

Voorbeelden van PaaS diensten zijn: Microsoft Azure, Force.com en ServiceNow.

Bij **Infrastructure as a Service (IaaS)** kan de klant gebruik maken van infrastructuurcomponenten (verwerkingscapaciteit, dataopslag, etc.) van de Cloud-aanbieder om zelf besturingssystemen en applicaties te installeren. De klant beheert zelf de systemen vanaf het besturingssysteem maar hoeft geen weet te hebben van de dieperliggende infrastructuur.

Het meest bekende voorbeeld van IaaS is Amazon Web Services (AWS).

2.2.2 Cloud implementatiemodellen

Bij een **Private Cloud** wordt de infrastructuur uitsluitend door één organisatie geëxploiteerd. Het beheer daarvan kan door de organisatie zelf, een externe partij, of een combinatie daarvan plaatsvinden. Dit geldt ook voor de locatie van de infrastructuur. Deze kan bij de organisatie zelf staan maar ook bij een derde partij (bijvoorbeeld een hostingprovider). In dit model heeft het publiek geen toegang tot de dienst en maakt de organisatie op geen enkele wijze gebruik van een publieke Cloud-dienst.

Een **Community Cloud** richt zich op een specifieke groep gebruikers die gelijke doelstellingen (zoals bijvoorbeeld missie, beleid, informatiebeveiliging of compliance regels) nastreven. Het beheer kan bij een organisatie, derde partij of combinatie daarvan liggen. Dit geldt ook voor de locatie van de infrastructuur.

Bij een **Public Cloud** staat de dienst ter beschikking voor gebruik door het algemene publiek. Iedereen kan gebruik maken van de dienst. Het eigendom, beheer en exploitatie van de dienst kan liggen bij een particulier bedrijf, academische organisatie, de overheid of een combinatie daarvan.

Een **Hybrid Cloud** is een combinatie van twee of meer Private -, Community - of Public Cloud-diensten waarbij de unieke entiteiten blijven bestaan maar onderling zijn verbonden waardoor gegevens en applicaties heen en weer verplaatst kunnen worden. De onderliggende infrastructuren kunnen op de eigen locatie of bij derden ondergebracht en in beheer zijn. Een Hybrid Cloud is een “smeltvorm” van de andere implementatiemodellen, inclusief de mogelijke verschijningsvormen van locatie, beheer en exploitatie.

2.3 Relatie tussen Cloud-diensten en uitbesteding

Op basis van de beschrijving van Cloud-diensten is kenmerkend dat er altijd een bepaalde dienst wordt afgenomen van een aanbieder. Daarbij maakt het gehanteerde servicemodel uit waar in de infrastructuur de invloed van de gebruiker stopt. De implementatiemodellen geven vervolgens aan voor wie de infrastructuur beschikbaar is en de mate waarin de dienst gedeeld wordt met andere gebruikers.

	SaaS	PaaS	IaaS
Private	1	2	3
Community	4	5	6
Public	7	8	9
Hybrid	10	11	12

Wanneer de verschillende implementatiemodellen in een tabel worden afgezet tegen de verschillende servicemodellen, dan wordt duidelijk dat er alleen op basis van die indeling al 12 varianten kunnen bestaan. In werkelijkheid kunnen dat er meer zijn omdat er combinaties kunnen bestaan en er ook andere servicemodellen worden aangeboden, al is de vraag of die modellen niet een variant van één van de bestaande modellen is. In iedere variant is de mate van controle (“span of control”) verschillend voor de uitbestedende organisatie. De verantwoordelijkheid voor de dienst “schuift” als het ware tussen de aanbieder en afnemer van de dienst bij de verschillende varianten.

De variatie in de soorten dienstverlening en de variaties in verantwoordelijkheden maakt dat het afnemen van Cloud-diensten een bijzondere vorm van uitbesteding is. Daaruit volgt eveneens dat de maatregelen die financiële instellingen moeten nemen om de risico’s te beheersen voor iedere variant weer anders zijn.

Het kan echter nog complexer worden: Uit de beschrijving van de service modellen blijkt in ieder geval dat er altijd sprake is van één derde bij het afnemen van Cloud-diensten; de aanbieder van de Cloud-dienst. De implementatiemodellen gaan echter nog veel verder en geven aan dat delen van de dienst ook uitgevoerd c.q. geleverd kunnen worden door andere partijen dan die Cloud-aanbieder.

In termen van uitbesteding is het niet alleen de financiële instelling die een dienst afneemt van een Cloud-aanbieder en daarmee een uitbesteding doet, maar kan de Cloud-aanbieder zelf ook weer werkzaamheden hebben uitbesteed. Hierdoor kan een complexe keten van verantwoordelijkheid ontstaan, in vakkringen “Cloud stacking” genoemd, waarvoor de onder toezicht staande organisatie uiteindelijk eindverantwoordelijk blijft en doorlopend, aantoonbaar “in-control” moet zijn.

3 Wettelijke basis, toezicht en uitbesteding

De huidige pensioenwet is als voorstel van wet[11] ingediend in december 2005 en na behandeling door de beide Kamers in werking getreden op 1 januari 2007[12, 13].

3.1 Beheerste en integere bedrijfsvoering

Dit onderzoek kijkt specifiek naar het huidige artikel 143 lid 1 en lid 2 aanhef en sub a Pensioenwet (Pw)[14], wat luidt:

Artikel 143. Beheerste en integere bedrijfsvoering

1. Een pensioenfonds richt zijn organisatie zodanig in dat deze een beheerste en integere bedrijfsvoering waarborgt.
2. Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot het eerste lid. De regels hebben in ieder geval betrekking op:
    a. het beheersen van bedrijfsprocessen en bedrijfsrisico's;
    b. integriteit;
    c. de soliditeit van het pensioenfonds, waaronder wordt verstaan:
        1°. het beheersen van financiële risico's; en
        2°. het beheersen van andere risico's die de soliditeit van het pensioenfonds kunnen aantasten;
    d. het beheersen van de financiële positie over de lange termijn door periodiek een haalbaarheidstoets te maken.

Om de wetgeving voor de beroepspensioenregelingen in gelijke pas te houden met de Pensioenwet is een gelijkluidend artikel 138 opgenomen in de Wet verplichte beroepspensioenregelingen. Om dezelfde reden is de formulering van dit artikel zelf weer grotendeels gebaseerd op artikel 2:45 eerste en tweede lid[15] van het wetsvoorstel Wet op het financieel toezicht (Wft)[16].

Met betrekking tot lid 1 wordt toegelicht in de Memorie van Toelichting[17]:
"Het is van belang dat het pensioenfonds zelf een analyse maakt van de risico's en daarnaar zijn taakuitvoering inricht. Het pensioenfonds kan zelf bepalen welke maatregelen moeten worden getroffen gelet op de risico's die het loopt. Een beheerste uitvoering is ook van belang voor een efficiënte en effectieve uitvoering van het toezicht. Een beheerste uitvoering levert betrouwbare rapportages op: het systeem van maatregelen en procedures waarborgt de kwaliteit van de output."

In de memorie van toelichting staat over artikel 143 lid 2 sub a[18] toegelicht dat regels worden gesteld *"(…) met betrekking tot de algemene aspecten van de bedrijfsvoering die zien op het beheersen van processen en risico's."* en dat beheersen *"(…) omvat het gehele traject van plannen, besturen, monitoren en bijsturen van doelstellingen en processen."*

De inhoud van dit artikel is (op punten) verschillende keren gewijzigd tijdens de parlementaire behandeling en door de jaren heen. Voor de leden die van belang zijn voor dit onderzoek beperkt de aanpassing zich tot de aanvulling "in ieder geval" in de aanhef

[11] Kamerstukken II 2005/2006, 30413, 2
[12] Stb. 2006, 707
[13] Delen van de Pensioenwet die verder geen betrekking hebben op dit onderzoek zijn per 1 januari 2008 en 1 januari 2009 in werking getreden.
[14] In het oorspronkelijke wetsvoorstel was dit artikel 131. Als gevolg van wetswijzigingen is het tegenwoordig artikel 143. In dit rapport zal verder worden gesproken van artikel 143.
[15] Het huidige artikel 3:17 Wft.
[16] Kamerstukken II 2004/2005, 29708, 10, p. 22
[17] Kamerstukken II 2005/2006, 30413, 3, p. 264
[18] Kamerstukken II 2005/2006, 30413, 3, p. 264

van lid 2. In de parlementaire behandeling is slechts weinig te vinden over de tekst van artikel 143 lid 2 sub a Pw en de aanvulling die voor het eerst terug komt in het gewijzigd voorstel van wet[19] lijkt uit te willen drukken dat de risicoaspectgebieden van het artikel geen uitputtende lijst is.

Daar waar de artikelen 143 Pw en 138 Wet verplichte beroepspensioenregelingen verplichtingen opleggen ten aanzien van een beheerste en integere bedrijfsvoering voor pensioenfondsen, doen de artikelen 3:17 en 4:14 Wft dat voor andere financiële instellingen zoals banken, premiepensioeninstellingen, verzekeraars (allen in artikel 3:17 Wft) en beleggingsinstellingen en pensioenbewaarders (beiden in artikel 4:14 Wft).

Het onderscheid tussen de wetgeving voor pensioenfondsen en andere financiële instellingen komt met name tot uitdrukking in het toezicht daarop.

3.2 Toezicht

Door de uitvoeringswerkzaamheden uit te besteden aan APG dient het pensioenfonds zich ervan te vergewissen dat deze uitbestede werkzaamheden op een beheerste en integere manier plaatsvinden zodat het pensioenfonds aan haar wettelijke verplichting voldoet. Het toezicht door de AFM en DNB is primair gericht op het pensioenfonds en daarmee staan APG Rechtenbeheer N.V. en APG Asset Management N.V. als contractpartner voor deze werkzaamheden onder indirect toezicht.

Daarnaast is APG zelf ook een financiële onderneming in de zin van de Wet op het financieel toezicht (Wft) door als beleggingsinstelling (APG Asset Management N.V.), premiepensioeninstelling (APG PPI) en verzekeraar (Loyalis N.V.) actief te zijn. Voor het verlenen van deze financiële diensten staat APG onder direct toezicht.

Volledigheidshalve dient in de specifieke situatie van APG nog vermeld te worden dat met de combinatie van beleggen en verzekeren binnen een groep (APG Groep N.V.), APG ingevolge artikel 2 sub 14 van de Richtlijn 2002/87/EG wordt aangemerkt als Financieel Conglomeraat (FiCo) en daardoor onder direct toezicht van DNB staat. Deze vorm van toezicht wordt echter expliciet buiten het kader van dit onderzoek gehouden.

De wet onderkent verschillende vormen van toezicht. De Pw kent een onderverdeling in gedragstoezicht, prudentieel toezicht en materieel toezicht, terwijl de Wft alleen gedragstoezicht en prudentieel toezicht kent.

3.2.1 Gedragstoezicht

In artikel 151 lid 2 Pw en artikel 146 lid 2 Wet verplichte beroepspensioenregeling[20] wordt de volgende definitie gehanteerd voor gedragstoezicht:
"Gedragstoezicht is toezicht gericht op de naleving van de normen ten aanzien van voorlichting door pensioenuitvoerders aan deelnemers, gewezen deelnemers, gewezen partners en pensioengerechtigden en de normen ten aanzien van de advisering van de deelnemer of gewezen deelnemer bij de uitvoering van premieovereenkomsten met beleggingsvrijheid waarbij de deelnemer of gewezen deelnemer de verantwoordelijkheid voor de beleggingen heeft overgenomen."

In het kort ziet het gedragstoezicht in het kader van de pensioenwetgeving toe op de voorlichting en advisering door pensioenuitvoerders.

[19] Kamerstukken II 2005/2006, 30413, 18, p. 13
[20] De Wet verplichte beroepspensioenregeling spreekt echter van "premieregelingen" in plaats van "premieovereenkomsten".

In artikel 1:25 Wft staat de volgende definitie van gedragstoezicht:
"Gedragstoezicht is, mede in het belang van de stabiliteit van het financiële stelsel, gericht op ordelijke en transparante financiële marktprocessen, zuivere verhoudingen tussen marktpartijen en zorgvuldige behandeling van cliënten."

Het verschil met de gehanteerde definitie in de Pw en Wet verplichte beroepspensioenregeling zit in de werking van het toezicht. Daar waar deze toezien op de relatie tussen pensioenuitvoerder en deelnemer, ziet de Wft toe op de marktprocessen en de verhoudingen tussen partijen. In het algemeen kan gesteld worden dat gedragstoezicht toeziet op de vraag hoe partijen zich gedragen in de markt.

Op basis van de artikelen 151 lid 1 Pw, 146 lid 1 Wet verplichte beroepspensioenregeling en 1:25 lid 2 Wft is de AFM belast met het gedragstoezicht.

3.2.2 Prudentieel toezicht

Prudentieel toezicht is in artikel 151 lid 4 Pw en artikel 146 lid 4 Wet verplichte beroepspensioenregeling[21] als volgt gedefinieerd:
"Prudentieel toezicht is toezicht gericht op de normen ten aanzien van de financiële soliditeit van pensioenfondsen en het bijdragen aan de financiële stabiliteit van de sector van pensioenfondsen."

In artikel 1:24 lid 1 Wft luidt de definitie van prudentieel toezicht:
"Prudentieel toezicht is gericht op de soliditeit van financiële ondernemingen en de stabiliteit van het financiële stelsel."

Ook hier is het verschil in werking te zien tussen de pensioenwetgeving en de andere financiële ondernemingen. Inhoudelijk ziet het prudentieel toezicht op de financiële stabiliteit van partijen en de sector waarin zij opereren.

Op basis van de artikelen 151 lid 3 Pw, 146 lid 3 Wet verplichte beroepspensioenregeling en 1:24 lid 2 Wft is DNB belast met het prudentieel (en materieel) toezicht.

3.2.3 Materieel toezicht

Materieel toezicht komt alleen voor in de pensioenwetgeving en wordt in artikel 151 lid 5 Pw en artikel 146 lid 5 Wet verplichte beroepspensioenregeling gedefinieerd als:
"Materieel toezicht is toezicht gericht op alle normen in deze wet die geen onderdeel uitmaken van gedrags- of prudentieel toezicht."

Met deze definitie wordt het materieel toezicht gepositioneerd als "kapstok" voor zaken waarbij niet expliciet vaststaat of ze onder gedrags- of prudentieel toezicht horen.

Op basis van de artikelen 151 lid 3 Pw en 146 lid 3 Wet verplichte beroepspensioenregeling is DNB belast met het materieel (en prudentieel) toezicht.

[21] De Wet verplichte beroepspensioenregeling spreekt echter van "beroepspensioenfondsen" in plaats van "pensioenfondsen".

3.3 Toezicht op een beheerste en integere bedrijfsvoering

Op het punt van een beheerste bedrijfsvoering heeft de Raad van State in haar advies en nader rapport op het wetsvoorstel Pensioenwet[22] gezegd:
"Prudentieel toezicht is, in lijn met de definitie in de Wft, gedefinieerd als het toezicht op de normen gericht op de financiële soliditeit van pensioenfondsen en financiële stabiliteit van de sector van pensioenfondsen. Het gaat hierbij vooral om normen die erop gericht zijn dat een pensioenfonds aan zijn financiële verplichtingen richting deelnemers, gewezen deelnemers en pensioengerechtigden kan voldoen. Toezicht op normen ten aanzien van beheerste bedrijfsvoering horen hier bij."

