“Gebruik clouddiensten door Nederlandse financiële instellingen”

Bezien vanuit een uitbestedingsrisicomanagement perspectief

Bron: https://networksunlimited.africa/2-solutions/207-cloud-datacenter

Naam:	A.J. (Arend) van de Wetering BBA
Datum:	24 april 2023
Versie:	Definitief

“Gebruik clouddiensten door Nederlandse financiële instellingen”

Bezien vanuit een uitbestedingsrisicomanagement perspectief

Naam:	A.J. (Arend) van de Wetering BBA
Universiteit:	Universiteit Twente
Universiteit (1e begeleider):	prof. dr. Ir. L.J.M. (Bart) Nieuwenhuis
Universiteit (2e begeleider):	dr. M. (Matthias) de Visser
Datum:	24 april 2023
Versie:	Definitief

Voorwoord

Deze masterthesis vormt de afronding van de Executive Master Risicomanagement (MRM) van de Universiteit Twente. Het onderzoek is uitgevoerd in de periode 1 april tot 30 november 2022 voor pensioenfonds A. In verband met de wetenschappelijke bijdrage ligt de nadruk in het afstudeeronderzoek op Nederlandse financiële instellingen in plaats van alleen op pensioenfonds A. Het afstudeeronderzoek is gebaseerd op wetenschappelijke literatuur, wet- en regelgeving, en een validatie door middel van een casestudy en interviews. De uitkomsten van dit onderzoek bieden financiële instellingen mogelijk handvatten bij het gebruik van clouddiensten van grote buitenlandse cloudaanbieders. In het onderzoek ligt de nadruk op de beheersing van uitbestedingsrisico's op basis van wetenschappelijke literatuur en wet- en regelgeving. De masterthesis heb ik op persoonlijke titel geschreven.

Ik ben blij dat ik de kans heb gekregen om deze Master Risicomanagement te volgen en het risicomanagementvakgebied verder te verkennen en doorgronden. Mijn begeleiders bij pensioenfonds A wil ik graag via deze weg bedanken.

Tenslotte wil ik graag mijn begeleiders vanuit de Universiteit Twente, Professor Bart Nieuwenhuis en Assistent Professor Matthias de Visser, hartelijk bedanken voor de gegeven adviezen, hulp en begeleiding bij het onderzoek. Het schrijven van deze masterthesis was een unieke kans om meer ervaring op te doen op het gebied van onderzoek. Het proces van het schrijven van de scriptie was niet altijd even gemakkelijk, maar het heeft mijn kennis vergroot en mij ervaring gegeven om wetenschappelijke theorieën met mijn praktijk te combineren en hieruit gefundeerde conclusies te trekken.

Ik wens u veel plezier met het lezen van deze masterthesis.

Wijk bij Duurstede, 24 april 2023
Arend van de Wetering

Inhoudsopgave

Samenvatting

Het gebruik van clouddiensten groeit enorm hard en wordt steeds meer een standaard in de markt voor IT-uitbesteding. Nederlandse financiële instellingen en hun uitbestedingspartijen kunnen onder voorwaarden gebruik maken van clouddiensten. De doelstelling van het onderzoek is om door middel van kwalitatief onderzoek inzicht te krijgen in bestaande cloud-life-cycle modellen in wetenschappelijke literatuur, de wettelijke vereisten voor Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse aanbieders en hoe deze financiële instellingen het gebruik maken van deze clouddiensten kunnen beheersen. Hiervoor is de volgende hoofdvraag opgesteld:

> *"Hoe kunnen Nederlandse financiële instellingen blijven voldoen aan de wettelijke vereisten en verwachtingen van toezichthouders bij uitbesteding van hun ICT aan grote buitenlandse aanbieders van clouddiensten?"*

Uit de resultaten van het kwalitatieve onderzoek blijkt dat het gebruik van clouddiensten op grond van wet- en regelgeving als een vorm van (IT-)uitbesteding wordt beschouwd. Voor uitbesteding gelden wettelijke vereisten en verwachtingen van toezichthouders, zoals het beheersen van risico's en in kennis stellen toezichthouders. Het bestuur van de Nederlandse financiële instelling blijft te allen tijde eindverantwoordelijk.

Op basis van wetenschappelijke literatuur, Nederlandse en Europese wet- en regelgeving en verwachtingen van toezichthouders is in het kader van deze masterthesis een conceptueel (cloud)uitbestedingsmodel voor banken, verzekeraars en pensioenfondsen ontwikkeld. Dit model bestaat uit een figuur en checklist. Het model is gevalideerd door middel van een casestudy met vigerend beleid van een financiële instelling en een cloudovereenkomst, en interviews.

Een kanttekening van het conceptueel (cloud)uitbestedingsmodel is dat het in de praktijk zelden tot nooit zal voorkomen dat een Nederlandse financiële instelling een combinatie is van bank, verzekeraar én pensioenfonds. Het model is daarom conceptueel van aard. Het conceptueel model kan daarentegen wel praktische handvatten bieden voor Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse aanbieders. Het kan tevens bijdragen aan het invulling geven aan de beheerste en integere bedrijfsvoering.

1 Inleiding

Dit hoofdstuk zet eerst uiteen wat de aard en relevantie van het onderzoek is, gevolgd door een beschrijving van de context van de Nederlandse financiële sector en het gebruik van clouddiensten binnen deze sector. Het hoofdstuk sluit af met de opbouw van het onderzoek.

1.1 Aard en relevantie van het onderzoek

Sinds de beginjaren van 2000 is door technologische innovatie een nieuwe vorm van IT-uitbesteding opgekomen, namelijk cloudcomputing (Wikipedia, 2018). Volgens Oracle (2022) is 'cloudcomputing' het huren van IT in plaats van het kopen. Het wordt als een dienst geleverd die bijvoorbeeld gericht is op hardware, software of beveiliging. De aanbieders van clouddiensten zijn veelal grote buitenlandse partijen, zoals Microsoft Azure, Amazon Web Services en Google Cloud (Synergy Research Group, 2022), die zich richten op klanten wereldwijd in alle sectoren. De verwachting is dat de wereldwijde omzet voor publieke clouddiensten in 2022 circa $ 500 miljard zal bedragen en in 2023 circa $ 600 miljard (Gartner, 2022). In 2021 was de omzet volgens Gartner nog circa $ 410 miljard. De wereldwijde omzetgroei voor publieke clouddiensten zet dus onverminderd door.

Voor het uitbesteden van werkzaamheden door Nederlandse financiële instellingen gelden wettelijke vereisten, zoals dat de instelling verantwoordelijk blijft en uitbesteding niet leidt tot belemmering van de toezichthouder (DNB, 2020). Deze vereisten gelden ook voor het gebruik van clouddiensten. Dit leidt tot uitdagingen en onzekerheden, omdat de aanbieders van clouddiensten veelal buitenlandse bedrijven zijn. Deze bedrijven moeten voldoen aan andere wet- en regelgeving, staan onder toezicht van andere overheden en de clouddiensten worden op basis van veelal standaardovereenkomsten geleverd.

Dit onderzoek heeft ten doel om de besturen van Nederlandse financiële instellingen handvatten te bieden bij de beheersing van het gebruik van clouddiensten. In het onderzoek is een model ontwikkeld voor de beheersing van het gebruik van clouddiensten van grote buitenlandse aanbieders op basis van wetenschappelijke literatuur, wet- en regelgeving en toezichthouder 'good practices'.

1.2 Context

De Nederlandse financiële sector bestaat uit circa 1.400 financiële instellingen (DNB, 2022) die ervoor zorgen dat consumenten kunnen betalen, sparen, lenen en verzekeren (Rijksoverheid, 2022). Voorbeelden van financiële instellingen zijn banken, verzekeraars en pensioenfondsen. Deze financiële instellingen vallen onder toezicht van nationale en internationale toezichthouders, zoals: DNB, AFM, AP, EBA en EIOPA[1]. Dit houdt in dat naast nationale ook internationale wet- en regelgeving van toepassing is. Het internationale karakter is ook afhankelijk van de locaties waar de financiële instellingen opereren. In dit onderzoek ligt de nadruk op wet- en regelgeving gericht op de beheersing van (cloud) uitbesteding voor financiële instellingen in Nederland.