Op basis hiervan kan geconcludeerd worden dat het toezicht op een beheerste bedrijfsvoering onderdeel uitmaakt van het prudentieel toezicht en daarom is opgedragen aan DNB.

3.4 Uitbesteding

Uitbesteding van uitvoeringswerkzaamheden door pensioenfondsen is mogelijk gemaakt in de artikelen 34 Pw en 43 Wet verplichte beroepspensioenregeling. Nadere regels over het uitbesteden zijn voor beide wetten vastgelegd in hoofdstuk 4 Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling.

Bepalingen met betrekking tot uitbesteding van werkzaamheden in het kader van de Wft zijn vastgelegd in artikel 3:18 Wft. Nadere regels hiervoor zijn vastgelegd in hoofdstuk 5 Besluit prudentiële regels Wft en hoofdstuk 6 Besluit Gedragstoezicht financiële ondernemingen Wft.

Voordat er gekeken kan worden naar de eisen die bij uitbesteding worden opgelegd is het van belang om een afbakening toe te passen. De wet ziet toe op het gehele scala van uitbesteding, inclusief het volledig door een derde laten uitvoeren van "eigen" werkzaamheden. Bijvoorbeeld het laten uitvoeren van de gehele pensioenuitvoering. Het gebruik van Cloud-diensten valt hier niet onder. Cloud-aanbieders bieden IT diensten waarmee een instelling haar eigen werkzaamheden kan uitvoeren. De instelling blijft verantwoordelijk voor de uitvoering van de werkzaamheden en de Cloud-aanbieder biedt daarvoor een platform en een zekere mate van dienstverlening aan, afhankelijk van het gekozen service- en implementatiemodel[23].

[22] Kamerstukken II, 2005/2006, 30413, 4, p. 12-13
[23] Zie paragraaf 2.3 (Relatie tussen Cloud-diensten en uitbesteding).

4 Eisen bij uitbesteding

4.1 Eisen vanuit de wetgever

De eisen die vanuit de wetgever zijn opgelegd met betrekking tot uitbesteding en zoals vastgelegd in hoofdstuk 4 van het Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling, hoofdstuk 5 Besluit prudentiële regels Wft en hoofdstuk 6 Besluit Gedragstoezicht financiële ondernemingen Wft hebben betrekking op de volgende aspect gebieden:

1. werkzaamheden die niet mogen worden uitbesteed,
2. vormvereisten voor de overeenkomst tot uitbesteding,
3. beheersing van de risico's.

In de volgende paragrafen worden de specifieke eisen nader uitgewerkt. Daarbij zal de eis zo generiek mogelijk worden beschreven en kan de feitelijk inhoud van de desbetreffende artikelen enigszins afwijken. Tevens worden niet alle eisen uitputtend weergegeven. Alleen de eisen die betrekking hebben op de specifieke situatie van APG als pensioenuitvoerder, vermogensbeheerder, premiepensioeninstelling en verzekeraar worden meegenomen en alleen voor zover ze van toepassing zijn op het afnemen van Cloud-diensten.

4.1.1 Werkzaamheden die niet mogen worden uitbesteed

Eisen	**H4**	**H5**	**H6**
Werkzaamheden waarvan uitbesteding de verantwoordelijkheid van de uitvoerder voor de organisatie en beheersing van bedrijfsprocessen en het toezicht daarop kan ondermijnen	Art 12 onder b		
Indien de uitbesteding een belemmering kan vormen voor een adequaat toezicht op de naleving van het bij of krachtens de wet bepaalde	Art 12 onder c	Art 27 lid 1	Art 37
Een instelling gaat niet over tot het uitbesteden van werkzaamheden indien dat afbreuk doet aan de kwaliteit van haar onafhankelijke interne toetsing		Art 28	Art 38b

Het is bijzonder in deze op te merken dat het Besluit Gedragstoezicht financiële ondernemingen Wft (H6) niet direct een verbod legt op het uitbesteden van bepaalde werkzaamheden maar de verplichting oplegt om de uitbesteding geen afbreuk te laten doen. In die zin wijkt de opzet van dit besluit af ten opzichte van de andere besluiten.

4.1.2 Vormvereisten voor de overeenkomst tot uitbesteding

Eisen	**H4**	**H5**	**H6**
Een instelling legt de overeenkomst met de derde waaraan de werkzaamheden worden uitbesteed schriftelijk vast.	Art 13 lid 1	Art 31 lid 1	Art 38e lid 1
Daarin wordt in ieder geval vastgelegd:	**H4**	**H5**	**H6**
Welke werkzaamheden worden uitbesteed onder verwijzing, indien mogelijk, naar de administratieve organisatiebeschrijving van de instelling, alsmede de voorwaarden waaronder de uitbesteding plaatsvindt	Art 13 lid 2 sub a		

Eisen	H4	H5	H6
De informatie-uitwisseling tussen de instelling en de derde	Art 13 lid 2 sub c	Art 31 lid 2 sub a	
De verplichting voor de derde om informatie waar de toezichthouder ter uitvoering van zijn wettelijke taak om vraagt rechtstreeks aan de toezichthouder ter beschikking te stellen	Art 13 lid 2 sub d	Art 31 lid 2 sub a	Art 38l onder a
De mogelijkheid voor de instelling om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt	Art 13 lid 2 sub e	Art 31 lid 2 sub b	Art 38l onder b
De verplichting voor de derde om de instelling in staat te stellen blijvend te voldoen aan het bij of krachtens de wet bepaalde	Art 13 lid 2 sub f	Art 31 lid 2 sub c	Art 38l onder c
De mogelijkheid voor de toezichthouder om onderzoek ter plaatse te doen of te laten doen bij de derde	Art 13 lid 2 sub g	Art 31 lid 2 sub d	
De wijze waarop de overeenkomst wordt beëindigd, en de wijze waarop wordt gewaarborgd dat de instelling de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere derde kan laten uitvoeren	Art 13 lid 2 sub h	Art 31 lid 2 sub e	Art 38l onder b

De vormvereisten zoals opgelegd vanuit het Besluit Gedragstoezicht financiële ondernemingen Wft (H6) kunnen alleen maar worden afgeleid. Het besluit stelt zelf geen eisen aan onderwerpen die in een overeenkomst vastgelegd moeten worden maar eist maatregelen die wel schriftelijk vastgelegd moeten worden om effect te kunnen hebben.

Een ander groot verschil is dat in het Besluit Gedragstoezicht financiële ondernemingen Wft (H6) rechtstreeks eisen worden gesteld aan de derde die getoetst kunnen worden door de uitbestedende partij, terwijl de andere twee besluiten verplichtingen opleggen aan de uitbestedende partij om bepaalde maatregelen te nemen.

4.1.3 Beheersing van de risico's

Eisen	H4	H5	H6
Een instelling draagt zorg voor een systematische analyse van de risico's die samenhangen met de uitbesteding van werkzaamheden en legt deze vast. De instelling maakt de analyse op het niveau van zijn eigen organisatie in zijn geheel en op het niveau van de onderscheiden bedrijfsonderdelen	Art 14 lid 1		Art 38c lid 1
Een instelling voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot de uitbesteding van werkzaamheden	Art 14 lid 2	Art 29	Art 38c lid 1
Een instelling hanteert een adequate selectieprocedure voor derden aan wie werkzaamheden worden uitbesteed. De instelling legt vast op grond van welke afwegingen zij tot de keuze voor een bepaalde derde is gekomen	Art 14 lid 3		Art 38c lid 1

Eisen	H4	H5	H6
Een instelling beschikt over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de uitbestede werkzaamheden te kunnen beoordelen	Art 14 lid 4	Art 30	Art 38c lid 1 Art 38l onder a
Een instelling heeft zicht op het beloningsbeleid van de derde aan wie werkzaamheden worden uitbesteed, betrekt het beloningsbeleid bij de keuze voor de derde waaraan de werkzaamheden worden uitbesteed en maakt zijn beleid dienaangaande openbaar	Art 14 lid 5		
Door de uitbesteding de relatie en verplichtingen van de instelling jegens haar cliënten niet worden gewijzigd			Art 38d lid 1 sub b
De voorwaarden waaraan de instelling moet voldoen om een vergunning te verkrijgen en om deze te behouden niet worden ondermijnd			Art 38d lid 1 sub c
Door de uitbesteding geen afbreuk wordt gedaan aan de naleving van voorschriften verbonden aan de vergunning			Art 38d lid 1 sub d
De onderneming beschikt over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen		Art 20 lid 2	

Een bijzonder punt van aandacht gaat uit naar verplichtingen rondom procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen[24]. Deze verplichting is niet opgenomen in de eisen rondom het uitbesteden van werkzaamheden maar komen voort uit de eisen rondom een beheerste uitoefening van het bedrijf in het kader van de Wft.

In het Open Boek Toezicht geeft DNB aan dat deze waarborgen niet vanuit de pensioenwetgeving wordt opgelegd maar desondanks toch van toepassing worden geacht[25]: *"Dit laat onverlet dat DNB van oordeel is dat de overeenkomstige toepasselijkheid voor deze (beroeps)pensioenfondsen van de algemene norm inzake een zodanige organisatie-inrichting dat deze een beheerste en integere bedrijfsvoering waarborgt, met zich brengt dat ook deze instellingen voor zover van toepassing – dat wil zeggen proportioneel toegepast - dienen te beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen."*

4.2 Uitvoering door en afstemming tussen de toezichthouders

Vanuit de wetgever zijn twee verschillende instanties belast met het uitvoeren van prudentieel-, gedrags- en materieel toezicht over de financiële ondernemingen en pensioenuitvoerders. Om die werkzaamheden op elkaar af te stemmen hebben beide partijen het "Convenant Stichting Autoriteit Financiële Markten en De Nederlandsche Bank N.V."[26] afgesloten.

[24] Artikel 20 lid 2 Besluit prudentiële regels Wft.
[25] DNB, Open Boek Toezicht, http://www.toezicht.dnb.nl/2/5/50-230429.jsp
[26] Stcrt. 2007, nr. 130, p. 20

In het convenant zijn (op hoofdlijnen) de volgende afspraken gemaakt:

- Afspraken over het voorkomen van overlap op het raakvlak van toezicht
- Afspraken over het bevorderen van efficiency en doelgerichtheid van de uitvoering van het toezicht
- Afspraken over het gebruik van de beschikbare informatie, expertise en infrastructuur
- Afspraken over de onderlinge afstemming over beleid en regelgeving

In het gezamenlijk uitgegeven "Handhavingsbeleid van de Autoriteit Financiële Markten en De Nederlandsche Bank"[27] worden de verschillende werkwijzen van de toezichthouders toegelicht, de uitgangspunten die zij ten grondslag leggen aan het handhavingsbeleid, welke factoren een rol spelen bij de inzet van hun handhavingsinstrumenten en hoe de toezichthouders daarover verantwoording afleggen.

Over de wijze waarop AFM inhoud geeft aan het toezicht staat in het handhavingsbeleid:
"Voor de AFM is hierbij het zogeheten bijdragemodel een centraal instrument. Het bijdragemodel is een self-assessment op basis van een vragenlijst die periodiek door onder toezicht staande ondernemingen wordt ingevuld, waarbij die ondernemingen hun eigen bijdrage aan de doelstellingen van de voor hen relevante wet- en regelgeving beoordelen. Daarnaast hanteert de AFM andere vormen van self-assessment."

Over de manier waarop DNB dat doet staat er :
"DNB hanteert een risicoanalysemodel (het zogeheten FIRM model: Financiële Instellingen Risicoanalyse Methode), waarmee de belangrijkste risico's van onder toezicht staande ondernemingen worden geïdentificeerd. De toezichthouders zetten hun toezichtcapaciteit vooral in op risico's, die op basis van de gehanteerde modellen als hoogste naar voren komen."

Aangezien de beheerste bedrijfsuitvoering valt binnen het prudentieel toezicht, zal de uitvoering daarvan uitsluitend worden benaderd vanuit het DNB perspectief, waarbij het gestelde rondom de eisen met betrekking tot de voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens[28] van toepassing wordt geacht op de (beroeps)pensioenfondsen.

4.2.1 Invloed van Cloud-diensten op de organisatie

DNB is een organisatie, net als iedere andere organisatie, die zich moet aanpassen aan de veranderende wereld om zich heen. Het fenomeen Cloud-diensten heeft tot een verschuiving van de aandacht geleidt en daar moet DNB zich op (her)inrichten. Dat inrichten is een continu proces dat altijd een beetje achter de feiten aan loopt; mogelijkheden tot verdere optimalisaties worden pas zichtbaar nadat er op zijn minst een beetje "pijn" verwacht wordt of al is gevoeld.

Dat blijkt ook uit de reactie van DNB[29]. In eerste instantie werd door de financiële instellingen terughoudend gereageerd op de mogelijkheden die Cloud-diensten bieden. Met name de onduidelijkheid over de manier waarop risico's kunnen worden beheerst heeft geleidt tot die terughoudendheid. In die tijd keek DNB wel naar Cloud-diensten, maar dat beperkte zich tot individuele expertise. Het werd "erbij" gedaan, naast de reguliere werkzaamheden. Naarmate de volwassenheid van de Cloud-diensten toenam en daarmee ook de interesse van de financiële instellingen, is DNB in gesprek gegaan met verschillende serviceproviders en heeft nader onderzoek verricht.

[27] Stcrt. 2008, nr. 132, p. 30
[28] Artikel 20 lid 2 Besluit prudentiële regels Wft.
[29] DNB, vraag 2.

Volgens DNB[30] is het gebruik van Cloud-diensten sinds het uitbrengen van de circulaire aanzienlijk toegenomen. Daarnaast heeft ook het van kracht worden van het nieuwe risicogebaseerde toezichtraamwerk voor verzekeraars, Solvency II, invloed gehad op de sector verzekeringen omdat daarin expliciet(er) de meldingsplicht van voorgenomen uitbesteding is opgenomen. Ook vinden er reparatieacties[31] plaats bij grotere instellingen wat leidt tot tientallen meldingen.

Ook op het gebied van kennis en vaardigheden heeft DNB[32] zich moeten aanpassen. Zeker nu het gebruik van Cloud-diensten steeds meer gemeengoed wordt en vele implementaties gelijktijdig plaatsvinden in de financiële markt, neemt de vraag naar capaciteit ook toe. Er is ook specifieke (technische) ICT kennis nodig om het toezicht effectief uit te kunnen voeren. Er wordt ook gekeken of de huidige sectorale indeling wel het meest optimaal is en DNB stelt zich de vraag hoe de eigen bedrijfsprocessen geoptimaliseerd kunnen worden om het toezicht m.b.t. Cloud-diensten efficiënter uit te kunnen voeren. Tot nu toe is veel aandacht uitgegaan naar het behandelen van meldingen over het afnemen van nieuwe Cloud-diensten, maar DNB moet ook periodiek controleren en mogelijk zelfs optreden; ook dat proces van lopend toezicht moet geoptimaliseerd worden voor het aspect Cloud-diensten. In die zin is DNB als organisatie ook volop in beweging.

Ook de financiële instellingen zelf hebben effecten ondervonden van de opkomst van Cloud-diensten. Volgens APG[33] is het afnemen van Cloud-diensten strikt gezien gewoon een vorm van inkopen. Cloud-diensten zijn daarbij wel wat “ontastbaarder” waardoor het allemaal als een stuk gecompliceerder wordt gezien. Er zal een strakke regie gevoerd moeten worden om zeker te stellen dat een organisatie aantoonbaar “in-control” is.

Bij het inkopen van Cloud-diensten zullen alle mogelijke operationele en tactische risico’s afgetikt moeten worden en op die activiteit zal heel hard op gestuurd moeten worden. Feitelijk is het niet anders dan intern een systeem hosten maar de sturing vind niet meer plaats tussen afdelingen maar met externe partijen.

Een organisatie moet wel klaar zijn om Cloud-diensten in te kunnen zetten. Voor de dienstverlening is een organisatie afhankelijk van een externe partij. Voorbeelden hierbij zijn de gehanteerde “software lifecycle” en “maintenance cycles” van de aanbieder. Afhankelijk van de dienstverlener heeft een afnemer wel enige “speelruimte”, maar over het algemeen zal deze mee moeten kunnen bewegen met de kalender van de aanbieder. Voorheen was er nog de mogelijkheid om een upgrade te verplaatsen naar een ander onderhoudsweekend, of het onderhoudsweekend zelf te verplaatsen. Bij Cloud-diensten wordt er voorgeschreven wanneer een organisatie naar een nieuwe versie moet en de organisatie moet daarin kunnen meebewegen. Een organisatie moet veel strakker en beter plannen bij Cloud-diensten en wanneer een organisatie veel verschillende Cloud-diensten gebruikt kan dat best een uitdaging zijn.

In kort hangt het succesvol gebruik van Cloud-diensten af van het correct invullen van de regiefunctie daarover.

[30] DNB, vraag 7.
[31] Hiermee wordt het achteraf melden van het gebruik van Cloud-diensten bedoeld.
[32] DNB, vragen 3 en 4 gecombineerd.
[33] APG, vraag 2.

4.2.2 Toezicht op het gebruik van Cloud-diensten

Vanuit de wettelijke mogelijkheid, vastgelegd in de Wft, om regelgeving vast te stellen m.b.t. de wijze waarop en de voorwaarden waaronder wijzigingen mogen worden uitgevoerd, heeft DNB[34] in december 2011 de “Circulaire cloud computing”[35] uitgebracht. De doelstelling daarvan was om duidelijkheid te geven aan de instellingen hoe omgesprongen diende te worden met Cloud-diensten. Bewustwording creëren dat hier sprake is van uitbesteding, maar wel van een nieuwe vorm van uitbesteding waarvoor maatregelen genomen moeten worden voor de additionele risico’s (waar is de data, hoe krijg ik mijn data terug etc.).

Een van de bepalingen in de circulaire is dat wezenlijke veranderingen vooraf gemeld dienen te worden. Wanneer DNB in het lopend toezicht moet constateren dat Cloud-diensten worden ingezet voor wezenlijke bedrijfsprocessen en dan pas kan beoordelen of de risico’s afdoende zijn gemitigeerd, is te laat, de contracten zijn immers al getekend en de dienst in gebruik. Zaken die in ieder geval geregeld moeten zijn, zijn onder andere het “right-to-examine” door DNB, de mogelijkheid om het contract aan te kunnen passen bij een wijziging in de wet- of regelgeving en het hebben van een exit-strategie en plan.

Gezien[36] het grote aantal financiële instellingen die gebruik maken van Cloud-diensten hanteert DNB de aanpak om grotere instellingen direct te controleren en het toezicht op kleinere instellingen thema-gebaseerd uit te voeren. Bij het laatste wordt een bepaald onderwerp (bijvoorbeeld “right-to-examine” in contracten van grote aanbieders en het hebben van een “exit-strategie”) uitgelicht en nader bekeken. DNB[37] geeft “best practices” uit en deelt resultaten van eigen onderzoeken. Door die thema-gebaseerde aanpak van DNB zou afgeleid kunnen worden op welk aspect de focus zou kunnen komen te liggen in het toezicht.

Naast de circulaire[38] heeft DNB een sjabloon uitgegeven met daarin een aantal risico’s en risicogebieden dat financiële instellingen kunnen gebruiken om aan te tonen dat ze daarin volledig zijn geweest en de restrisico’s voldoende gemitigeerd c.q. formeel geaccepteerd hebben. Gezien de aard van Cloud-diensten is het vrijwel onmogelijk om geen restrisico’s te hebben. In het kader van risico gebaseerd toezicht is het van belang om aan te tonen dat er voldoende aandacht is geweest voor restrisico’s en dat ze zo goed mogelijk worden gemitigeerd. De financiële instelling blijft verantwoordelijk voor het restrisico.

Ook heeft DNB met een aantal Cloud-aanbieders afspraken gemaakt over het “right-to-examine” door DNB. Daardoor hoeft niet iedere financiële instelling daarover afzonderlijk afspraken te maken met desbetreffende aanbieders, wat overigens niet in de weg staat om zelf afspraken te maken met andere aanbieders. De afspraken die DNB heeft gemaakt moeten dan ook als een hulpmiddel worden gezien (financiële instelling kan vragen voor de met DNB afgestemde standaardpassage in het contract) en zeker niet als “sturend” worden opgevat om marktinvloed te voorkomen.

Voor het samenstellen van hulpmiddelen (zoals bijvoorbeeld het sjabloon) maakt DNB gebruik van standaarden en raamwerken van “National Institute of Standards and Technology” (NIST), “European Union Agency for Network and Information Security” (ENISA), “Information Security Forum” (ISF) en “Control Objectives for Information and

[34] DNB, vraag 2.
[35] Chilvers-van der Kruk & Koning, 2011
[36] DNB, vraag 3.
[37] ABP, vraag 11.
[38] DNB, vraag 5.

related Technology" (COBIT). Financiële instellingen kunnen deze standaarden zien als een suggestie maar zijn uiteindelijk vrij in de keuze voor een raamwerk of standaard.

Daarnaast voert DNB doorlopend onderzoek uit (thema gebaseerd) en publiceert de resultaten daarvan, tezamen met opgedane kennis en ervaring, in het "Open Boek Toezicht" op de website van DNB.

4.2.3 Afstemming tussen toezichthouders

Naast een algemene waardering voor de goede samenwerking[39] met de toezichthouders, is er verbetering[40] mogelijk in de hoek van stapeling van toezicht en de coördinatie daarvan.

In de afgenomen interviews is per toeval hetzelfde voorbeeld gebruikt om de samenwerking met, en de stapeling van, toezichthouders te illustreren. Daaruit blijkt dat de toezichthouders op verschillende manieren naar de materie kijken en daar hun eigen belang aan hechten.

In het verleden[41] heeft zich de situatie voorgedaan waarin een werkgever pas maanden na indiensttreding de nieuwe werknemer heeft aangemeld bij het pensioenfonds. Het fonds heeft de verplichting om binnen 3 maanden na datum indiensttreding een zogenaamde "Start-brief" te versturen, maar is daar te laat mee geweest omdat de werkgever de werknemer te laat heeft aangemeld. Is dat dan een overtreding waarvoor de toezichthouders handhavend zouden moeten optreden of een verklaarbare afwijking? De wet zegt immers dat de datum indiensttreding leidend is hoewel deze (schijnbaar) niet altijd haalbaar is. Beide toezichthouders kijken vanuit hun eigen wettelijke opdracht naar deze situatie. Waar DNB vanuit het prudentieel toezicht begrip kon opbrengen voor de situatie hield AFM vanuit het gedragstoezicht vast aan de eis dat 100% van de deelnemerscommunicatie op tijd zou plaatsvinden. Doordat deze situatie in een gezamenlijk overleg met de beide toezichthouders is besproken, zijn partijen daar redelijk snel uit gekomen, maar als er met alle partijen afzonderlijk gecommuniceerd had moeten worden dan was dat een stuk lastiger geweest. Door de stapeling van toezicht blijkt dat de individuele toezichthouders potentieel een ander gewicht toekennen aan dezelfde verplichting en een goede coördinatie daartussen zorgt ervoor dat knelpunten goed aangepakt worden.

4.2.4 Beoordelen van risicoanalyses

DNB[42] vraagt financiële instellingen uitdrukkelijk om het sjabloon te gebruiken dat door DNB is uitgegeven. De financiële instelling is uiteraard vrij om de risicoanalyse uit te voeren op de manier waarop zij wenst, maar wanneer de meldingen op verschillende wijzen gedaan worden, dan is het lastiger voor DNB om deze te beoordelen. Bij een afwijkend sjabloon/indeling schuilt het gevaar dat er elementen worden gemist. Het zou DNB onnodig veel tijd en energie kosten om een grote diversiteit van sjablonen en indelingen te beoordelen, vandaar in ieder geval het verzoek om de standaard sjabloon te gebruiken of de eigen indeling te vertalen naar die van DNB

Meldingen komen op een centraal punt binnen en worden geregistreerd in een centraal register. Na[43] het binnenkomen van de melding wordt eerst een "quick-scan" uitgevoerd op

[39] ABP, vragen 8, 9 en 11. APG, vraag 4.
[40] APG, vraag 6.
[41] APG, vraag 6 en ABP, vraag 9 gecombineerd.
[42] DNB, vraag 6.
[43] DNB, vraag 8.

"compliancy" met de richtlijnen die DNB heeft uitgegeven, wordt gekeken naar de wijze waarop invulling is gegeven aan het identificeren van restrisico's en het mitigeren daarvan en kijkt DNB naar waarborgen die garanderen dat de regiefunctie goed wordt uitgevoerd. Het criterium is daarbij hoe realistisch de maatregelen zijn en de mate van haalbaarheid. Ervaring speelt daarbij een belangrijke rol.

DNB krijgt vele meldingen binnen die vaak betrekking hebben op dezelfde Cloud-aanbieder. De wijze waarop de financiële instelling de vragen rondom de risico's in het format heeft beantwoord c.q. geformuleerd geeft een goede indicatie over de manier waarop en hoe diepgaand de risicoanalyse is uitgevoerd.

Van belang is dat de financiële instelling de regie houdt over de uitvoering van de dienstverlening door Cloud-aanbieders.

Om[44] de financiële instellingen te helpen in het voldoen aan de wettelijke eisen heeft DNB het Toetsingskader Informatiebeveiliging[45] gepubliceerd. Dit toetsingskader is tot stand gekomen na een thema-onderzoek. Binnen het toetsingskader wordt onder andere gebruik gemaakt van (delen van) COBIT en een verwacht volwassenheidsniveau voorgeschreven. Het is aan de financiële instelling om dat aan te tonen.

DNB is terughoudend in het verder concretiseren van de eisen. Het verplicht voorschrijven van specifieke methoden of technieken zou marktinvloed kunnen hebben en daardoor voordeel kunnen opleveren voor bepaalde aanbieders.

Volgens ABP[46] ligt het ook niet voor de hand dat de toezichthouder specifieker zou worden. Daarmee zou de toezichthouder zelf in een lastige positie gebracht kunnen worden door reactief te moeten zijn. Het gevaar bestaat dan dat de goedkeuring van DNB gezien gaat worden als een "keurmerk" en DNB daarin wordt gehinderd om later handhavend op te treden. XYZ[47] is echter van mening dat DNB nu al te voorschrijvend is en veel meer terug zou moeten naar een "principle-based" aanpak, waarin veel meer wordt gewerkt met open normen waaraan zelf invulling gegeven kan worden door de onder toezicht staande organisatie.

4.2.5 Overzicht over de gehele financiële markt

Meldingen[48] komen op een centraal punt binnen en worden geregistreerd in een centraal sheet. Daarmee wordt het totaaloverzicht gehouden. DNB kan door deze centrale registratie ook informatie destilleren over een mogelijke concentratie van uitbestede diensten bij een bepaalde Cloud-aanbieder. Daarmee houdt DNB overzicht over de sectoren en de financiële markt.

Een[49] concentratie van systemen bij dezelfde provider heeft wel eens geleidt tot vragen over het gebruik van de aanbieder tijdens het toezicht. Het is inderdaad een risico als er concentratie ontstaat bij één partij. Faillissement of ander onheil zou grote gevolgen kunnen hebben voor (delen van) de financiële markt. Een melding zal er niet op worden afgewezen. Het is ook meer een punt van aandacht voor DNB zelf. De verwachting is dat DNB zelf maatregelen neemt zoals bijvoorbeeld het uitvoeren van een audit bij die partij.

[44] DNB, vraag 10.
[45] DNB, 2014
[46] ABP, vraag 10.
[47] XYZ, vraag 14.
[48] DNB, vraag 6.
[49] ABP, vraag 12.

Door het gebruik van die centraal bijgehouden registratie is het tevens mogelijk om over alle meldingen heen te kijken naar de wijze van beoordelen.

Potentieel is DNB door het inzicht in de risicoanalyses van de financiële instellingen in staat om fouten in de beoordeling, of risico's die niet of onvoldoende zijn erkend, te detecteren en daar in het toezicht op te toetsen. Volgens ABP[50] wijst de praktijk anders uit: DNB geeft "best practices" uit en deelt resultaten van eigen onderzoeken. DNB detecteert dus wel maar deelt die informatie ook met de instellingen. Door die mate openheid en actieve kennisdeling wordt de kwaliteit alleen maar bevorderd.

In het interview[51] heeft ABP dat verduidelijkt met een voorbeeld uit de praktijk: DNB heeft ooit een vraag gesteld over de sleutellengte die gebruikt werd voor dataversleuteling. De eis die aan de Cloud-aanbieder werd gesteld was namelijk lager dan de eis voor systemen die in het eigen datacenter draaiden. DNB heeft dat opgemerkt. DNB heeft daar geen inhoudelijke waardeoordeel over geveld, maar alleen gedetecteerd en gevraagd of er nog andere, aanvullende maatregelen zijn genomen om te kunnen komen tot een lagere eis. Dat geeft ABP focus.

APG[52] benadrukt de gezamenlijke verantwoordelijkheid ten opzichte van het financiële stelsel: Iedere partij vervult zijn eigen rol in het stelsel, moet daarin zijn verantwoordelijkheid nemen en daarover transparant zijn. Delen van kennis, ervaring en informatie is belangrijk voor het geheel. We hebben een gezamenlijke verantwoordelijkheid richting een behoorlijk deel van de bevolking en zijn toevertrouwd met een behoorlijk kapitaal. Iedere partij moet die verantwoordelijkheid nemen vanuit zijn eigen rol en met elkaar samenwerken.

[50] ABP, vraag 11.
[51] ABP, vraag 7.
[52] APG, vraag 5.

5 Risicomitigerende maatregelen in het algemeen

In dit hoofdstuk wordt antwoord gegeven op de vraag welke risico mitigerende maatregelen een financiële instelling moet nemen in “in-control” te zijn over de Cloud-dienst. Alvorens te kijken hoe financiële instellingen de risicoanalyse uitvoeren, wordt eerst gekeken naar de hulpmiddelen daarvoor vanuit de toezichthouder en naar de manier waarop de financiële instellingen invulling geven aan het proces van risicobeheersing.

5.1 Hulpmiddelen van de toezichthouder

Eerder in dit rapport is al vastgesteld dat DNB terughoudend is in het aanreiken van hulpmiddelen om te voorkomen dat er een soort van “keurmerk” ontstaat waarachter financiële instelling zich zouden kunnen “verstoppen”. In een dergelijke situatie zou DNB gedwongen worden om zichzelf te verdedigen wanneer aanvullende risico’s moeten worden onderkend of risicomitigerende maatregelen genomen hadden moeten worden. Een dergelijke situatie is zeer onwenselijk vanuit de methodiek van toezicht en ook niet hetgeen de wetgever daarvoor voor ogen heeft gestaan.