Het gebruik van cloudcomputing in de financiële sector biedt voordelen en nadelen (Scott et al., 2019). Voordelen zijn bijvoorbeeld: schaalbaarheid, lagere kosten, verbeterde beveiliging en weerbaarheid. Scott et al. (2019) onderscheiden de nadelen in technische en operationele risico's, zoals onzekerheden over onvolledige datavernietiging, kwetsbaarheden in multi-tenancy[2] en hypervisor[3], lock-in risico en concentratierisico. De laatste twee risico's hebben betrekking op de afhankelijkheid voor de financiële instelling en voor de financiële sector als geheel doordat zij voor hun kritieke infrastructuur afhankelijk kunnen worden van een klein aantal dominante aanbieders van clouddiensten (Scott et al., 2019).

Technologische transformatie kan aldus leiders in de financiële dienstverlening leiden tot een aanzienlijk concurrentie voordeel (Tapestry Network, 2021). Beschreven is dat de COVID-19-pandemie technologische transformaties bij grote financiële instellingen heeft versneld doordat werknemers zijn overgestapt op het werken op afstand en dat klanten steeds meer laagdrempelige en volledig gepersonaliseerde digitale producten en diensten verwachten. Het gebruik van clouddiensten kan hierbij ondersteunen.

[1] Zie Bijlage 9 voor de afkortingenlijst.
[2] 'Multi-tenancy' betekent dat meerdere klanten dezelfde fysieke infrastructuur delen. Dit is een uniek kenmerk van cloud (Scott et al., 2019).
[3] 'Hypervisor' is software die de virtuele machines beheert waaruit de cloud bestaat en wijst zo nodig cloudresources toe aan klanten. Virtualisatie is het vermogen van meerdere gebruikers om dezelfde fysieke infrastructuur te delen alsof ze hun eigen afzonderlijke machines gebruiken (Scott et al., 2019).

1.3 Opbouw van de masterthesis

De opbouw van de masterthesis is opgenomen in Tabel 1. Deze is gebaseerd op de beschrijving van de masterthesis voor de Master Risicomanagement (Universiteit Twente, 2019).

Hoofdstuk	Beknopte omschrijving
1. Inleiding	Dit hoofdstuk zet eerst uiteen wat de aard en relevantie van het onderzoek is, gevolgd door een beschrijving van de context van de Nederlandse financiële sector en clouddiensten binnen deze sector. Het hoofdstuk sluit af met de opbouw van het onderzoek.
2. Probleemstelling en onderzoeksdoel	Dit hoofdstuk zet eerst uiteen wat de probleemcontext is voor Nederlandse financiële instellingen leidend tot een hoofdvraag, deelvragen en doelstelling van het onderzoek.
3. Onderzoeks-model en dataverzameling	Dit hoofdstuk beschrijft het onderzoeksmodel en methode van dataverzameling. Het hoofdstuk sluit af met de toegepaste ethische code binnen het onderzoek.
4. Literatuur-onderzoek	Dit hoofdstuk beschrijft de voor het onderzoek gebruikte wetenschappelijk literatuur op het gebied van cloudcomputing voor Nederlandse financiële instellingen.
5. Wet- en regelgeving	Dit hoofdstuk beschrijft de voor het onderzoek gebruikte relevante wet- en regelgeving op het gebied van cloudcomputing voor Nederlandse financiële instellingen.
6. Conceptueel model voor (cloud)uitbesteding	In dit hoofdstuk is de wetenschappelijke literatuur en wet- en regelgeving gebruikt voor de totstandkoming van een conceptueel model voor de beheersing van clouduitbesteding door een Nederlandse financiële instelling.
7. Resultaten & analyse	Dit hoofdstuk beschrijft de resultaten van het onderzoek aan de hand van de beantwoording van de deelvragen.
8. Resultaten validatie	Dit hoofdstuk beschrijft de validatie van het conceptueel (cloud)uitbestedingsmodel voor de beheersing van clouduitbesteding op basis van validatie door middel van een casestudy bij een pensioenfonds en een clouduitbestedingsovereenkomst, en interviews.
9. Conclusies, aanbevelingen en reflectie	In dit hoofdstuk is de conclusie opgenomen waarin een antwoord wordt gegeven op de hoofdvraag. Gevolgd door aanbevelingen en onderwerpen voor vervolgstudies. Het hoofdstuk sluit af met een reflectie op het leerproces en uitvoering van de masterthesis.

Tabel 1: Overzicht hoofdstukken en beknopte omschrijving van de masterthesis

2 Probleemstelling en onderzoeksdoel

Dit hoofdstuk zet eerst uiteen wat de probleemcontext is voor Nederlandse financiële instellingen leidend tot een hoofdvraag, deelvragen en doelstelling van het onderzoek.

2.1 Probleemcontext

Het bestuur van een Nederlandse financiële instelling is eindverantwoordelijk voor alle activiteiten van de instelling en het voldoen aan wet- en regelgeving (DNB, 2020). Dit geldt ook bij uitbesteding van werkzaamheden (Wft, art. 3:18, lid 1 en Pw, art. 34 lid 1) aan een IT-uitbestedingspartij of aanbieder van clouddiensten. De uitbestedingspartij is verantwoordelijk voor de uitvoering van de uitbestede werkzaamheden. De financiële instelling moet hiervoor met de uitbestedingspartij afspraken maken in een overeenkomst en service level agreement (DNB, 2014). Ditzelfde geldt voor een uitbestedingspartij met een mogelijke onder-uitbestedingspartij (Brudenall, 2005). Bovendien eist toezichthouder DNB dat uitbesteding niet mag leiden tot enige belemmering voor het uitoefenen van adequaat toezicht door DNB (DNB, 2020). Dit geldt voor de hele keten van uitbesteding.

Uit een onderzoek van pensioenfonds A (2021) blijkt dat vrijwel al haar uitbestedingspartijen en adviesorganisaties clouddiensten afnemen of voornemens zijn deze te gaan afnemen bij grote buitenlandse aanbieders van clouddiensten. Het inzetten van clouddiensten varieert hierbij van de standaard kantoorautomatisering tot het verplaatsen van complete datacenters. Dit stelt het bestuur van het pensioenfonds voor de volgende uitdagingen (ditzelfde geldt ook voor andere Nederlandse financiële instellingen):

- Hoe kan het bestuur haar verantwoordelijkheid blijven nemen?
- Hoe kan het bestuur blijven voldoen aan wet- en regelgeving?
- Hoe houdt het bestuur zicht op de keten van uitbesteding? [4 & 5]
- Hoe zorgt het bestuur dat gebruik van clouddiensten niet leidt tot een belemmering voor toezichthouder DNB?

[4] Pensioenfondsen hebben onvoldoende zicht op langer wordende uitbestedingsketens (dnb.nl)
[5] Verzekeraars hebben onvoldoende zicht op langer wordende uitbestedingsketens (dnb.nl)

2.2 Hoofdvraag

Nederlandse financiële instellingen zijn eindverantwoordelijk voor al hun activiteiten en voor het voldoen aan wet- en regelgeving. Voorwaarden bij uitbesteding zijn dat blijvend wordt voldaan aan wet- en regelgeving en dat de uitbesteding geen belemmering vormt voor toezichthouders bij de uitvoering van haar toezichtstaken. Op basis hiervan is de hoofdvraag in het onderzoek als volgt geformuleerd:

Hoe kunnen Nederlandse financiële instellingen blijven voldoen aan de wettelijke vereisten en verwachtingen van toezichthouders bij uitbesteding van hun ICT aan grote buitenlandse aanbieders van clouddiensten?