Het sjabloon van DNB[53] voor het uitvoeren van een risicoanalyse, is gebaseerd op algemeen beschikbare standaarden (zoals NIST, ENISA, ISF en COBIT)[54] en bevat 44 vragen die gegroepeerd zijn in een aantal algemene risicogebieden.

Het sjabloon is onderverdeeld in de volgende risicogebieden:

1. Organizational risks
2. Technical risks
3. Compliance risks
4. Other not cloud specific risks

In de vragen die opgenomen zijn in de vragenlijst zijn onder andere de wettelijke eisen terug te vinden zoals deze zijn opgesomd in paragraaf 4.1 (Eisen vanuit de wetgever).

Zoals DNB[55] heeft aangegeven staat het een financiële instelling vrij om de risicoanalyse uit te voeren op de wijze en met de hulpmiddelen die zij daartoe het meest geschikt vinden, maar stelt wel op prijs dat de melding wordt gedaan via het format van DNB, of de eigen indeling vertaald naar die van DNB.

5.2 Opstellen beleid en uitvoeren van risicoanalyse

Om te kunnen beoordelen of de gehanteerde werkwijze overeenkomt met de wettelijke verplichtingen, zal aan de hand van de gestelde eisen in artikel 14 Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling, een beoordeling plaatvinden.

5.2.1 Een systematische analyse van de risico’s

Eis 1: Een instelling draagt zorg voor een systematische analyse van de risico’s die samenhangen met de uitbesteding van werkzaamheden en legt deze vast. De instelling maakt de analyse op het niveau van zijn eigen organisatie in zijn geheel en op het niveau van de onderscheiden bedrijfsonderdelen.

[53] Opgenomen in Bijlage E (Sjabloon risicoanalyse DNB).
[54] Zie paragraaf 4.2.2 (Toezicht op het gebruik van Cloud-diensten).
[55] DNB, vraag 6.

Door DNB is hier invulling aan gegeven door het uitbrengen van de Circulaire cloud computing[56] in 2011 waarin duidelijk wordt gemaakt wat DNB verwacht van de financiële instellingen wanneer deze gebruik wensen te maken van Cloud-diensten. DNB is daar nog verder in gegaan door het beschikbaar stellen van veelvoorkomende vragen en resultaten uit thema-gebaseerd onderzoek in het "Open Boek Toezicht" en stelt DNB zich beschikbaar voor vragen en doet dat open en laagdrempelig; iets dat door de financiële instellingen ook wordt gewaardeerd[57], al blijft de realisatie dat DNB ook een handhavende taak heeft[58].

Bij alle financiële instellingen die geïnterviewd zijn in dit onderzoek heeft het begrip "Cloud" niet alleen uitdrukkelijk de aandacht van de Risk & Compliance afdelingen maar ook op bestuursniveau wordt de invloed van Cloud technologieën meegenomen in de koers en inrichting van de organisatie.

5.2.2 Een adequaat beleid

Eis 2: Een instelling voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot de uitbesteding van werkzaamheden.

Het uitbesteden van werkzaamheden is iets dat al jaren wordt gedaan binnen de financiële wereld. Iedere organisatie heeft daarvoor beleid en procedures in plaats die garanties geven dat ze "in-control" zijn. Aangezien Cloud feitelijk een bijzondere vorm van uitbesteding is waarbij de mate van controle over de dienstverlening varieert[59], dienen financiële instellingen hun beleid en procedures aan te passen aan het specifieke karakter van het afnemen van Cloud-diensten.

ABP[60] heeft er voor gekozen om het beleid daaromtrent "simpel" te houden en slechts producten van één aanbieder af te nemen en gebruik te maken van standaard dienstverlening. ABP heeft een groot deel van de uitvoeringswerkzaamheden uitbesteed aan APG en is als organisatie daarom redelijk klein en overzichtelijk.

APG en XYZ daarentegen hebben wel specifieke beleidskaders rondom Cloud-diensten ontwikkeld. APG[61] kijkt dan specifiek vanuit de behoefte voor het invullen van de regiefunctie over Cloud-diensten, daarin inbegrepen het opstellen van een "Cloud first" beleid, dataclassificatie standaarden, meldingsplicht en richt daar de organisatie verder op in. XYZ[62] spreekt daarbij zelfs over een transitieproces van onbewust-onbekwaam naar bewust-bekwaam waar het doorheen gaat. Hierin ligt besloten dat XYZ zowel de noodzaak onderkent over het specifieke karakter van Cloud-diensten, alsook de onderkenning dat daarvoor specifieke kennis en kunde opgebouwd moet worden. XYZ voert dit proces onder andere uit door het bezoeken van seminars, raadplegen van verschillende bronnen en advisering door externe specialisten.

5.2.3 Een adequate selectieprocedure

Eis 3: Een instelling hanteert een adequate selectieprocedure voor derden aan wie werkzaamheden worden uitbesteed. De instelling legt vast op grond van welke afwegingen zij tot de keuze voor een bepaalde derde is gekomen.

[56] Chilvers-van der Kruk & Koning, 2011
[57] ABP, vraag 8. APG, vraag 4 en 5. XYZ, vraag 14.
[58] XYZ, vraag 14.
[59] Zie paragraaf 2.3 (Relatie tussen Cloud-diensten en uitbesteding).
[60] ABP, vraag 5.
[61] APG, vragen 2, 3 en 7.
[62] XYZ, vraag 1.

De manier waarop de risicoanalyse wordt uitgevoerd verschilt tussen de financiële instellingen. Iedere instelling heeft dat op haar eigen manier ingeregeld. Zo heeft ABP vanwege de beperkte omvang van de organisatie relatief weinig hoeven vast te leggen op het gebied van Cloud-diensten om toch adequaat te zijn. Dat ligt uiteraard wel anders over de uitbesteding van uitvoeringswerkzaamheden aan APG.

Zowel APG als XYZ hebben eigen vragenlijsten gecreëerd om te helpen bij het uitvoeren van de risicoanalyse. Beiden zijn tot de conclusie gekomen dat de aangedragen risicoaspecten en risico's in het sjabloon van DNB niet volledig toereikend zijn en dat zij additionele en/of specifiekere risico's onderkennen. De melding richting de toezichthouder gebeurt wel op basis van het sjabloon maar daarin is een vertaling naar het eigen formaat gemaakt.

De manier waarop deze vragenlijsten tot stand zijn gekomen varieert ook per organisatie. Daar waar APG eigen kennis en kunde met betrekking tot het integreren van Cloud-diensten heeft opgebouwd door werving, heeft XZY[63] gebruik gemaakt van externe deskundigheid door zich te laten ondersteunen door een vooraanstaand jurist op het gebied van Internationaal ICT recht, tevens hoogleraar aan de Tilburg University.

Wat XYZ[64] bijzonder maakt ten opzichte van andere financiële instellingen is de houding ten opzichte van Amerikaanse dienstverleners. XYZ wil geen enkele connectie met Amerikaanse dienstverleners ter bescherming tegen het doorwerken van Amerikaanse wetgeving. Zowel "Safe Harbor" als het EU Modelcontract bevatten onvoldoende waarborgen tegen de ongewenste effecten van de Amerikaanse wetgeving zoals "data seizure", waarbij de opsporingsdiensten data kunnen opeisen zonder geldige reden zolang er maar een redelijk vermoeden bestaat dat er een misdaad is gepleegd. In die zin zit de Amerikaanse wetgeving fundamenteel anders in elkaar en kunnen opsporingsdiensten alle data opvragen om daarin te kunnen zoeken naar sporen van een misdaad in plaats van data op te vragen voor de bewijslast in een onderzoek.

Een tweede nadelig effect van Amerikaanse wetgeving is "e-discovery" waarbij ook civiele partijen data van elkaar kunnen opvragen bij Amerikaanse Cloud-aanbieders ter bewijsvoering in een geschil. Dat hoeven zelfs geen Amerikaanse bedrijven te zijn die een geschil met elkaar hebben, ook Nederlandse bedrijven kunnen data opvragen wanneer de andere partij gebruik maakt van de Amerikaanse aanbieder. Daarbij is iedere juridische link naar een Amerikaanse partij voldoende om de data op te kunnen vragen, ongeacht waar in de wereld de dienst wordt aangeboden of de data staat.

Zowel binnen APG als XYZ wordt de risicoanalyse uitgevoerd door een team. APG hanteert daarbij de indeling Risk & Compliance, Legal, ICT en Security die ieder vanuit hun eigen perspectief de onderkende risico's beoordelen. Aanvragen voor het gebruik van Cloud-diensten komen doorgaans vanuit de business binnen. Er worden[65] echter ook wel risicoanalyses uitgevoerd die niet vanuit de business zijn geïnitieerd maar voortkomen uit reparatieacties voor Cloud-diensten die al in gebruik zijn. De behandeling daarvan vind bij XYZ plaats binnen de driehoek information security, compliance en privacy. Vanuit die perspectieven wordt de risicoanalyse uitgevoerd. Het is belangrijk om de risicoanalyse te bekijken vanuit de lijnen business, risicobewaking en audit.

[63] XYZ, vraag 4.
[64] XYZ, vraag 1.
[65] XYZ, vraag 5/6.

5.2.4 Toereikende procedures, maatregelen, deskundigheid en informatie

Eis 4: Een instelling beschikt over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de uitbestede werkzaamheden te kunnen beoordelen.

Iedere instelling beschikt over een goed functionerende Risk & Compliance functie die rapporteert over de uitvoering van uitbestede werkzaamheden. Als die er niet zou zijn dan had DNB al lang geleden maatregelen genomen. De vraag die in dit kader gesteld moet worden is in hoeverre het afnemen van Cloud-diensten hierop invloed heeft gehad?

APG[66] ziet duidelijk de noodzaak tot het goed invullen van de regiefunctie over Cloud-diensten. Het beoordelen van de uitvoering van de Cloud-dienst, valt daar binnen. Die regiefunctie wordt momenteel ingericht bij APG en naarmate het gebruik van Cloud-diensten toeneemt zal die regiefunctie volgens APG het verschil maken.

DNB[67] ziet ook dat sommige instellingen overgaan tot het weer “in-sourcen” van bepaalde systemen vanwege problemen met de regievoering. Instellingen zijn op zoek naar de juiste balans tussen uitbesteden en eigen beheer in de deliveryketens.

APG[68] wijst in dit kader op het gevaar dat schuilt in het gebruik van kleine Cloud-aanbieders, zeker vanuit een security perspectief. De markt kent al een aantal afhakers die een aantal jaren geleden nog onaantastbaar leken en lijkt zich te concentreren op slechts enkele grote spelers zoals Microsoft, Amazon en Salesforce. Om te kunnen beoordelen of een aanbieder voldoet aan de gestelde eisen staan er bij de grote Cloud-dienstverleners veel meer middelen ter beschikking. Grote dienstverleners zijn zich veel meer bewust van de risico’s en hebben ook veel meer te verliezen als ze het verprutsen.

Kleine Cloud-dienstverleners weten vaak helemaal niet waaraan zij zouden moeten voldoen en waarom, terwijl bestaande organisaties de grootste moeite hebben met het aanpassen van hun bestaande applicaties naar een Cloud delivery model en daarbij het aspect “compliancy” nauwelijks begrijpen.

Uiteindelijk zal de Cloud-wereld zich concentreren rondom een aantal grote spelers. Daarmee is een “lock-in” bij die partijen onvermijdelijk; dat moet als een gegeven worden beschouwd.

Het heeft een tijd geduurd om te wennen aan het gebruik van Cloud-diensten maar uiteindelijk is dat wel het model van de toekomst en zal binnen niet al te lange tijd een substantieel aandeel van IT functionaliteit uit de Cloud gehaald worden. Ook hier is het de regiefunctie bij de uitbesteder die het verschil zal maken.

5.2.5 Het beloningsbeleid van de derde

Eis 5: Een instelling heeft zicht op het beloningsbeleid van de derde aan wie werkzaamheden worden uitbesteed, betrekt het beloningsbeleid bij de keuze voor de derde waaraan de werkzaamheden worden uitbesteed en maakt zijn beleid dienaangaande openbaar.

Dit is een punt wat de toezichthouder niet direct lijkt te betrekken op Cloud-aanbieders. Het onderwerp komt bijvoorbeeld niet naar voren in de Circulaire cloud computing[69] en ook niet

[66] APG, vraag 2.
[67] DNB, vraag 11.
[68] APG, vraag 7.
[69] Chilvers-van der Kruk & Koning, 2011

in het sjabloon[70] van DNB voor het uitvoeren van de risicoanalyse. Het komt wel expliciet naar voren in de brochure[71] over het uitbesteden van pensioenuitvoering, waarin wordt gesproken over "*het beloningsbeleid van de pensioenuitvoerder*", terwijl in de letterlijke tekst van het artikel wordt gesproken over *"een derde"*. Daarmee lijkt de wetgever in ieder geval geen onderscheid te willen maken tussen een pensioenuitvoerder en een Cloud-aanbieder.

De inhoudelijke risicoanalyse is niet meegenomen in dit onderzoek en daarom kan niet met zekerheid worden beoordeeld of het beloningsbeleid van de Cloud-aanbieder niet toch deel uitmaakt van de aangepaste vragenlijsten van financiële instellingen.

5.3 Verantwoording afleggen

In essentie vind het verantwoording afleggen over het voldoen aan de wettelijke eisen plaats door het aantoonbaar, doorlopend "in-control" zijn. Het "in-control" zijn is een uitvloeisel van de verplichting tot een "beheerste en integere bedrijfsvoering".

Er[72] zijn vele aspecten die daaraan invulling geven. Op hoofdlijnen komt het erop neer dat in ieder geval de klantafspraken goed worden vastgelegd en de eisen die worden opgelegd ook weerspiegelen. Hulpmiddelen zijn daarbij Service Level Agreements en procescontroleverklaringen als ISAE3402. Een tweede aandachtsgebied is het inrichten van de juiste "checks and balances" die evenwichtig zijn verdeeld over de eerste lijn die toeziet op de uitvoering, de tweede lijn die verantwoordelijk is voor het toetsen en de derde lijn die weer toezicht houdt op de tweede lijn. Het derde aandachtsgebied is het inrichten van een goede "governance". Dat komt bijvoorbeeld tot uitdrukking in het creëren van een een cultuur waarin transparant en open over fouten kan worden gecommuniceerd, zodat daarvan kan worden geleerd.

De[73] wijze van aantonen richting de toezichthouder is gelijk aan de wijze waarop richting de fondsen wordt gerapporteerd. Het is van belang om een geïntegreerd controlemechanisme te hebben waardoor steeds op dezelfde manier en inhoudelijk consistent wordt gerapporteerd. Dit controlemechanisme moet dan weer gebaseerd zijn op internationale standaarden als bijvoorbeeld ICS, ISAE en COS 3000.

[70] Bijlage E (Sjabloon risicoanalyse DNB).
[71] DNB-Guidance, 2014, p. 9
[72] APG, vraag 1.
[73] APG, vraag 3.