2.3 Doelstelling

De doelstelling van het onderzoek is om door middel van kwalitatief onderzoek inzicht te krijgen in bestaande cloudlevenscyclus modellen in wetenschappelijke literatuur, de wettelijke vereisten voor Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse aanbieders en hoe deze financiële instellingen het gebruik maken van deze clouddiensten kunnen beheersen. Met de verzamelde informatie wordt een model ontwikkeld dat Nederlandse financiële instellingen mogelijk handvatten biedt bij het gebruik van clouddiensten van grote buitenlandse aanbieders. Hiermee wordt beoogd een bijdrage te leveren voor zowel de wetenschap als de Nederlandse financiële instellingen.

2.4 Deelvragen

Om de hoofdvraag op een toereikende wijze te beantwoorden, worden de volgende deelvragen in het onderzoek beantwoord:

1. Wat is cloudcomputing en wie bieden clouddiensten aan?
2. Wat zijn de belangrijkste risico's van het gebruik van clouddiensten door Nederlandse financiële instellingen?
3. Welke cloudlevenscyclus-/uitbestedingscyclusmodellen zijn beschreven in de wetenschappelijke literatuur en wat zijn de verschillen hiertussen?
4. Welke wettelijke vereisten & toezichthouder verwachtingen gelden voor Nederlandse financiële instellingen bij uitbesteding en het gebruik maken van clouddiensten?
5. Welke maatregelen moet een Nederlandse financiële instelling nemen om haar risico's bij het gebruik maken van clouddiensten te beheersen?

3 Onderzoeksmodel en dataverzameling

Dit hoofdstuk beschrijft het onderzoeksmodel en methode van dataverzameling. Het hoofdstuk sluit af met de toegepaste ethische code binnen het onderzoek.

3.1 Onderzoeksmodel

Het onderzoeksmodel is gebaseerd op het ontwerp van een conceptueel (cloud)uitbestedings-model voor de beheersing van het gebruik van clouddiensten door Nederlandse financiële instellingen. Dit model komt tot stand op basis van wetenschappelijke literatuur en wet- en regelgeving bij het gebruik maken van clouddiensten door Nederlandse financiële instellingen. In dit onderzoek is de reikwijdte van soorten financiële instellingen beperkt tot banken, verzekeraars en pensioenfondsen. Het model wordt gevalideerd aan de hand van een casestudy bij een pensioenfonds, een cloudovereenkomst en interviews met specialisten uit de financiële sector. De casestudy bestaat uit een vergelijking met vigerend beleid van een pensioenfonds en een vergelijking met een overeenkomst van een aanbieder van clouddiensten. Mogelijke verschillen tussen het model en de casestudy kunnen leiden tot aanbevelingen voor het verbeteren van de beheersing van cloud uitbesteding en/of aanscherping van het model. Het onderzoeksmodel is in Figuur 1 weergegeven.

Figuur 1: Het onderzoeksmodel in de masterthesis

3.2 Methode van dataverzameling

Voor het geven van een antwoord op de hoofd- en deelvragen is gebruik gemaakt van kwalitatief onderzoek. In het boek “Real world research” (McCartan & Robson, 2016) zijn methoden van dataverzameling beschreven. In dit onderzoek is gebruik gemaakt van de volgende methoden van dataverzameling:

- Gebruik van bestaande literatuur (secondary information / desk-based research)
- Gebruik van wet- en regelgeving (primary information / desk-based research)
- Gebruik van bedrijfsdocumenten (primary information / desk-based research)
- Verkrijgen van informatie door mondelinge interviews (primary information / fieldresearch)

Iedere deelvraag in het onderzoek vereist een andere manier van dataverzameling. In Tabel 2 hieronder is een overzicht gegeven van de gebruikte methode(n) per deelvraag. In de sub-paragrafen 3.2.1 en 3.2.2 is de uitvoering van het desk- en fieldresearch toegelicht.

Onderwerpen deelvragen	Desk research	Field research
Definitie cloudcomputing & aanbieders clouddiensten	Wetenschappelijke literatuur en wet- en regelgeving onderzocht voor theoretische benadering.	-
Risico’s gebruik maken van clouddiensten	Wetenschappelijke literatuur en wet- en regelgeving voor risico’s van gebruik maken clouddiensten onderzocht.	Interviews met specialisten uit de financiële sector.
Cloudlevenscyclus-/uitbestedings-cyclus modellen & verschillen	Wetenschappelijke literatuur en toezichthouder bronnen	-
Wettelijke vereisten & toezicht-houder verwachtingen bij gebruik clouddiensten door Nederlandse financiële instellingen	Wet- en regelgeving over cloud en uitbesteding onderzocht.	Interviews met specialisten uit de financiële sector.
Maatregelen voor beheersing risico’s gebruik clouddiensten door financiële instellingen	Wetenschappelijke literatuur en wet- en regelgeving over beheersing cloud risico’s onderzocht.	Interviews met specialisten uit de financiële sector.
Conclusie en aanbevelingen	Gebruik van alle gevonden informatie.	

Tabel 2: Gebruikte methoden van dataverzameling voor onderwerpen in de deelvragen

3.2.1 Uitvoering deskresearch

Het deskresearch vindt plaats op basis van (niet-)wetenschappelijke literatuur, wet- en regelgeving en bedrijfsdocumenten. Deze zijn als volgt geraadpleegd:

- **Wetenschappelijke literatuur** is geraadpleegd via fysieke wetenschappelijke literatuur die is aangeboden in de Master Risicomanagement. Daarnaast is veel gebruik gemaakt van Google Scholar en Scopus die via een koppeling van het 'Microsoft UT student account' toegang gaven tot veel bronnen. Zoektermen waren onder meer: cloud, cloudcomputing, cloudlevenscyclus, uitbestedingscyclus, uitbesteding, risico's voor deze onderwerpen en de Nederlandse financiële sector (zowel in het Nederlands als Engels).
- **Niet-wetenschappelijke literatuur** is geraadpleegd via de zoekmachines Google en Bing (van Microsoft) voor het verkrijgen van zicht op de huidige stand van zaken, problemen en actuele ontwikkelingen op het gebied van cloud en het gebruik maken van clouddiensten. Voorbeelden van geraadpleegde websites zijn: Gartner (www.gartner.com), Microsoft (azure.microsoft.com), Oracle (www.oracle.com) en Salesforce (www.salesforce.com). Zoektermen waren: cloud aanbieders, cloud, cloud computing & vormen en cloud risico's (zowel in het Nederlands als Engels).
- **Wet- en regelgeving** is voor Nederlandse financiële instellingen geraadpleegd via wettenbanken van de Nederlandse overheid (wetten.overheid.nl) en Europese Unie (eur-lex.europa.eu). Daarnaast zijn de websites van de Nederlandse en Europese toezichthouders AFM (www.afm.nl), AP (www.autoriteitpersoonsgegevens.nl), DNB (www.dnb.nl), EBA (www.eba.europa.eu) en EIOPA (www.eiopa.europa.eu) geraadpleegd. Andere bronnen waren het Amerikaanse NIST (csrc.nist.gov) en de Staatscourant van het Koninkrijk der Nederlanden (zoek.officielebekendmakingen.nl). De zoektermen zijn opgenomen in Bijlage 2a van dit onderzoek.
- **Bedrijfsdocumenten** van pensioenfonds A zijn geraadpleegd via de vergaderapplicatie. De gebruikte bedrijfsdocumenten waren onder meer het Beleid Uitbesteding & Advisering, Integraal risicomanagementbeleid, IT-beleid en Informatiebeveiligingsbeleid. De genoemde documenten zijn niet publiek toegankelijk.

3.2.2 Uitvoering van interviews

Met behulp van de interviews wordt aanvullende informatie verzameld. Het doel van de interviews is om:

- Verificatie van de verzameling van de belangrijkste uitbesteding- en cloudrisico's;
- Verificatie van de verzameling van de belangrijkste relevante eisen uit wet- en regelgeving en toezichthouder verwachtingen;
- Verificatie van de uitvoerbaarheid van het model, het voldoen aan wet- en regelgeving en het omgaan met afwijkingen bij uitbesteding aan aanbieders van clouddiensten.

McCartan & Robson (2016) beschrijven drie stijlen van interviews, namelijk: volledig gestructureerde, semigestructureerde en ongestructureerde interviews. In dit onderzoek wordt gebruik gemaakt van semigestructureerde interviews. De interviews worden gehouden met vijf deskundigen die werkzaam zijn in of voor de Nederlandse financiële sector. Dit zijn functionarissen in het senior management en specialisten met ondermeer een economische, juridische of IT-/cybersecurity achtergrond. De interviews worden opgenomen met Microsoft Teams en de antwoorden op de vragen worden uitgeschreven. Na afronding van dit onderzoek worden de opnames vernietigd. Op basis van de verslagen van de interviews worden patronen onderzocht. De uitkomsten worden samengevat. In Bijlagen 6 en 7 zijn de interviewvragen en samengevatte antwoorden opgenomen.

3.3 Ethische code

Het uitgangspunt voor mijn onderzoek is dat ik mijn onderzoek verricht volgens de volgende vijf principes: eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid. Deze zijn opgenomen in de Nederlandse gedragscode wetenschappelijke integriteit (2018).

4 Literatuuronderzoek

Dit hoofdstuk beschrijft de voor het onderzoek gebruikte wetenschappelijke literatuur op het gebied van cloudcomputing voor Nederlandse financiële instellingen.

4.1 Wat is cloudcomputing?

4.1.1 Oorsprong cloudcomputing

Voor een goed begrip van cloudcomputing is het belangrijk om te weten waar de term 'cloud' en de combinatie 'cloudcomputing' vandaan komt. In het artikel 'Wat is Cloud computing?' (Ferreira Pires, 2011) is omschreven dat de term 'cloud' (of in het Nederlands 'wolk') correspondeert met het symbool (of icoon) dat wordt gebruikt om een netwerk of het internet in de IT architectuur aan te duiden. Computing betekent letterlijk in het Nederlands 'computergebruik'. Tezamen betekent cloudcomputing vervolgens 'computergebruik dat ergens op het internet plaatsvindt'. De term 'cloudcomputing' stamt uit 1996 (Wikipedia, 2018). Aldus Wikipedia kwam rond het jaar 2000 de 'Software as a Service' (zie paragraaf 4.1.3) sterk op doordat het bedrijf Salesforce.com technologieën van Google en Yahoo! ombouwde tot bedrijfstoepassingen. Vanaf medio 2000 bieden grote Amerikaanse bedrijven, zoals Amazon (2005), Google (2007) en Microsoft (2008) clouddiensten aan.

4.1.2 Definitie cloudcomputing

In de literatuur wordt veelvuldig verwezen naar een definitie van cloudcomputing van het *National Institute of Standards and Technology* (NIST). Het NIST is een wetenschappelijke instelling die onder de Amerikaanse federale overheid valt die zich inzet voor standaardisatie in de wetenschap. In een publicatie van het NIST uit 2011 worden naast de definitie van cloudcomputing ook de karakteristieken, servicemodellen en implementatiemodellen van cloudcomputing opgenomen. Het NIST omschrijft cloudcomputing als volgt:

> *"A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell & Grance, 2011)*

Vrij vertaald in het Nederlands betekent dit:

> *"Een model om via een netwerk overal eenvoudig op verzoek toegang te verlenen tot een gedeelde pool van configureerbare IT-middelen (bijvoorbeeld netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald." (Mell & Grance, 2011)*

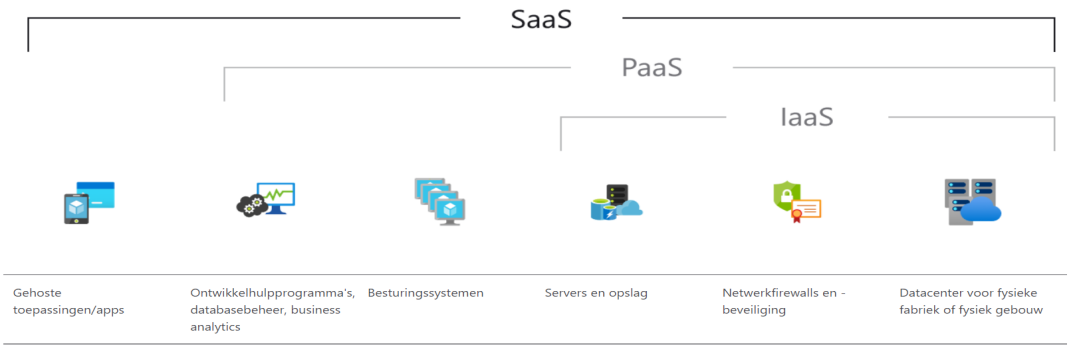
Cloudcomputing gaat aldus Feirreira Pires (2011) verder dan computergebruik dat ergens op het internet plaatsvindt. Uit de NIST-definitie blijkt bijvoorbeeld ook dat de hardware en software flexibel toegankelijk is voor gebruikers. Ook toezichthouder DNB hanteert de definitie voor cloudcomputing op basis van het NIST (2011). Datzelfde geldt voor EIOPA in de *Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten* (2020) en EBA in de *Richtsnoeren inzake uitbesteding* (2019).

4.1.3 Vormen cloudcomputing: service modellen

Cloudcomputing komt in veel verschillende vormen voor. In de NIST-publicatie 800-145 (Mell & Grance, 2011) zijn de onderstaande servicemodellen weergegeven. De voorbeelden zijn beschreven door Ferreira Pires (2011), AWS (2022), Microsoft (2022) en Google (2022):

- **Software as a Service (SaaS):** de aanbieder van clouddiensten biedt gebruikers applicatie / software aan via het internet. Bijvoorbeeld: Gmail, Microsoft 365 en Salesforce.
- **Platform as a Service (PaaS):** de aanbieder van clouddiensten biedt gebruikers en ontwikkelaars hardware en software tools aan via het internet. Bijvoorbeeld: AWS Elastic Beanstalk, Google Apps en Apache Stratos.
- **Infrastructure as a Service (IaaS):** de aanbieder van clouddiensten biedt gebruikers op aanvraag essentiële computer-, opslag- en netwerkresources via het internet. Bijvoorbeeld: AWS S3, Microsoft Azure Disk Storage en Google Cloud Storage.

Als voorbeeld zijn in Figuur 2 deze vormen van cloudcomputing op basis van Microsoft Azure weergegeven.



Figuur 2: Service modellen Microsoft Azure (clouddiensten) (Microsoft, 2022)

In het boek 'Cloud Computing and SOA Convergence in Your Enterprise: Step-by-Step Guide' (Linthicum, 2009) zijn acht aanvullende vormen van cloudcomputing opgenomen, zoals: Storage as a Service, Security as a Service en Testing as a Service. Verder leidt een zoektocht op het internet nog tot veel meer vormen van cloudcomputing. In het oog springende voorbeelden zijn: Artificial Intelligence as a Service, Disaster Recovery as a Service en Ransomware as a Service (LaFlamme, 2020). Cloudcomputing biedt bedrijven kansen, maar ook bedreigingen.