6 Risico mitigerende maatregelen bij onderaanneming

In het vorige hoofdstuk is antwoord gegeven op de vraag welke risico mitigerende maatregelen genomen moeten worden bij het gebruiken van Cloud-diensten. Deze maatregelen dient een onder toezicht staande organisatie te nemen richting de Cloud-aanbieder. Maar wat als deze Cloud-aanbieder zelf ook weer gebruik maakt van de diensten van een andere aanbieder? Moet de onder toezicht staande organisatie diezelfde maatregelen nemen richting de onderaannemers?

In de beantwoording van deze vraag zal worden uitgegaan van de volgende situatie:

Het perspectief van de toezichthouder:
DNB houdt toezicht op ABP

Het perspectief van de onder toezicht staande organisatie:
ABP heeft pensioenuitvoering uitbesteedt aan APG

Het perspectief van de aannemer die wil uitbesteden:
APG wil een Cloud dienst gebruiken

6.1 Het perspectief van de toezichthouder

Het uitgangspunt van DNB[74] is dat de financiële instelling uiteindelijk verantwoordelijk blijft voor de beheerste en integere bedrijfsvoering en dus regie moet nemen over de uitbesteding. Als de aannemer zelf ook weer uitbesteedt, dan moet de financiële instelling waarborgen hebben zodat ze weten of er sprake is van uitbesteding, beoordelen of die verdere uitbesteding niet conflicteert met de wettelijke plicht, geïnformeerd worden over wijzigingen daarin, de mogelijkheid hebben om daar zelf toezicht op te houden en de mogelijkheid hebben het contract te kunnen beëindigen of andere maatregelen te nemen.

Het advies in deze is om “common sense” te gebruiken: Als de financiële instelling twijfels heeft over de mogelijkheid om grip te houden op de stapel onderaannemers dan zou de instelling zich moeten afvragen of het wel verstandig is om met die partij in zee te gaan.

6.2 Het perspectief van de onder toezicht staande organisatie

ABP[75] moet aantoonbaar “in-control” zijn en heeft daarvoor een stelsel van maatregelen genomen. Het bestuursbureau, waartoe de afdeling Interne Beheersing behoort, ondersteunt het bestuur om “in-control” te blijven en dat ook aantoonbaar te maken. Het bestuursbureau bestaat uit een aantal teams die zich richten op specifieke aspectgebieden waaronder (maar niet exclusief) fondsbeleid, beleggingsbeleid en communicatie.

Voor de uitbesteding aan APG hanteert ABP contractuele bepalingen, Service Level Agreements (SLA) en stelt ABP kaders waarbinnen APG kan c.q. mag opereren. ABP ziet er bijvoorbeeld op toe dat APG haar Risk & Compliancy processen op orde heeft en ook

[74] DNB, vragen 11 en 12.
[75] ABP, vragen 2, 3 en 4 gecombineerd.

daadwerkelijk naleeft. APG legt verantwoording af richting ABP en ABP houdt toezicht op APG.

In de SLA is vastgelegd dat APG toestemming van ABP nodig heeft indien men gegevens van ABP (deelnemers of vermogensgegevens) naar de Cloud wil brengen. Er is contractueel afgesproken dat minimaal dezelfde eisen die ABP aan APG oplegt moeten worden doorgegeven aan onderaannemers. Er wordt expliciet gesproken over “minimaal” vanuit de wetenschap dat APG zelf ook rechtstreeks onder toezicht staat en er daarom redenen kunnen zijn om additionele eisen op te leggen aan onderaannemers. APG moet daarover verantwoording afleggen als onderdeel van het toezicht door ABP en moet aantonen dat alle onderaannemers voldoen aan de wettelijke eisen en verplichtingen.

Wanneer APG gebruik wil maken van een Cloud-dienst dan wordt er een melding gestuurd naar ABP met daarbij het resultaat van de uitgevoerde risicoanalyse. Ingekomen meldingen[76] worden volledig doorgenomen en inhoudelijk beoordeeld. ABP gaat het werk niet nogmaals doen maar controleert wel alles. In de beoordeling kijkt ABP onder andere of de melding voldoet aan het gestelde in de circulaire Cloud-diensten van DNB en naar de opgestelde risicoanalyse. Na de beoordeling stelt het bestuursbureau een advies op voor het bestuur van ABP.

Voor ABP maakt het in principe niet zo veel uit of die Cloud-aanbieder zelf ook weer gebruik maakt van onderaannemers zolang alle onderaannemers maar voldoen aan wet- en regelgeving.

6.3 Het perspectief van de aannemer die wil uitbesteden

Volgens APG[77] zal een eventueel onderaannemerschap door de beoogde Cloud-aanbieder volledig juridisch dichtgetimmerd moeten worden. APG zal zich ervan moeten vergewissen dat de contractpartij ook een regiefunctie heeft over hun dienstverleners en dat ook zij “in-control” zijn. APG blijft immers eindverantwoordelijk richting de toezichthouder en daarom zal APG daarop strak moeten toezien. Ook hier speelt een punt tegen het gebruik van kleine Cloud-aanbieders: Daar moet veel meer tijd en energie in gestoken worden om de waarborgen boven water te krijgen en uiteindelijk is er maar een kleine financiële ruimte om vorderingen in te stellen wanneer het mis gaat.

XYZ[78] voert zelf de screening uit op de contractpartij. Wanneer deze partij zelf ook weer gebruik maakt van onderaannemers dan zullen ze dezelfde screening op die onderaannemers moeten uitvoeren. Vanuit de risicoanalyse wordt dan bekeken of de contractpartij daarin aantoonbaar doorlopend “in-control” is. Bij het afsluiten van een overeenkomst zal deze verplichting expliciet worden vastgelegd in standaard clausules.

6.4 Het belang van certificeringen

Zoals[79] ook in het toetsingskader is aangegeven gaat het over de aantoonbare, doorlopende werking. Enkel de vaststelling dat een aanbieder bezit over een geldig certificaat is onvoldoende. DNB certificeert niet en steunt bij het toezicht niet op certificeringen. DNB baseert haar oordeel op basis van een risicoanalyse, welke maatregelen daarin zijn beschreven, of die maatregelen voldoende waarborgen bevatten en of ze doorlopend aantoonbaar werken (bijvoorbeeld door periodieke audits, “in-control” verklaringen of assuranceverklaringen zoals ISAE3402).

[76] ABP, vraag 6.
[77] APG, vraag 8.
[78] XYZ, vraag 12.
[79] DNB, vraag 12.

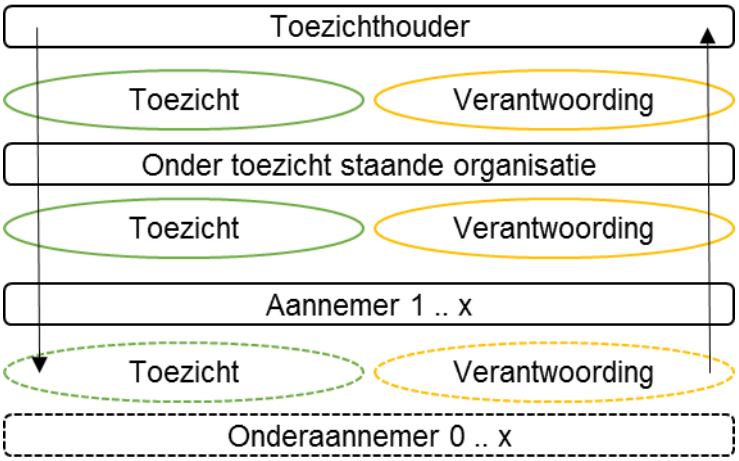
Wanneer[80] een partij niet de gewenste certificeringen bezit dan dringt de vraag zich aan wat de redenen zouden kunnen zijn om toch te kiezen voor de desbetreffende partij. In die overweging kan de aanwezigheid van mogelijke alternatieven een rol spelen maar kunnen strategische overwegingen ook aanleiding zijn om toch met die partij in zee te gaan. Dan zal er wel een grotere inspanning verricht moeten worden voor het uitvoeren van de risicoanalyse en krijgt die meer het karakter van een audit op die partij. De gemiddelde doorlooptijd van een “normale” risicoanalyse is nu eerder dagen dan weken.

6.5 Stapeling van toezicht

Wanneer alle perspectieven rondom onderaanneming in betracht worden genomen dan kunnen er een aantal conclusies worden getrokken:

1. Vanaf de onder toezicht staande organisatie ontstaat er een keten van partijen, die daarmee allemaal een verantwoordelijkheid krijgen in c.q. voor het financiële stelsel
2. Iedere partij is eindverantwoordelijk voor de hele keten daaronder
3. Iedere partij moet “in-control” zijn over de eerstvolgende partij
4. Iedere partij moet daarvoor dezelfde wettelijke eisen, zoals die gelden voor de onder toezicht staande organisatie, opleggen aan de eerstvolgende partij
5. Iedere partij legt daarover verantwoording af aan de opdrachtgever

Wanneer de geschetste situatie die het uitgangspunt was voor dit hoofdstuk wordt gegeneraliseerd, dan ontstaat het volgende model die de stapeling van toezicht inzichtelijk maakt:



[80] XYZ, vraag 11.

7 Conclusies en aanbevelingen

De reden voor het uitvoeren van dit onderzoek was gelegen in de opgedane ervaringen met betrekking tot het afnemen van Cloud-diensten en de verschillende manieren waarop daar tegenaan wordt gekeken.

Door die verschillende interpretaties van hetgeen daadwerkelijk uitgevoerd moet worden was de indruk ontstaan dat er onnodig zware trajecten werden doorlopen. Tijd dus om te onderzoeken wat er nu echt gedaan moet worden zodat iedereen weet wat er wordt verwacht. Dat heeft geleidt tot de volgende centrale vraag:

"Welke eisen worden door DNB en AFM opgelegd aan onder toezicht staande organisaties bij het afnemen van Cloud-diensten en welke risico mitigerende maatregelen moeten worden genomen om te voldoen aan deze eisen in het algemeen en specifiek wanneer sprake is van onderaanneming bij de aanbieder van de Cloud-dienst?"

Het onderzoek heeft aangetoond dat op het afnemen van Cloud-diensten dezelfde wettelijke eisen[81] van toepassing zijn als op alle andere vormen van uitbesteding, maar dat het specifieke karakter van Cloud-diensten aanvullende maatregelen[82] vergen. Deze maatregelen zijn in het onderzoek geïnventariseerd en er is tevens vastgesteld dat dezelfde wettelijke eisen en aanvullende maatregelen van toepassing zijn op alle partijen[83] in de keten.

De achterliggende reden voor het onderzoek was om het beoordelingsproces van Cloud-diensten duidelijk te maken voor iedereen die er bij betrokken is. Uit het onderzoek blijkt dat de Cloud-aanbieder en alle partijen die daarvan deel uit maken ook betrokken moeten worden om de uitbestedende partij uiteindelijk "in-control" te kunnen laten zijn.

Door de verschillende service- en implementatiemodellen van Cloud-diensten ontstaan vele varianten waarbinnen de mate van verantwoordelijkheid en daarmee de controle over de dienst, verschuift tussen de aanbieder en de afnemer. Daarnaast kunnen er al snel complexe ketens van onderaanneming ontstaan wanneer aanbieders zelf ook weer uitbesteden. Wat alle partijen in de keten echter gemeen hebben is dat ze daardoor allemaal deel zijn gaan uitmaken van het financiële stelsel in Nederland en daarmee een maatschappelijke verantwoordelijkheid hebben, hoe beperkt het aandeel daarin dan ook is.

Dat besef is uiteraard aanwezig bij de partijen die bewust actief zijn in het financiële stelsel, maar dat zal steeds minder worden naarmate de keten langer wordt. Het is zelfs niet ondenkbaar dat de aanbieder van een bepaald onderdeel van een dienst helemaal niet weet dat het betreffende onderdeel uiteindelijk gebruikt wordt voor een bedrijfsproces van een financiële instelling.

Het verdient aanbeveling om de bewustwording van de gezamenlijke verantwoordelijkheid voor het financiële stelsel actief uit te dragen tijdens het beoordelingsproces. Daarin hebben zowel de toezichthouders als de financiële instellingen een taak.

[81] Zie de hoofdstukken 2 (Cloud-diensten) en 3 (Wettelijke basis, toezicht en uitbesteding).
[82] Zie de hoofdstukken 4 (Eisen bij uitbesteding) en 5 (Risicomitigerende maatregelen in het algemeen).
[83] Zie hoofdstuk 6 (Risico mitigerende maatregelen bij onderaanneming).

Het bewustwordingsproces kan ondersteund worden door inzichtelijk te maken dat ketens ontstaan, op iedere partij dezelfde wettelijke eisen van toepassing zijn, iedere partij eindverantwoordelijk is voor de naleving daarvan door de hele keten daaronder, iedere partij “in-control” moet zijn over de eerstvolgende partij en dat iedere partij daarover verantwoording moet afleggen aan de opdrachtgever.

Feitelijk kan geconcludeerd worden dat iedere partij in de keten een toezichthouder is. De toezichthouders noemen het “toezicht” en financiële instellingen hebben het over “de regie functie”. Daar zit eigenlijk geen verschil in omdat de wettelijke verplichtingen moeten worden doorgegeven naar de onderliggende partijen. Als er al een verschil is dan heeft dat alleen betrekking op de manier waarop handhavend kan worden opgetreden en het feit dat de toezichthouders, binnen het wettelijk kader, de eisen kunnen veranderen.

Een laatste aanbeveling gaat uit naar DNB: Tijdens het onderzoek is gebleken dat de wettelijke eis tot het beoordelen van het beloningsbeleid van de Cloud-aanbieder niet expliciet is meegenomen in de eisen[84]. Dit zou nader onderzocht moeten worden en wellicht geadresseerd in het Open Boek Toezicht.

Op dit punt is het tijd om de “verborgen” vraag te beantwoorden die is opgenomen in de ondertitel van dit rapport: Iets nieuws onder de zon? Uit het onderzoek is gebleken dat het antwoord “ja, nee en een beetje” zou moeten zijn. Als model is Cloud in technische zin iets nieuws en biedt het kansen die ook door de financiële instelling gezien en aangegrepen worden. Als dienst is het “gewoon” een vorm van uitbesteding waarop dezelfde eisen van toepassing zijn, maar tegelijk ook weer niet want het vereist aanvullende maatregelen.

[84] Zie paragraaf 5.2.5 (Het beloningsbeleid van de derde).

Literatuurlijst

Geraadpleegde regelingen
Stcrt. 2007, nr. 130/pag. 20
Convenant Stichting Autoriteit Financiële Markten en De Nederlandsche Bank N.V.