4.1.4 Vormen cloudcomputing: toegankelijkheid

In de NIST-publicatie 800-145 (Mell & Grance, 2011) zijn naast de servicemodellen van cloudcomputing ook vier implementatiemodellen aanwezig. Deze zijn gericht op de toegankelijkheid van de cloudcomputing. Dit zijn:

- **Private cloud:** De infrastructuur is beschikbaar en toegankelijk voor een specifieke organisatie. Het beheer kan door de organisatie zelf en/of een externe leverancier worden uitgevoerd.
- **Community cloud:** De infrastructuur is beschikbaar en toegankelijk voor een specifieke groep gebruikers die een gemeenschappelijk belang hebben. Het beheer kan door een van de organisaties zelf en/of een externe leverancier worden uitgevoerd.
- **Public cloud:** De infrastructuur is beschikbaar en toegankelijk voor het grote publiek. De infrastructuur wordt beheerd door een externe leverancier. De diensten en data kunnen overal ter wereld staan.
- **Hybrid cloud:** Deze infrastructuur bestaat uit een samenstelling van twee of meer verschillende cloudinfrastructuren (private, community of public).

4.1.5 Kenmerken van cloudcomputing

In de literatuur is een aantal specifieke kenmerken van cloudcomputing beschreven (Mell & Grance, 2011; Feirreira Pires, 2011). Deze hebben betrekking op:

- **On-demand self-service:** De gebruiker kan de clouddiensten automatisch op basis van behoefte organiseren.
- **Broad network access:** De clouddiensten zijn beschikbaar via een netwerk en kunnen gebruikt worden door verschillende platforms en devices.
- **Resource pooling:** De bronnen van de aanbieder van clouddiensten worden gedeeld met verschillende gebruikers (ook wel het 'multi-tenant model' genoemd). De bronnen worden dynamisch verdeeld naar de behoefte van gebruikers. De gebruikers hebben geen controle of kennis over de exacte locatie van de bronnen. Het is wel mogelijk om op een hoger niveau de locatie van de bronnen, zoals land of datacenter, te duiden.
- **Schaalbaarheid:** De bronnen of de capaciteit hiervan worden voor gebruikers (automatisch) op-/afgeschaald afhankelijk van de vraag naar deze bronnen.
- **Pay-per-use:** De kosten worden berekend op basis van het gebruik van clouddiensten door gebruikers. Bijvoorbeeld: opslag, licenties, actieve gebruikersaccounts, opslag, rekencapaciteit en bandbreedte.

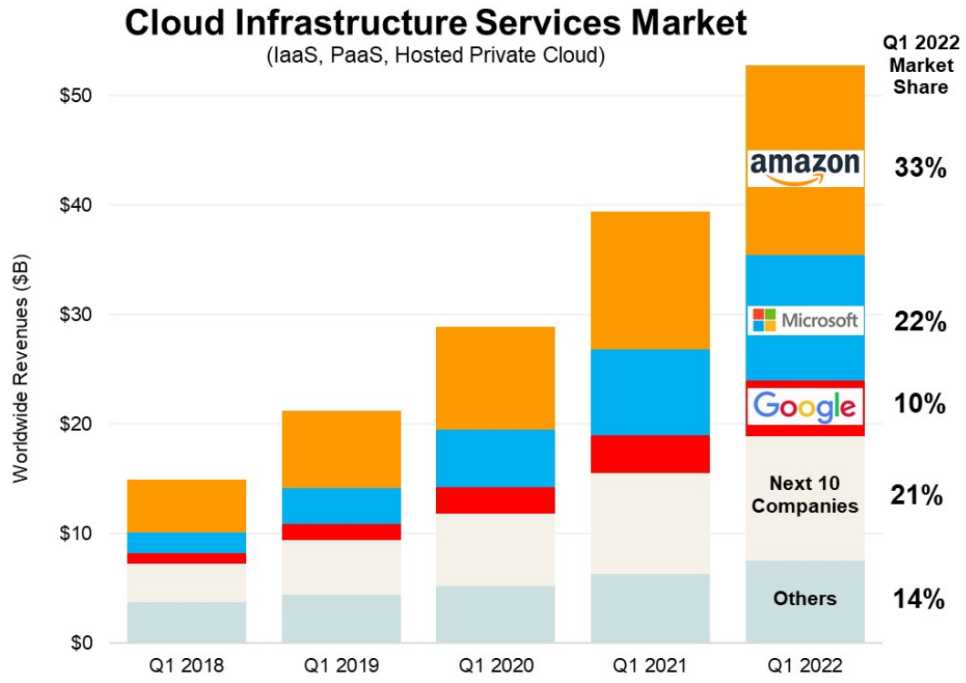
4.1.6 Voordelen van cloudcomputing

In de 'Whitepaper NCSC Cloudcomputing & Security' zijn door het Nationaal Cyber Security Centrum (2012) onder meer de volgende kansen van cloudcomputing beschreven: het voldoen aan wet- en regelgeving, verhogen van het beveiligingsniveau, kostenbesparingen op ICT-investeringen, concentratie op kernactiviteiten, het verhogen productiviteit/standaardisatie en het gebruikersgemak. Het Europese instituut voor cybersecurity (ENISA, 2009) beschrijft in haar rapport *Risicobeoordeling voor cloudcomputing* verschillende kansen op het gebied van informatiebeveiliging voor cloudcomputing, zoals:

- Het inzetten van beveiligingsmaatregelen wordt voordeliger door deze op grotere schaal in te zetten (voorbeelden: patchmanagement en hardening VM's);
- De beschikbaarheid, integriteit en vertrouwelijkheid van clouddiensten zijn belangrijk voor klanten. Daarom is dit een belangrijke drijfveer voor een cloudaanbieder.
- De weerbaarheid van clouddiensten wordt vergroot doordat aanbieders van cloud-diensten dynamisch bronnen toewijzen voor bijvoorbeeld authenticatie en encryptie.

4.1.7 Grote buitenlandse aanbieders van clouddiensten

De wereld kent steeds meer grote aanbieders van clouddiensten waarvan Amazon Web Services ('AWS'), Microsoft Azure en Google Cloud, de grootste zijn (Synergy Research Group, 2022). Andere partijen zijn bijvoorbeeld IBM Cloud Services, Alibaba Cloud, Adobe Creative Cloud en SAP. In het Figuur 3 hieronder wordt het marktaandeel van de cloud infrastructuur services markt weergegeven (Synergy Research Group, 2022).



Figuur 3: Verdeling markaandeel in het 1e kwartaal 2022 (bron: Synergy Research Group, 2022)

Standaardovereenkomsten en service level agreements

Uit onderzoek naar de overeenkomsten met de grootste drie aanbieders van clouddiensten (Microsoft, AWS en Google cloud) blijkt dat zij alle drie standaardovereenkomsten en service level agreements voor hun klanten hanteren. Deze documenten zijn ten dele openbaar raadpleegbaar via hun websites. Deze aanbieders hebben ook een addendum om Europese / Nederlandse financiële instellingen beter in staat te stellen om te kunnen voldoen aan wet- en regelgeving. Op basis van vertrouwelijke bronnen (van uitbestedingspartijen) van pensioenfonds A is vastgesteld dat AWS en Microsoft beschikken over het genoemde addendum.

4.2 Risicomanagement: (cloud)uitbesteding

4.2.1 Integraal risicomanagement

Integraal risicomanagement is aldus DNB (2011): “het interactieve proces van het opstellen van de strategie en hieraan gekoppeld het risicoprofiel en de risicobereidheid, het identificeren van risico’s, het opstellen en implementeren van het beleid voor risicobeheersing, tot de uitvoering, monitoring en terugkoppeling over risico’s en beheersmaatregelen”. Het integraal risicomanagement is in de Nederlandse wet verankerd via beheerste en integere bedrijfsvoering (zie paragraaf 5.1.8).

Het woord “integraal” heeft betrekking op het management van de verschillende financiële en niet-financiële risicogebieden in onderlinge samenhang (DNB, 2011). DNB geeft verder aan dat door het proces continu te doorlopen dat een “op het gebied van risicomanagement een zelflerende en zelfsturende organisatie bestaat, die zich bewust is van de impact van verschillende risico’s en onderlinge samenhang, alsook van de opties voor beheersing en de verschillende consequenties hiervan”. In dit onderzoek is onderzoek gedaan naar de beheersing van (cloud)uitbesteding. Het belangrijkste risico hierbij is het uitbestedingsrisico. Aanpalende risicogebieden zijn: IT, informatiebeveiliging, privacy en continuïteit.

De financiële instellingen beschikken over een integraal risicomanagement kader dat zich uitstrekt over alle bedrijfsonderdelen (EBA, 2019). Op grond hiervan identificeren en beheren financiële instellingen al hun risico’s inclusief risico’s die worden veroorzaakt door uitbestedingspartijen. Dit risicomanagement kader stelt financiële instellingen in staat om goed geïnformeerde besluiten te nemen over het aangaan van risico’s en het treffen van beheersmaatregelen.

4.2.2 Systematische risicoanalyse

Op basis van de Wet op het financieel toezicht (art. 3:17 lid 2a), het Besluit prudentieel toezicht Wft (art. 23 lid 6) en Pensioenwet (art. 143 lid 2a en 143a lid 1) beschikken banken, verzekeraars en pensioenfondsen over een risicobeheerfunctie die op een systematische wijze onafhankelijk risicobeheer uitvoert dat gericht is op het identificeren, meten en evalueren van (uitbestedings)risico’s.

In het kader van beheerste en integere bedrijfsvoering geeft DNB in de *Guidance: uitbesteding door Pensioenfondsen* (2014) aan dat zij verwacht dat een pensioenfonds een systematische risicoanalyse uitvoert met als uitgangspunt de missie, visie en strategie van het pensioenfonds en dat de randvoorwaarden voor de beheerste uitvoering van alle kernactiviteiten worden vastgelegd. DNB (2019) benoemt de systematische risicoanalyse ook als startpunt voor uitbesteding door een verzekeraar, waarna de doelstelling en reikwijdte van uitbesteding worden genoemd (zie paragraaf 5.2.1). De methode op basis waarvan de systematische risicoanalyse kan worden uitgevoerd vormt geen onderdeel van dit onderzoek.

4.2.3 Uitbestedingsrisicoanalyse voor kritieke of belangrijke functies

Het art. 14 lid 1 B Pw is expliciet gericht op uitvoering van een systematische analyse van risico's die samenhangen met uitbesteding. DNB geeft in de *Guidance: uitbesteding door Pensioenfondsen* (2014) aan dat een pensioenfonds naast de systematische risicoanalyse ook periodiek een risicoanalyse uit op kritieke bedrijfsprocessen (DNB, 2014) moet uitvoeren. Op de DNB-website (2011) is door middel van een questionnaire benadrukt dat het bestuur zich bewust moet zijn van de risico's van uitbesteding en specifieke acties moet nemen om de risico's van uitbesteding te identificeren en te beheren. Ook wordt expliciet benoemd het nemen van verantwoordelijkheid bij uitbesteding en het bieden van tegenwicht ('countervailing power'). Een soortgelijke risicoanalyse voor uitbesteding van kritieke of belangrijke functies komt ook terug in de EIOPA *Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten* (2020) en EBA *Richtsnoeren inzake uitbesteding* (2019).

4.2.4 Uitbestedingsrisico's o.b.v. DNB-template

Toezichthouder DNB (2020) heeft voor financiële instellingen een template risicoanalyse (zie Tabel 3) voor uitbesteding van kritieke processen in brede zin opgesteld. De financiële instellingen moeten ten minste de tien risico's in de risicoanalyse beoordelen als onderdeel van de melding van de voorgenomen uitbesteding aan de toezichthouder (zie paragraaf 5.2.4).

#	Omschrijving risico
1	**Vendor lock-in:** Het risico dat niet of niet eenvoudig naar een andere dienstverlener kan worden overgestapt, bijvoorbeeld doordat zich technische beperkingen voordoen, er te weinig andere dienstverleners zijn of de huidige dienstverlener geen ondersteuning kan of wil verlenen bij de overstap naar een concurrent.
2	**Te weinig middelen om acquisities en/of bestaande uitbestedingsovereenkomsten te managen:** De instelling heeft middelen (d.w.z. kennis en personeel) nodig voor de acquisitie, voor de toepassing van uitbestedingsoplossingen en voor de monitoring van leveranciers. Bij dit laatste gaat het om de prestaties van de dienstverlener, maar ook om de interne beheersing, de beheersing van IT-risico's en de beveiliging. Door een tekort aan middelen wordt de uitbesteding niet (langer) gemanaged, waardoor de instelling ongewenste risico's kan lopen, die niet worden gesignaleerd of aangepakt.
3	**Concentratie:** Als één dienstverlener meerdere uitbestedingsoplossingen levert, kan de totale impact van eventuele uitval steeds verder toenemen bij iedere activiteit die de dienstverlener nog meer aan de instelling levert.
4	**Dienstverlener staakt activiteiten:** Het risico dat gegevens, systemen en diensten (direct) niet langer beschikbaar zijn zodra een dienstverlener zijn activiteiten staakt. Mogelijk worden de dagelijkse werkzaamheden van de instelling verstoord en is het moeilijk of onmogelijk om gegevens op te vragen.
5	**Naleving wet- en regelgeving:** De instelling behoudt de verantwoordelijkheid over de uitbestede activiteiten en dient er zorg voor te dragen dat de dienstverlener (en onderaannemers) voldoet aan toepasselijke wet- en regelgeving.
6	**Onvoldoende performance / resultaten:** De dienstverlener houdt zich niet aan de kwaliteitsnormen of voldoet niet aan de gemaakte afspraken, ook al worden kwantitatieve servicelevels wel gehaald. Of de dienstverlening voldoet aan kwantitatieve service levels, maar de kwaliteitsnormen worden niet gehaald. Of kwalitatieve en kwantitatieve normen worden niet gehaald. Hierbij gaat het om monitoring en evaluatie; certificering, service level rapporten, assurancerapporten, audits.
7	**Gegevenslocatie:** De gegevens vallen onder de wetgeving van de locatie waar ze worden opgeslagen of langs worden geleid. Mogelijk verschilt dergelijke lokale wetgeving van de Nederlandse, wat een risico kan vormen met betrekking tot de eisen inzake vertrouwelijkheid.
8	**Scheiding van omgeving:** Voorzieningen kunnen wegvallen die zorgen voor de scheiding van opslag, geheugen, routing en zelfs impact kunnen hebben op de reputatie van de diverse huurders van de gedeelde infrastructuur.
9	**Gegevenstoegang:** Wordt er op een wettelijk juiste manier met de gegevens omgegaan. Hierbij gaat het om de naleving van de regelgeving, zoals over encryptiestandaarden, beheer van encryptiesleutels, het vierogenbeginsel en authenticatie.
10	**Cyberaanvallen:** Alle risico's die verband houden met cyberaanvallen, zoals DDoS-aanvallen, het onderscheppen of uitlekken van gegevens, social engineering, ongeoorloofde toegang, het ongeoorloofd verkrijgen van rechten en ransomware.

Tabel 3: Overzicht uitbestedingsrisico's (bron: DNB risicoanalyse template uitbesteding (2020)

4.2.5 Uitbestedingsrisico's aanvulling o.b.v. dit onderzoek

De risico's in Tabel 3 zijn generiek gericht op uitbesteding van kritieke processen. In Tabel 4 hieronder zijn zeven aanvullende (cloud)gerelateerde uitbestedingsrisico's beschreven die naar voren zijn gekomen in dit onderzoek.