Stcrt. 2008, nr. 132
Handhavingsbeleid van de Autoriteit Financiële Markten en De Nederlandsche Bank

Geraadpleegde Europese regelgeving
Richtlijn 2002/87/EG

Geraadpleegde rechtspraak
Rb. Rotterdam 31 juli 2015, ECLI:NL:RBROT:2015:5635

Geraadpleegde kamerstukken
Kamerstukken II 2004/2005, 29708, 10 (Wft: Nota van wijziging)
Kamerstukken II 2005/2006, 30413, 2 (Pw: Voorstel van wet)
Kamerstukken II 2005/2006, 30413, 3 (Pw: Memorie van Toelichting)
Kamerstukken II 2005/2006, 30413, 4 (Pw: Advies Raad van State en nader rapport)
Kamerstukken II 2005/2006, 30413, 18 (Pw: Tweede nota van wijziging)

Geraadpleegde literatuur, artikelen, publicaties en rapporten
APG Groep NV 2016
APG Groep NV Jaarverslag 2015

Bergamin e.a. 2010
E. Bergamin e.a., *Pensioenwet. Wetteksten, parlementaire behandeling en relevante regelgeving per artikel gerubriceerd* (Tweede druk), Den Haag: SDU Uitgevers, 2010

Chilvers-van der Kruk & Koning, 2011
M.J. Chilvers-van der Kruk & E. Koning, *Circulaire cloud computing*, Amsterdam: DNB, 06 december 2011

DNB, 2014
DNB, *Toelichting op Toetsingskader Informatiebeveiliging 2014*, Amsterdam: DNB, 22 mei 2014

DNB-Guidance, 2014
DNB-Guidance, *Uitbesteding door pensioenfondsen. Werken aan vertrouwen*, Amsterdam: DNB, juni 2014

Kaal & Koomans, PBM 2016/2, p. 25-28
HJ. Kaal & J. Koomans, 'Pensioen van de toekomst', *Pensioen Bestuur & Management* 2016/2, p. 25-28

Laaper 2015
P. Laaper, *Uitbesteding in de financiële sector*, Nijmegen: Wolters Kluwer 2015.

NIST SP 800-145
P. Mell & T. Grance, The NIST Definition of Cloud Computing (NIST SP 800-145), Gaithersburg: NIST september 2001

Geraadpleegde websites
DNB, Open Boek Toezicht
http://www.toezicht.dnb.nl

Bijlage A Interview DNB

Interview mevrouw I. Talsma, toezichthouder ICT, De Nederlandse Bank d.d. 7 april 2016

Vraag 1: Wat is uw functie en taak binnen DNB?
Mevrouw Talsma is al 20 jaar werkzaam bij DNB als IT auditor bij de interne accountantsdienst (10 jaar) en Toezichthouder ICT en rekent ICT risico's tot haar expertisegebied. Binnen DNB Toezicht zijn diverse expertisecentra die sectoraal (banken, verzekeraars /pensioenfondsen) zijn ingericht. Mevrouw Talsma werkt bij het expertisecentrum IT risk en ondersteunt de algemene toezichtteams op het gebied van ICT risicobeheersing in het uitvoeren van toezicht. Het expertisecentrum IT risk werkt voor alle drie de sectoren.

Vraag 2: Zijn er veranderingen noodzakelijk geweest op organisatorisch vlak om de meldingen m.b.t. Cloud-diensten te kunnen verwerken? Zien we die taak bijvoorbeeld terug in de organisatorische indeling?
De organisatie van DNB is in beweging. In eerste instantie werd door de financiële instellingen terughoudend gereageerd op de mogelijkheden die Cloud-diensten bieden. Met name de onduidelijkheid over de manier waarop risico's kunnen worden beheerst heeft geleidt tot die terughoudendheid. In die tijd keek DNB wel naar Cloud-diensten, maar dat beperkte zich tot individuele expertise. Het werd "erbij" gedaan, naast de reguliere werkzaamheden. Naarmate de volwassenheid van de Cloud-diensten toenam en daarmee ook de interesse van de financiële instellingen, is DNB in gesprek gegaan met verschillende serviceproviders en heeft nader onderzoek verricht.

Vanuit de wettelijke mogelijkheid, vastgelegd in de Wft, om regelgeving vast te stellen m.b.t. de wijze waarop en de voorwaarden waaronder wijzigingen mogen worden uitgevoerd, heeft DNB in december 2011 de "Circulaire cloud computing" uitgebracht. De doelstelling daarvan was om duidelijkheid te geven aan de instellingen hoe omgesprongen diende te worden met Cloud-diensten. Awareness creëren dat hier sprake is van uitbesteding, maar wel van een nieuwe vorm van uitbesteding waarvoor maatregelen genomen moeten worden voor de additionele risico's (waar is de data, hoe krijg ik mijn data terug etc.)

Een van de bepalingen in de circulaire is dat wezenlijke veranderingen vooraf gemeld dienen te worden. Wanneer DNB in het lopend toezicht moet constateren dat Cloud-diensten worden ingezet voor wezenlijke bedrijfsprocessen en dan pas kan beoordelen of de risico's afdoende zijn gemitigeerd, is te laat, de contracten zijn immers al getekend en de dienst geïmplementeerd. Zaken die in ieder geval geregeld moeten zijn, zijn onder andere het "right-to-examine" door DNB, de mogelijkheid om het contract aan te kunnen passen bij een wijziging in de wet- of regelgeving en het hebben van een exit-strategie en plan.

Vraag 3: Heeft het onderwerp "Cloud" invloed (gehad) op de benodigde inhoudelijke capaciteiten of vaardigheden van de toezichthouder (competenties)?
Dit werd bevestigd. Zeker nu het gebruik van Cloud-diensten steeds meer een "commodity" wordt en vele implementaties gelijktijdig plaatsvinden in de financiële markt, neemt de vraag naar capaciteit ook toe. Er wordt ook gekeken of de huidige sectorale indeling wel het meest optimaal is en DNB stelt zich de vraag hoe de eigen bedrijfsprocessen geoptimaliseerd kunnen worden om het toezicht m.b.t. Cloud-diensten efficiënter uit te kunnen voeren. Tot nu toe is veel aandacht uitgegaan naar het behandelen van meldingen over het afnemen van nieuwe Cloud-diensten, maar DNB moet ook periodiek controleren en mogelijk zelfs optreden; ook dat proces van lopend toezicht moet geoptimaliseerd worden voor het aspect Cloud-diensten. In die zin is DNB als organisatie ook volop in beweging.

Gezien het grote aantal financiële instellingen die gebruik maken van Cloud-diensten hanteert DNB de aanpak om grotere instellingen direct te controleren en het toezicht op kleinere instellingen thema-gebaseerd uit te voeren. Bij het laatste wordt een bepaald onderwerp (bijvoorbeeld "right-to-examine" in contracten van grote aanbieders en het hebben van een exit-strategie) uitgelicht en nader bekeken.

Vraag 4: Vindt het aspect (technische) ICT zijn weerslag in de benodigde competenties?
Ja, er is toch specifieke kennis nodig om het toezicht effectief uit te kunnen voeren.

Vraag 5: Welke faciliteiten heeft DNB beschikbaar gesteld aan onder toezicht staande organisaties om te ondersteunen met het (juist) uitvoeren van risicoanalyses voor Cloud-diensten? Hoe is DNB daartoe gekomen? Gebruikt DNB daarvoor externe hulpmiddelen/standaarden/etc?
Een belangrijk hulpmiddel voor de financiële instellingen is de circulaire clouddiensten. Daarnaast heeft DNB een sjabloon uitgegeven met daarin een aantal risico's en risicogebieden wat financiële instellingen kunnen gebruiken om aan te tonen dat ze daarin volledig zijn geweest en de restrisico's voldoende gemitigeerd c.q. formeel geaccepteerd hebben. Gezien de aard van Cloud-diensten is het vrijwel onmogelijk om geen restrisico's te hebben. In het kader van risico gebaseerd toezicht is het van belang om aan te tonen dat er voldoende aandacht is geweest voor restrisico's en dat ze zo goed mogelijk worden gemitigeerd. De financiële instelling blijft verantwoordelijk voor het restrisico.

Ook heeft DNB met een aantal Cloud-aanbieders afspraken gemaakt over het "right-to-examine" door DNB. Daardoor hoeft niet iedere financiële instelling daarover afzonderlijk afspraken te maken met desbetreffende aanbieders, wat overigens niet in de weg staat om zelf afspraken te maken met andere aanbieders. De afspraken die DNB heeft gemaakt moeten dan ook als een hulpmiddel worden gezien (financiële instelling kan vragen voor de met DNB afgestemde standaardpassage in het contract) en zeker niet als "sturend" worden opgevat om marktinvloed te voorkomen.

Voor het samenstellen van hulpmiddelen (zoals bijvoorbeeld het sjabloon) maakt DNB gebruik van standaarden en raamwerken van "National Institute of Standards and Technology" (NIST), "European Union Agency for Network and Information Security" (ENISA), "Information Security Forum" (ISF) en "Control Objectives for Information and related Technology" (COBIT). Financiële instellingen kunnen deze standaarden zien als een suggestie maar zijn uiteindelijk vrij in de keuze voor een raamwerk of standaard.

Daarnaast voert DNB doorlopend onderzoek uit (thema-gebaseerd) en publiceert de resultaten daarvan, tezamen met opgedane kennis en ervaring, in het "Open Boek Toezicht" op de website van DNB.

Vraag 6: Een grote groep mensen met verschillende expertises zijn betrokken bij het beoordelen van binnengekomen meldingen. Hoe zorgt DNB er voor dat de meldingen van verschillende financiële instellingen en sectoren eenduidig worden beoordeeld?
DNB vraagt financiële instellingen om het sjabloon te gebruiken dat door DNB is uitgegeven. De financiële instelling is uiteraard vrij om de risicoanalyse uit te voeren op de manier waarop zij wenst, maar wanneer de meldingen op verschillende wijzen gedaan worden, dan is het lastiger voor DNB om deze te beoordelen. Bij een afwijkend sjabloon/indeling schuilt het gevaar dat er elementen worden gemist. Het zou DNB onnodig veel tijd en energie kosten om een grote diversiteit van sjablonen en indelingen te beoordelen, vandaar in ieder geval het verzoek om de standaard sjabloon te gebruiken of de eigen indeling te vertalen naar die van DNB

Meldingen komen op een centraal punt binnen en worden geregistreerd in een centraal sheet. Daarmee wordt het totaaloverzicht gehouden. DNB kan door deze centrale registratie ook informatie destilleren over een mogelijke concentratie van uitbestede diensten bij een bepaalde Cloud-aanbieder. Daarmee houdt DNB overzicht over de sectoren en de financiële markt.

Door het gebruik van die centraal bijgehouden registratie is het mogelijk om over alle meldingen heen te kijken naar de wijze van beoordelen.

Vraag 7: Sinds het uitbrengen van de circulaire Cloud-diensten: Kunt u zeggen dat er een toename is van het aantal meldingen? Is er een trend waarneembaar?
Er is zeker sprake van een toename. Naast de redenen zoals eerder gegeven heeft ook het van kracht worden van het nieuwe risicogebaseerde toezichtraamwerk voor verzekeraars, Solvency II, invloed gehad op de sector verzekeringen omdat daarin expliciet(er) de meldingsplicht van voorgenomen uitbesteding is opgenomen.

Daarnaast vinden er reparatieacties plaats bij grotere instellingen wat leidt tot tientallen meldingen. Sinds 2011 is het aantal meldingen zeker toegenomen.

Vraag 8: Hoe worden binnengekomen meldingen beoordeeld? Is daar een proces voor wat doorlopen wordt? Op basis van welke criteria wordt besloten om de feitelijke risicoanalyse (onderliggende stukken) op te vragen en te beoordelen? Wanneer gaat DNB daartoe over? Waar let u op bij de beantwoording over het mitigeren van de risico's?
Na het binnenkomen van de melding wordt eerst een "quick-scan" uitgevoerd op "compliancy" met de richtlijnen die DNB heeft uitgegeven, wordt gekeken naar de wijze waarop invulling is gegeven aan het identificeren van restrisico's en het mitigeren daarvan en kijkt DNB naar waarborgen die garanderen dat de regiefunctie goed wordt uitgevoerd. Het criterium is daarbij hoe realistisch de maatregelen zijn en de mate van haalbaarheid. Ervaring speelt daarbij een belangrijke rol.

DNB krijgt vele meldingen binnen die vaak betrekking hebben op dezelfde Cloud-aanbieder. De wijze waarop de financiële instelling de vragen rondom de risico's in het format heeft beantwoord c.q. geformuleerd geeft een goede indicatie over de manier waarop en hoe diepgaand de risicoanalyse is uitgevoerd.

DNB heeft een controleprogramma om meldingen te beoordelen. Dat programma wil DNB nog dieper uitwerken.

Van belang is dat de financiële instelling de regie houdt over de uitvoering van de dienstverlening door Cloud-aanbieders.

Vraag 9: Wat zouden onder toezicht staande organisaties kunnen verbeteren in de uitvoering van de risicoanalyses en het invullen van de evaluatie c.q. meldingen?
DNB is gebaat bij standaardisatie om de beoordeling efficiënt te kunnen uitvoeren en wil daarom in ieder geval meegeven om het standaard sjabloon te gebruiken.

Vraag 10: DNB hanteert open normen door het identificeren van een aantal risico's: Welke criteria hanteert DNB bij de invulling daarvan?
Om de financiële instellingen te helpen in het voldoen aan de wettelijke eisen heeft DNB het Toetsingskader Informatiebeveiliging gepubliceerd. Dit toetsingskader is tot stand gekomen na een thema-onderzoek. Binnen het toetsingskader wordt onder andere gebruik gemaakt van (delen van) COBIT en een verwacht volwassenheidsniveau voorgeschreven. Het is aan de financiële instelling om dat aan te tonen.

DNB is terughoudend in het verder concretiseren van de eisen. Het verplicht voorschrijven van specifieke methoden of technieken zou marktinvloed kunnen hebben en daardoor voordeel kunnen opleveren voor bepaalde aanbieders.

Vraag 11: Hoe kijkt DNB aan tegen onderaannemers in het licht van risico gebaseerd toezicht? Wat verwacht DNB van onder toezicht staande organisaties bij het uitvoeren van de risicoanalyse wanneer de Cloud-aanbieder zelf ook weer gebruik maakt van onderaannemers? Hoe moeten ze hiermee omgaan?
Het uitgangspunt van DNB is dat de financiële instelling uiteindelijk verantwoordelijk blijft voor de beheerste en integere bedrijfsvoering en dus regie moet nemen over de uitbesteding. Als de Cloud-aanbieder zelf ook weer uitbesteed dan moet de financiële instelling waarborgen in plaats hebben zodat ze weten of er sprake is van uitbesteding, beoordelen of die verdere uitbesteding niet conflicteert met de wettelijke plicht, geïnformeerd worden over wijzigingen daarin, de mogelijkheid hebben om daar zelf toezicht op te houden en de mogelijkheid hebben het contract te kunnen beëindigen of andere maatregelen te nemen.

Het advies in deze is om “common sense” te gebruiken: Als de financiële instelling twijfels heeft over de mogelijkheid om grip te houden op de stapel onderaannemers dan zou de instelling zich moeten afvragen of het wel verstandig is om met die partij in zee te gaan.

DNB ziet ook dat sommige instellingen overgaan tot het weer “in-sourcen” van bepaalde systemen vanwege problemen met de regievoering. Instellingen zijn op zoek naar de juiste balans tussen uitbesteden en eigen beheer in de deliveryketens.

Vraag 12: Ligt het zwaartepunt op het bezitten van een certificering of de audit daarop?
Zoals ook in het toetsingskader is aangegeven gaat het over de aantoonbare, doorlopende werking. Enkel de vaststelling dat een aanbieder bezit over een geldig certificaat is onvoldoende. DNB certificeert niet en steunt bij het toezicht niet op certificeringen. DNB baseert haar oordeel op basis van een risicoanalyse, welke maatregelen daarin zijn beschreven, of die maatregelen voldoende waarborgen bevatten en of ze doorlopend aantoonbaar werken (bijvoorbeeld door periodieke audits, “in-control” verklaringen of assuranceverklaringen zoals ISAE3402).