#	Risico	Bron
1	**Wijzigingen (1):** De financiële instelling kan (mogelijk) geen wijzigingen aanbrengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt.	Uitkomst van dit onderzoek (zie Bijlage 5). Art. 31 lid 2b, Bpr Wft & Art. 13 sub e, B Pw.
2	**Wijzigingen (2):** De aanbieder van clouddiensten voert eenzijdige wijzigingsbedingen op in de overeenkomst en gestandaardiseerde cloud leveringsvoorwaarden.	Daniels & Kits, 2015
3	**Deskundigheid:** De financiële instelling kan mogelijk onvoldoende 'countervailing power' / 'tegenwicht' bieden tegen een grote aanbieder van clouddiensten.	Interviews, 2022 (zie Bijlage 7)
4	**Ketenmanagement (1):** De financiële instelling heeft onvoldoende zicht op de keten van uitbesteding van kritieke of belangrijke functies.	DNB, 2022
5	**Ketenmanagement (2):** De financiële instelling kan onvoldoende haar risico's beheersen en haar verantwoordelijkheid nemen door onderuitbesteding naar een aanbieder van clouddiensten.	Interviews, 2022 (zie Bijlage 7)
6	**Toegang door buitenlandse overheidsdiensten:** Een aanbieder van clouddiensten kan door wetgeving met een extra-territoriale werking door een buitenlandse overheid worden gedwongen om gegevens te verstrekken. Ook als de gegevens in Europa worden verwerkt en opgeslagen.	NCSC, 2022
7	**Vernietiging data:** De onzekerheid van het verwijderen van data na het geven van een opdracht tot verwijdering van deze data. Een harde schijf kan bijvoorbeeld niet worden vernietigd als deze door meerdere partijen wordt gebruikt.	ENISA, 2009

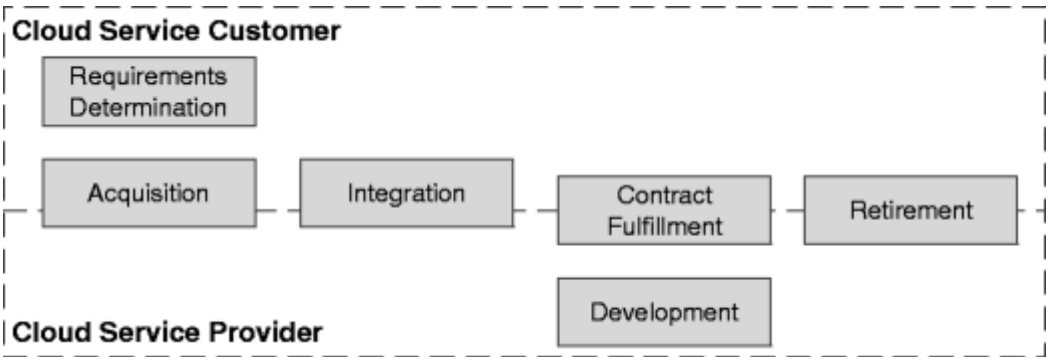
Tabel 4: Overzicht aanvullende (cloud) gerelateerde uitbestedingsrisico's o.b.v. dit onderzoek (2022)

4.3 Cloudlevenscyclus- & uitbestedingscyclus modellen

4.3.1 Cloudlevenscyclusmodel – Schneider & Sunyaev

Cloudcomputing heeft zich geëvolueerd naar een gangbare praktijk om nieuwe technologieën te bieden, zoals online samenwerking en communicatie. De integratie van clouddiensten maakt de flexibele inzet van IT-resources mogelijk, maar brengt ook nieuwe uitdagingen met zich mee. Dit wordt veroorzaakt doordat organisaties hun bedrijfsprocessen opnieuw moeten definiëren, organisatiestructuren moeten aanpassen en servicerelaties met hun cloud-aanbieders moeten aangaan (Schneider & Sunyaev, 2015). De onderzoekers merken in hun conclusie op dat cloudcomputing veel overeenkomsten vertoont met bestaande concepten in de literatuur (bijvoorbeeld: IT-outsourcing). Dit maakt dat de uitdagingen niet volledig exclusief zijn voor cloudcomputing. In het model is gebruik gemaakt van de methode van Riedl et al. ("Quality management in service ecosystems", 2009) en verschillende levenscycluskaders uit de literatuur vanuit verschillende onderzoeksgebieden en belanghebbenden. Op basis van de literatuur en 13 semigestructureerde interviews met experts is het cloud sourcing life cycle model ontwikkeld voor cloudspecifieke en organisatorische aspecten.

Het omvat een iteratief proces van zes fasen (zie Figuur 4), waarvan één alleen betrekking heeft op de klant ('Requirement Determination') en één alleen op de cloudaanbieder ('Development'). De andere vier fasen hebben betrekking op zowel de klant als de cloudaanbieder. Na het figuur is een toelichting op de fasen opgenomen.



Figuur 4: Cloud sourcing life cycle (bron: Schneider & Sunyaev, 2015)

Fasen in de cloud sourcing life cycle van Schneider & Sunyaev (2015):

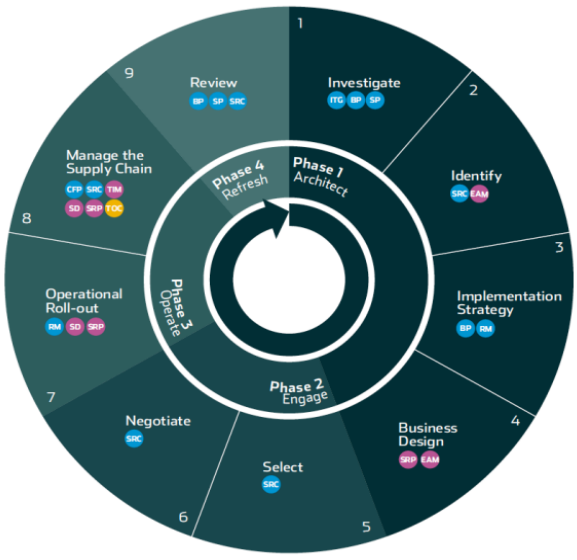
- **Fase 1 - Requirements Determination ('Bepaling van vereisten'):** In deze fase neemt de klant de beslissing of gebruik wordt gemaakt van clouddiensten, in welke mate, wat de vereisten en selectiecriteria zijn, het systeem dat wordt verplaatst, welk service model (IaaS, PaaS of SaaS) en implementatiemodel (publiek, privaat of hybride) zal worden gebruikt. Daarnaast moet een crossfunctioneel inkoopteam worden opgericht. Deze fase is alleen van toepassing op de klant.
- **Fase 2 – Acquisition ('Acquisitie fase'):** Deze fase omvat de evaluatie van de cloudaanbieders en -diensten, en beoordeling van kansen en risico's. Een verschil tussen traditionele IT-uitbesteding en clouduitbesteding is dat meer verantwoordelijkheid bij de klant ligt, doordat de aanbieder van clouddiensten minder betrokken is in deze fase. In plaats van het uitzetten van RFP's zoekt de klant zelf naar informatie, zoals online trials en beschrijvingen van de clouddiensten. Verder omvat de acquisitie fase de business case, on-site presentaties, contractonderhandelingen (w.o. kosten en SLA) en projectplanning voor de volgende fases.
- **Fase 3 – Integration ('Integratie fase'):** Deze fase heeft het meeste impact op de klant vanwege de hoge mate van clouddienststandaardisatie en lage mate van maatwerk voor de klant. De clouddienst wordt geconfigureerd, geïntegreerd in het IT-landschap van de klant en getest als geheel systeem. De clouddienst wordt operationeel in gebruik genomen. De IT-afdeling verandert hierbij van het leveren van een IT-dienst op basis van on-premise hardware en softwaretoepassingen naar het samenstellen en integreren van extern geleverde clouddiensten.
- **Fase 4 - Contract Fulfillment ('Contractuitvoeringsfase'):** De clouddienst aanbieder voert in deze fase o.a. het onderhoud uit, ondersteuning en factureringsactiviteiten. Voor de klant ligt de nadruk op het gebruik van de clouddienst, monitoring- en evaluatie-activiteiten. Daarnaast zijn processen voor relatiebeheer in verband met het (grote) aantal externe geïntegreerde diensten belangrijk.
- **Fase 5 – Development ('Ontwikkelfase'):** Deze fase is alleen van toepassing op de cloudaanbieder en omvat planningsactiviteiten zoals evaluatie marktpotentieel, identificatie van bestaande applicaties of diensten die kunnen worden geleverd als clouddienst en selectie van een prijsmodel. De ontwikkelfase omvat ook de daadwerkelijke implementatie van de dienst, hardware configuratie, testen en uitrollen.