Bijlage B Interview ABP

Interview met de heer F. Toebosch, Afdelingshoofd, Stichting pensioenfonds ABP d.d. 8 april 2016

Vraag 1: Wat is uw functie en taak binnen ABP?
De heer Toebosch is hoofd van de afdeling Interne Beheersing en geeft leiding en coaching aan het team.

De afdeling Interne Beheersing van het bestuursbureau van ABP richt zich op:
- Het t.b.v. het bestuur voorbereiden van de onderhandelingen met APG.
- Het voeren van contract en servicelevel management en het evalueren van de wijze waarop de dienstverleningsovereenkomsten door de uitvoeringsorganisatie APG worden uitgevoerd.
- De aansturing van de externe verslaglegging van het fonds.
- Het ondersteunen en adviseren van de Audit en SLA commissie van het bestuur.
- Het voorbereiden van andere overeenkomsten namens het fonds.
- Het coördineren en onderhouden van de relatie met de toezichthouders DNB en AFM.
- De voorbereiding van het periodieke overleg.
- De aansturing van APG in de contacten met de toezichthouders.
- Voert het secretariaat voor de Raad van Toezicht van het fonds.

Vraag 2: Wat betekent voor u een "beheerste en integere bedrijfsvoering" in het licht van Cloud-diensten? Welke invulling geeft ABP daar aan?
Dat moet bezien worden vanuit twee invalshoeken. Aan de ene kant is daar ABP als organisatie zelf en aan de andere kant als uitbesteder richting APG. ABP heeft bijvoorbeeld haar kantoorautomatiseringsomgeving uitbesteed aan een derde partij en is ook gebruik gaan maken van de Cloud-dienst Office365. Daar heeft ABP zelf een risicoanalyse voor moeten uitvoeren.

Voor de uitbesteding aan APG hanteert ABP contractuele bepalingen, Service Level Agreements (SLA) en stelt ABP kaders waarbinnen APG kan c.q. mag opereren. APG legt verantwoording af richting ABP en ABP houdt toezicht op APG.

Ondanks de verschillende invalshoeken realiseert ABP zich terdege dat het bestuur verantwoordelijk is voor het geheel.

APG heeft toestemming van het fonds nodig indien men gegevens van ABP (deelnemers of vermogensgegevens) naar de Cloud wil brengen. Ligt vast in de SLA.

Vraag 3: Hoe heeft ABP haar eigen toezicht op de onderaannemers ingericht?
ABP moet aantoonbaar "in-control" zijn en heeft daarvoor een stelsel van maatregelen genomen. Het bestuursbureau, waartoe de afdeling Interne Beheersing behoort, ondersteunt het bestuur om "in-control" te blijven en dat ook aantoonbaar te maken. Het bestuursbureau bestaat uit een aantal teams die zich richten op specifieke aspectgebieden waaronder (maar niet exclusief) fondsbeleid, beleggingsbeleid en communicatie.

ABP ziet er bijvoorbeeld op toe dat APG haar Risk & Compliancy processen op orde heeft en ook daadwerkelijk naleeft.

Vraag 4: Hoe gaat ABP om met de situatie waarin een onderaannemer zelf ook weer uitbesteedt d.m.v. Cloud? Hoe vergewist ABP zich dat ze zelf aan haar verplichtingen blijft voldoen?
Er is contractueel afgesproken dat minimaal dezelfde eisen die ABP aan APG oplegt moeten worden doorgegeven aan onderaannemers. Er wordt expliciet gesproken over “minimaal” vanuit de wetenschap dat APG zelf ook rechtstreeks onder toezicht staat en er daarom redenen kunnen zijn om additionele eisen op te leggen aan onderaannemers. APG moet daarover verantwoording afleggen als onderdeel van het toezicht door ABP en moet aantonen dat alle onderaannemers voldoen aan de wettelijke eisen en verplichtingen.

Niet alles kan altijd gecontroleerd worden en ABP hanteert een eigen auditplan met daarin bepaalde thema’s.

Vraag 5: In hoeverre let ABP daarbij op onderaannemers van de Cloud-aanbieder?
Bij het afnemen van Office365 wilde ABP het vooral zo simpel mogelijk houden door slechts producten van één aanbieder af te nemen en gebruik te maken van standaard dienstverlening.

In principe maakt het niet zo veel uit zolang alle onderaannemers maar voldoen aan wet- en regelgeving.

ABP heeft in ieder geval afgesproken dat wanneer het gaat over deelnemersgegevens of vermogen dan moet er altijd gemeld worden.

Vraag 6: Beoordeelt ABP ingekomen meldingen inhoudelijk? Hoe verloopt dat proces?
Ingekomen meldingen worden volledig doorgenomen en inhoudelijk beoordeeld. ABP gaat het werk niet nogmaals doen maar controleert wel alles. In de beoordeling kijkt ABP onder andere of de melding voldoet aan het gestelde in de circulaire Cloud-diensten van DNB en naar de opgestelde risicoanalyse . Na de beoordeling stelt het bestuursbureau een advies op voor het bestuur van ABP.

Vraag 7: Heeft u de indruk dat de toezichthouder de verstuurde meldingen ook inhoudelijk beoordeelt?
DNB geeft geen waardeoordeel over inhoudelijke maatregelen maar detecteert wel wanneer bepaalde aspecten niet meegenomen zijn en stelt daar vragen over. Dat verschaft ABP focus.

Een voorbeeld uit de praktijk: DNB heeft ooit een vraag gesteld over de sleutellengte die gebruikt werd voor dataversleuteling. De eis die aan de Cloud-aanbieder werd gesteld was namelijk lager dan de eis voor systemen die in het eigen datacenter draaiden. DNB heeft dat opgemerkt. DNB heeft daar geen inhoudelijke waardeoordeel over geveld, maar alleen gedetecteerd en gevraagd of er nog andere, aanvullende maatregelen zijn genomen om te kunnen komen tot een lagere eis.

Vraag 8: Krijgt u voldoende handvatten van de toezichthouder om de risicoanalyse juist en volledig uit te voeren? Weet u wat u moet doen?
DNB heeft in 2011 de Circulaire Cloud-diensten uitgegeven waarin duidelijk staat wat er verwacht wordt van de onder toezicht staande organisaties. Daarnaast heeft DNB ook nog een sjabloon aangeleverd waarmee de melding kan worden vormgegeven. Bij onduidelijkheid wordt contact opgenomen met DNB. Er bestaan korte lijnen en er is sprake van een open, constructieve houding.

DNB heeft aangegeven dat de manier waarop APG het self-assessment informatiebeveiliging uitvoert voorbeeldig is voor de pensioensector en misschien zelfs voor de hele financiële markt.

Vraag 9: Is er behoefte aan meer ondersteuning vanuit DNB en in welke vorm zou dat dan moeten?
ABP is content met de huidige vorm van ondersteuning.

De relatie met DNB gaat ook verder dan alleen maar toezicht en handhaving.

Een praktijkvoorbeeld: In de wet staat dat een pensioenfonds binnen 3 maanden na indiensttreding een zogenaamde “Startbrief” moet versturen. In het verleden is het wel eens voorgekomen dat een werkgever de indiensttreding te laat gemeld geeft waardoor die brief niet op tijd is verstuurd. Is dat dan een overtreding waarvoor DNB repressief zou moeten optreden of een verklaarbare afwijking? De wet zegt dat de datum indiensttreding leidend is hoewel deze niet altijd haalbaar is. Dat soort zaken zijn prima met DNB te bespreken en leiden uiteindelijk misschien wel tot een wetswijziging.

We hebben een gedeelde verantwoordelijk voor de stabiliteit van het pensioenstelsel.

Vraag 10: De circulaire Cloud-diensten van DNB is niet dwingend opgesteld. Wat vind u er van als DNB meer dwingend zou worden door bijvoorbeeld het opstellen van beleid?
Dat is niet de taak van de toezichthouder en het is ook niet de verwachting dat de toezichthouder dat doet. Daarmee zouden ze zelf in een lastige positie gebracht worden door reactief te moeten zijn. Het gevaar bestaat dan dat de goedkeuring van DNB gezien gaat worden als een “keurmerk” en DNB daarin wordt gehinderd om later handhavend op te treden.

Vraag 11: DNB krijgt meldingen uit de hele financiële “wereld” met daarin een beoordeling van dezelfde risico’s behorend tot dezelfde Cloud-aanbieder. Potentieel kan DNB daardoor inhoudelijke fouten in de risicoanalyse zien die door het fonds niet is opgemerkt. Ziet u dat als een bedreiging of een mogelijkheid om nog beter de risico’s te kunnen afdekken, zelfs al zou dat betekenen dat DNB zich met een inhoudelijke beoordeling bezig houdt?
DNB geeft “best practices” uit en deelt resultaten van eigen onderzoeken. DNB detecteert dus wel maar deelt die informatie ook met de instellingen. Door die mate openheid en actieve kennisdeling kan er niet gesproken worden over een bedreiging en wordt de kwaliteit alleen maar bevorderd.

Door de thema-gebaseerde aanpak van DNB zou je wel kunnen afleiden op welk aspect de focus zou kunnen komen te liggen in het toezicht.

Vraag 12: DNB heeft een overzicht van alle instellingen die bij één provider zitten en kan daardoor ongewenste concentraties signaleren. Potentieel zou een melding afgewezen kunnen worden om verdere concentratie tegen te gaan. Wat vind u daar van? Gaat DNB dan niet zijn boekje te buiten?
Een concentratie van systemen bij dezelfde provider heeft wel eens geleid tot vragen over het gebruik van de aanbieder. Het is inderdaad een risico als er concentratie ontstaat bij één partij. Faillissement of ander onheil zou grote gevolgen kunnen hebben voor (delen van) de financiële markt. Een melding zal er niet op worden afgewezen. Het is ook meer een punt van aandacht voor DNB zelf. Je zou verwachten dat DNB zelf maatregelen neemt zoals bijvoorbeeld het uitvoeren van een audit bij die partij.

Bijlage C Interview APG

Interview met de heer M. Boerekamp, lid Raad van Bestuur, APG d.d. 10 mei 2016

Vraag 1: De Pensioenwet en de Wet financieel toezicht leggen de verplichting op voor een "beheerste en integere bedrijfsvoering". Hoe geeft u daar invulling aan?
Er zijn vele aspecten die daaraan invulling geven. Op hoofdlijnen komt het erop neer dat in ieder geval de klantafspraken goed worden vastgelegd en de eisen die worden opgelegd ook weerspiegelen. Hulpmiddelen zijn daarbij Service Level Agreements en procescontroleverklaringen als ISAE3402. Een tweede aandachtsgebied is het inrichten van de juiste "checks and balances" die evenwichtig zijn verdeeld over de eerste lijn die toeziet op de uitvoering, de tweede lijn die verantwoordelijk is voor het toetsen en de derde lijn die weer toezicht houdt op de tweede lijn. Het derde aandachtsgebied is het inrichten van een goede "governance". Dat komt bijvoorbeeld tot uitdrukking in het creëren van een cultuur waarin fouten mogen worden gemaakt en we met zijn allen daarvan kunnen leren. Daarvoor is echter een randvoorwaarde dat iedereen eerlijk en open communiceert.

Vraag 2: Heeft de opkomst en het gebruik van Cloud-diensten daarin nog tot veranderingen geleid?
Strikt genomen is het afnemen van Cloud-diensten gewoon een vorm van inkopen. Cloud-diensten zijn daarbij wel wat "ontastbaarder" waardoor het allemaal als een stuk gecompliceerder wordt gezien. Er zal een strakke regie uitgevoerd moeten worden om zeker te zijn dat je aantoonbaar "in-control" bent.

Bij het inkopen zullen alle mogelijke operationele en tactische risico's afgetikt moeten worden en daar heel hard op gestuurd moeten worden. Feitelijk is het niet anders dan intern een systeem hosten maar de sturing vind niet meer plaats tussen afdeling maar met externe partijen.

Als organisatie moet je wel klaar zijn om Cloud-diensten te kunnen draaien. Voor de dienstverlening ben je afhankelijk van een externe partij. Voorbeelden hierbij zijn de gehanteerde "software lifecycle" en "maintenance cycles" van de aanbieder. Afhankelijk van de dienstverlener heb je daar als klant wel enige speelruimte, maar over het algemeen zul je mee moeten kunnen bewegen met de kalender van de aanbieder. Voorheen had je nog de mogelijkheid om een upgrade te verplaatsen naar een ander onderhoudsweekend, of het onderhoudsweekend zelf te verplaatsen. Bij Cloud-diensten wordt er voorgeschreven wanneer je naar een nieuwe versie moet en als organisatie moet je daarin mee kunnen bewegen. Je zult dus veel strakker en beter moeten gaan plannen bij Cloud-diensten, en wanneer je veel Cloud-diensten gebruikt kan dat best een uitdaging zijn.

In kort hangt het succesvol gebruik van Cloud-diensten af van het correct invullen van de regiefunctie. Aan die regiefunctie wordt hard gewerkt binnen APG.

Vraag 3: Hoe toont de RvB richting DNB aan dat het "in-control" is? Gebeurt dat op dezelfde manier als richting de fondsen?
De wijze van aantonen richting de toezichthouder is gelijk aan de wijze waarop richting de fondsen wordt gerapporteerd. Het is van belang om een geïntegreerd controlemechanisme te hebben waardoor steeds op dezelfde manier en inhoudelijk consistent wordt gerapporteerd. Dit controlemechanisme moet dan weer gebaseerd zijn op internationale standaarden als ICS, ISAE en COS 3000.

Vraag 4: Hoe zou u de relatie met DNB willen karakteriseren?
De relatie met de toezichthouders is erg goed. Er wordt op een open en transparante wijze met elkaar gecommuniceerd. Je kunt eigenlijk niet genoeg kennis met elkaar delen en intussen zijn we gewend geraakt om veelvuldig te doen. We delen zelfs "ruwe" data met onze toezichthouders. Daarnaast hebben we een informeel overleg waarin we veranderprogramma's en strategische programma's met elkaar bespreken. Daar zou eventueel een risico in kunnen schuilen dat we in ons enthousiasme informatie verstrekken die later tegen ons gebruikt zou kunnen worden maar doordat we zo open met elkaar zaken bespreken is dat nog nooit een issue geweest.

Vraag 5: Ligt voor u de focus meer op de toezichthoudende taak van DNB of de gezamenlijke taak tot bescherming van het financiële stelsel?
Iedere partij vervult zijn eigen rol in het stelsel, moet daarin zijn verantwoordelijkheid nemen en daarover transparant zijn. Delen van kennis, ervaring en informatie is belangrijk voor het geheel. We hebben een gezamenlijke verantwoordelijkheid richting een behoorlijk deel van de bevolking en zijn toevertrouwd met een behoorlijk kapitaal. Iedere partij moet die verantwoordelijkheid nemen vanuit zijn eigen rol en samen werken.

Vraag 6: Is er behoefte aan meer ondersteuning vanuit DNB en in welke vorm zou u dat graag willen zien?
We zijn op zich erg tevreden over de band met de toezichthouders. Per toezichthouder zou daarin niets hoeven te veranderen. Als er al iets beter zou kunnen dan zit dat in de hoek van stapeling van toezicht en de coördinatie daarvan.

Een voorbeeld: In het verleden heeft zich de situatie voorgedaan waarop een werkgever pas maanden na indiensttreding de nieuwe werknemer heeft aangemeld bij het pensioenfonds. Het fonds heeft de verplichting om binnen 3 maanden na datum indiensttreding een zogenaamde “Start-brief” te versturen, maar is daar te laat mee geweest omdat de werkgever de werknemer laat heeft aangemeld. Beide toezichthouders kijken vanuit hun eigen wettelijke opdracht naar deze situatie. Waar DNB vanuit het prudentieel toezicht begrip kon opbrengen voor de situatie hield AFM vanuit het gedragstoezicht vast aan de eis dat 100% van de deelnemerscommunicatie op tijd zou plaatsvinden. Doordat we gezamenlijk overlegd hebben over deze situatie zijn we daar redelijk snel uit gekomen, maar als we afzonderlijk hadden moeten communiceren met de toezichthouders dan was dat een stuk lastiger geweest. Door de stapeling van toezicht blijkt dat de individuele toezichthouders potentieel een ander gewicht toekennen aan dezelfde verplichting en een goede coördinatie daartussen zorgt ervoor dat knelpunten goed aangepakt worden.

Vraag 7: Denkt u dat in het huidige stelsel van toezicht de mogelijkheden die Cloud-diensten bieden optimaal kunnen worden benut?
Het gebruiken van kleine Cloud-aanbieders is gevaarlijk, zeker vanuit een security perspectief. De markt kent al een aantal afhakers die een aantal jaren geleden nog onaantastbaar leken en lijkt zich te concentreren op slechts enkele grote spelers zoals Microsoft, Amazon en Salesforce.

Om te kunnen beoordelen of een aanbieder voldoet aan de gestelde eisen staan er bij de grote Cloud-dienstverleners veel meer middelen ter beschikking. Grote dienstverleners zijn zich veel meer bewust van de risico’s en hebben ook veel meer te verliezen als ze het verprutsen.

Kleine Cloud-dienstverleners weten vaak helemaal niet waaraan zij zouden moeten voldoen en waarom, terwijl bestaande organisaties de grootste moeite hebben met het aanpassen van hun bestaande applicaties naar een Cloud delivery model en daarbij het aspect “compliancy” nauwelijks begrijpen.

Uiteindelijk zal de Cloud-wereld zich concentreren rondom een aantal grote spelers. Daarmee is een “lock-in” bij die partijen onvermijdelijk; dat moet als een gegeven worden beschouwd.

Het heeft een tijd geduurd om te wennen aan het gebruik van Cloud-diensten maar uiteindelijk is dat wel het model van de toekomst en zal binnen niet al te lange tijd alles uit de Cloud gehaald worden. Ook hier is het de regiefunctie bij de uitbesteder die het verschil zal maken.

Vraag 8: Hoe kijkt u zelf aan tegen een keten van onderaannemers bij Cloud-aanbieders in het licht van “in-control” zijn?
Onderaannemerschap zal volledig juridisch dichtgetimmerd moeten worden. Wij zullen ons ervan moeten vergewissen dat onze contractpartij ook een regiefunctie heeft over hun dienstverleners en dat ook zij “in-control” zijn. Wij blijven immers eindverantwoordelijk richting de toezichthouder en daarom zullen wij daarop strak moeten toezien. Ook hier speelt een punt tegen het gebruik van kleine Cloud-aanbieders: Je zult daar veel meer tijd en effort in moeten steken om de waarborgen boven water te krijgen en uiteindelijk is er maar een kleine financiële ruimte om vorderingen in te stellen wanneer het mis gaat.

Bijlage D Interview XYZ

Interview met X, directeur Global Compliance & Integrity, XYZ d.d. 23 mei 2016

Vraag 1: Heeft uw organisatie beleid opgesteld m.b.t. het gebruiken van Cloud-diensten?
Opstellen van een Cloud beleid hoort tot het transitieproces van onbewust-onbekwaam naar bewust-bekwaam waar XYZ doorheen gaat. Dit proces gebeurt onder andere door het bezoeken van seminars, raadplegen van verschillende bronnen en advisering door consultants.

Wat XYZ bijzonder maakt ten opzichte van andere financiële instellingen is de houding ten opzichte van Amerikaanse dienstverleners. XYZ wil geen enkele connectie met Amerikaanse dienstverleners ter bescherming tegen het doorwerken van Amerikaanse wetgeving. Zowel Safe Harbor als het EU Modelcontract bevatten onvoldoende waarborgen tegen de ongewenste effecten van de Amerikaanse wetgeving zoals “data seizure”, waarbij de opsporingsdiensten data kunnen opeisen zonder geldige reden zolang er maar een redelijk vermoeden bestaat dat er een misdaad is gepleegd. In die zin zit de Amerikaanse wetgeving fundamenteel anders in elkaar en kunnen opsporingsdiensten alle data opvragen om daarin te kunnen zoeken naar sporen van een misdaad in plaats van data op te vragen voor de bewijslast in een onderzoek.

Een tweede nadelig effect van Amerikaanse wetgeving is “e-discovery” waarbij ook civiele partijen data van elkaar kunnen opvragen bij Amerikaanse Cloud-aanbieders ter bewijsvoering in een geschil. Dat hoeven zelfs geen Amerikaanse bedrijven te zijn die een geschil met elkaar hebben, ook Nederlandse bedrijven kunnen data opvragen wanneer de andere partij gebruik maakt van de Amerikaanse aanbieder. Daarbij is iedere juridische link naar een Amerikaanse partij voldoende om de data op te kunnen vragen, ongeacht waar in de wereld de dienst wordt aangeboden of de data staat.

Vraag 2: Hoe bepaalt uw organisatie of er sprake is van een wezenlijk proces?
Vraag 3: Welke criteria hanteert u voor het wel of niet melden aan DNB?
De behoefte aan bepaalde functionaliteit komt hoofdzakelijk vanuit de business. De compliance officer voert een check uit en gebruikt daarbij, naast eigen kennis en opgedane ervaring, het eigen opgestelde Cloud beleid en hulpmiddelen zoals bijvoorbeeld de “good practices” brochure van DNB. XYZ controleert op meer risicogebieden dan DNB aanreikt in zijn sjabloon en meet dus strikter. Waar nodig zal er contact opgenomen worden met DNB via accountmanagement.

XYZ voert ook regelmatig controles uit op het gebruik van Cloud applicaties die niet via de business zijn aangevraagd. Dat gebeurt door externe tooling die detecteert welke Cloud-diensten benadert worden vanuit het XYZ netwerk. Hiermee wil XYZ voorkomen dat er Cloud-diensten worden gebruikt die niet mogen volgens het beleid of eigenlijk gemeld moeten worden bij DNB.

Daarnaast heeft XYZ een ICT Board waaraan alle aanvragen voorgelegd moeten worden voor applicaties c.q. functionaliteit die buiten het “risk appetite” vallen.

Vraag 4: Welke methode gebruikt u voor het uitvoeren van de risico analyse?
XYZ heeft gebruik van gemaakt van de diensten van een vooraanstaand specialist op het gebied van Internationaal ICT recht en tevens hoogleraar aan de Tilburg University, om een standaard vragenlijst op te stellen die toeziet op de specifieke situatie, wensen en behoeftes van XYZ.

Vraag 5: Is er een proces voor ingeregeld en hoe ziet dat er uit?
Vraag 6: Welke disciplines zijn betrokken bij het uitvoeren van de risicoanalyse?
Aanvragen voor het gebruik van Cloud-diensten komen doorgaans vanuit de business binnen. Er worden echter ook wel risicoanalyses uitgevoerd die niet vanuit de business zijn geïnitieerd maar voortkomen uit reparatieacties voor Cloud-diensten die al in gebruik zijn. De behandeling daarvan vindt plaats binnen de driehoek information security, compliance en privacy. Vanuit die perspectieven wordt de risicoanalyse uitgevoerd. Het is belangrijk om de risicoanalyse te bekijken vanuit de lijnen business, risicobewaking en audit.

Vraag 7: Gebruikt u standaard documenten (templates)?
Vraag 8: Welk raamwerk hanteert u om de risico's in kaart te brengen?
XYZ neemt het sjabloon van DNB als uitgangspunt en verwijst daarin naar risico's en maatregelen zoals die binnen de standaard vragenlijst van XYZ zijn geïdentificeerd en beoordeeld. Het raamwerk dat ten grondslag ligt aan het sjabloon van DNB voorziet niet in alle risico's die door XYZ onderkent worden en biedt daarmee geen volledig raamwerk voor de risicoanalyse. Ook hier speelt de gewenste onafhankelijkheid van Amerikaanse wetgeving een belangrijke rol.

Vraag 9: Hoe wordt er omgegaan met het invullen van de open normen die DNB stelt?
XYZ geeft daar een eigen invulling aan.

Vraag 10: Hoe worden certificeringen van de contractpartij beoordeeld?
Vanuit compliance wordt er op hoofdlijnen naar de certificeringen van de contractpartij gekeken. De inhoudelijke beoordeling wordt verzorgt vanuit de afdeling inkoop.

Vraag 11: Hoe wordt de beoordeling gedaan wanneer de contractpartij geen certificering heeft?
Wanneer een partij niet de gewenste certificeringen bezit dan dringt de vraag zich aan wat de redenen zouden kunnen zijn om toch te kiezen voor de desbetreffende partij. In die overweging kan de aanwezigheid van mogelijke alternatieven een rol spelen maar kunnen strategische overwegingen ook aanleiding zijn om toch met die partij in zee te gaan. Dan zal er wel een grotere inspanning verricht moeten worden voor het uitvoeren van de risicoanalyse en krijgt die meer het karakter van een audit op die partij. De gemiddelde doorlooptijd van een "normale" risicoanalyse is nu eerder dagen dan weken.

Vraag 12: Hoe ver gaat u met het bekijken en evalueren van onderaannemers door de contractpartij?
XYZ voert zelf de screening uit op de contractpartij. Wanneer deze partij zelf ook weer gebruik maakt van onderaannemers dan zullen ze dezelfde screening op die onderaannemers moeten uitvoeren. Vanuit de risicoanalyse wordt dan bekeken of de contractpartij daarin aantoonbaar doorlopend "in-control" is. Bij het afsluiten van een overeenkomst zal deze verplichting expliciet worden vastgelegd in standaard clausules.

Vraag 13: Voor onderaannemers gelden dezelfde eisen als voor de contractpartij; schieten we niet te ver door met stellen van eisen rechtstreeks aan de onderaannemer(s)?
Bij onderaanneming blijft de contractpartij verantwoordelijk. XYZ stelt geen rechtstreekse eisen aan eventuele onderaannemers maar beoordeeld of de contractpartij in staat is om die verantwoordelijkheid te kunnen nemen.

Vraag 14: Hoe ziet u de relatie met DNB? Wat zou DNB kunnen doen om te ondersteunen in het uitvoeren van risicoanalyses?
De relatie met DNB is ingewikkeld. Aan de ene kant wil je samenwerken vanuit de gedeelde verantwoordelijkheid voor de stabiliteit van het financiële stelsel en aan de andere kant blijft het de toezichthouder die sancties kan opleggen. De relatie en communicatie met DNB krijgt veel aandacht. Er wordt veelvuldig gecommuniceerd met DNB en de lijnen zijn kort. Relatiemanagers en accountmanagers hebben verschillende keren per dag contact met DNB.

DNB zou wat meer naar een “principle-based” aanpak moeten gaan in tegenstelling tot de “rules-based” aanpak die momenteel wordt gehanteerd. In een “principle-based” aanpak worden veel meer open normen gehanteerd waaraan zelf invulling gegeven kan worden door de onder toezicht staande organisatie.

Bijlage E Sjabloon risicoanalyse DNB

Deze standaard vragenlijst is samengesteld uit internationale standaarden en daarom in het Engels geschreven. Uit de vragenlijst zijn alleen de kolommen opgenomen die tekst bevatten.

De systematiek van de risicoanalyse is dat ieder risico wordt geanalyseerd naar de feitelijke situatie van de financiële instelling en vervolgens wordt beoordeeld op:

1. De kans dat het risico optreedt
2. De invloed die dat heeft
3. Het risico dat daardoor wordt gelopen
4. Hoe dat risico zoveel mogelijk gemitigeerd kan worden
5. Wat een eventueel een restrisico is wat niet gemitigeerd kan worden.

Nr	Risks	Remarks
Organizational risks		
1	Lock-in	Risk of not being able to migrate easily from one provider to another
2	Loss of Governance	Control and influence on the cloud providers, and conflicts between customer hardening procedures and the cloud environment.
3	Compliance challenges (i.e. right to examine, exit clause, privacy etc.)	The risk of Cloud Providers which cannot provide evidence of compliancy to all relevant requirements, policies, laws etc.
4	Loss of business reputation due to cotenant activities	Risk of malicious activities carried out by one tenant affecting the reputation of another tenant.
5	Cloud service termination or failure	The risk of providers going out of business. The risk of unclear data ownership.
6	Cloud provider acquisition	Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk.
7	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.
8	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 also impact the risks for the Otso[85].
9	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.
Technical risks		
10	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.
11	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.

[85] Deze afkoring staat voor “Onder toezicht staande organisatie”

Nr	Risks	Remarks
12	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.
13	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.
14	Intercepting data in transit	Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources.
15	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.
16	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).
17	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
18	EDOS	As 17, but with the effect of Cloud customer going bankrupt or stolen from.
19	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 unauthorized use for authentication and nonrepudiation (digital signature).
20	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.
21	Compromise service engine	Risk of compromise the highly specialized platform, the service engine located above the physical hardware resources and manages customer resources.
22	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.
Compliance risks		
23	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.

Nr	Risks	Remarks
24	Subpoena and e-Discovery	The risk of disclosure of centralized storage as well as shared physical hardware, to unwanted parties.
25	Where is the data	It should be clear where data is stored. This applies also for backup data in a vault location and replicated data in a secondary 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.
26	Risk from changes of jurisdiction	Change in location of data could lead to different jurisdiction, laws and regulations.
27	Data protection risks	The risk of not being able to validate if data is handled in a lawful way. Compliant to regulations like privacy laws, as well as encryption standards apply.
28	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;
29	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.
30	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.
31	Licensing risks	Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment.
Other not cloud specific risks		
32	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.
33	Network management	This could dramatically effect network uptime, experience, up-time and service delivery. 34 Modifying network traffic This could affect data integrity, loss and alteration of sensitive information. Eventually this will evolve as a reputational risk.
35	Privilege escalation	This could lead to access to information or parts of the system normally not accessible to these users. 36 Social engineering attacks Due to lack of security awareness, user provisioning vulnerabilities, lack of resource isolation, communication encryption vulnerabilities, inadequate physical security procedures.
37	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. 38 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.

Nr	Risks	Remarks
39	Backups lost, stolen	Due to inadequate physical security procedures, vulnerabilities, user provisioning vulnerabilities, user de-provisioning vulnerabilities.
40	Unauthorized access to premises	Due to inadequate physical security procedures. Since cloud providers concentrate resources in large data centers, and although the physical perimeter controls are likely to be stronger, the impact of a breach of those controls is higher.
41	Theft of computer equipment	Due to inadequate physical security procedures.
42	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.
43	Conflict of interest	Large cloud providers could use their resources as well as all the data stored on centralized storage, for other purposes.
44	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.