De fase loopt parallel aan fase 4 ('Contract Fulfillment'). Nieuwe functies, updates en patches worden namelijk toegepast als de clouddienst actief is. Afhankelijk van de impact van updates kunnen aanpassingen aan het contract noodzakelijk zijn. Indien de cloudaanbieder gebruik maakt van clouddiensten van andere partijen, dan omvat deze fase ook fase 2 ('Acquisition'). De cloudaanbieder is hierbij dan de klant.

- **Fase 6 – Retirement ('Uitfaseringsfase'):** Deze fase is van toepassing als de cloudaanbieder de clouddienst stopzet of de klant overstapt naar een andere aanbieder. De klant moet de cloud sourcing levenscyclus hervatten of terugkeren naar on-premise toepassingen. Voor de aanbieder van clouddiensten geldt dat de gegevens van de klant moeten worden verwijderd om te voldoen aan regelgeving inzake gegevensbescherming.

4.3.2 Cloudlevenscyclusmodel – Conway & Curry

Voor zowel de migratie naar als het lopende beheer van clouddiensten kan gebruik worden gemaakt van het cloudlevenscyclus model (zie Figuur 5) van Conway & Curry (2012). Dit model is ontwikkeld met behulp van gedefinieerde beoordelingsfasen en ontwikkelingsactiviteiten die zijn gebaseerd op de Design Science Research richtlijnen aanbevolen door Hevner et al. (2004). In het model is gebruik gemaakt van de Cullen life cycle over IT Outsourcing (2005), maar dan met een focus op publieke cloud. Binnen 11 organisaties zijn cloudprojecten onderzocht om de levenscyclus te valideren. Dit betroffen zowel succesvolle als mislukte cloudprojecten. De stappen in de cloudlevenscyclus moeten opvolgend worden uitgevoerd voor een succesvol resultaat.



Figuur 5: The cloud life cycle (Conway & Curry, 2012)

Vier fasen en negen stappen in de cloud life cycle van Conway & Curry (2012):

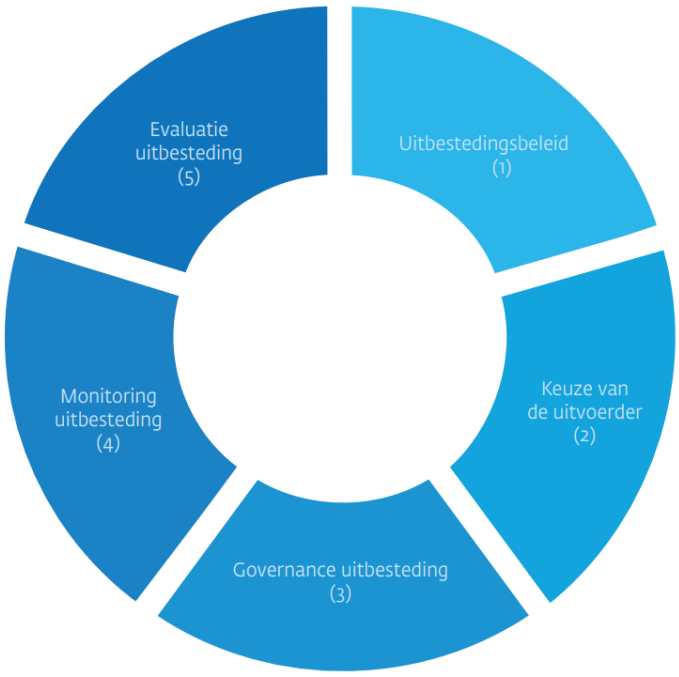
- **Fase 1 – Architect:** De fase begint met het onderzoek en planning van het project.
  - **Stap 1 - Investigate:** Het verkrijgen van inzicht waarom een organisatie naar de cloud wil, wat de doelen zijn en wat de verwachtingen van de clouddiensten zijn (incl. kosten). Hiervoor zijn ervaringen van peer-organisaties van belang en het valideren van het cloudontwerp met materie experts.
  - **Stap 2 – Identify:** Het bepalen welke diensten worden uitbesteed aan de cloudaanbieder, welke het type servicemodel, waarom deze geschikt is en wat de operationele en technische vereisten zijn.
  - **Stap 3 – Implementation strategy:** Het bepalen van de implementatie strategie en aansturing van de uitbesteding, de wijze waarop cloudaanbieders worden ingeschakeld, geselecteerd en beheerd, en hoe risico's worden beoordeeld en bijgewerkt (incl. gegevensherstel en in-sourcing).
  - **Stap 4 – business design:** Maak inzichtelijk hoe de (beoogde) uitbesteding er uit moet zien en definieer (niet-)onderhandelbare uitgangspunten rond contracten, service level agreement en kosten.
- **Fase 2 – Engage:** Omvat de selectie van de cloudaanbieder die de gewenste clouddiensten kan leveren.
  - **Stap 5 – Select:** Definieer het aanbesteding-/biedproces, betrek functionarissen bij de selectie, nodig cloudaanbieders uit, evalueer de cloudaanbieders o.b.v. de vooraf bepaalde criteria, maak een short list en voer een due diligence uit.
  - **Stap 6 – Negotiate:** Bepaal de onderhandelingsstrategie, voer de onderhandelingen, selecteer de gewenste cloudserviceprovider en onderteken de overeenkomst.
- **Fase 3 – Operate:** Omvat de implementatie en het dagelijkse beheer van de clouddiensten.
  - **Stap 7 – Operational Roll-out:** Voltooi de transitieplannen, bepaal acceptatie criteria, voer de transitie uit door het transitieteam, communiceer over de voortgang, voer kennisoverdracht uit en geef leiding aan (in)direct betrokkenen.
  - **Stap 8 – Manage the supply chain:** Beheer en rapporteer over de clouddiensten (inclusief problemen, wijzigingen en verbeteringen), voer de regie over de uitbestedingsrelatie (incl. beoordeling prestatie cloudaanbieder).

- **Fase 4 – Refresh:** Omvat de doorlopende beoordeling van de clouddiensten
  - **Stap 9 – Review:** Beoordeel de prestaties van de cloudaanbieder en vergelijk alternatieven, beoordeel veranderingen in de organisatie die van invloed zijn op de cloudovereenkomst en maak een business case voor het mogelijk starten van een nieuwe cyclus.

4.3.3 Uitbestedingscyclus voor pensioenfondsen

Toezichthouder DNB heeft in 2013 een onderzoek uitgevoerd naar "Risico's in de Uitbestedingsrelatie". Naar aanleiding van dit onderzoek is de *Guidance: uitbesteding door pensioenfondsen* (2014) (hierna: guidance uitbesteding) opgesteld. De guidance uitbesteding is een leidraad van 1 juni 2014. De guidance uitbesteding geeft niet-verplichtende aanbevelingen voor de toepassing van wet- en regelgeving (i.c. de Pensioenwet, Besluit Pensioenwet en Besluit FTK). Het is de afweging van pensioenfondsen of de guidance uitbesteding wordt toegepast. Het uitgangspunt van art. 143 Pw is 'beheersen' dat het hele traject van plannen, besturen, monitoren en bijsturen van doelstellingen en processen omvat. Deze cyclus is ook toepasbaar op het uitbestedingsproces.

DNB heeft in de *Guidance: uitbesteding door pensioenfondsen* (2014) een uitbestedings-cyclus met vijf stappen (zie Figuur 6) opgenomen.



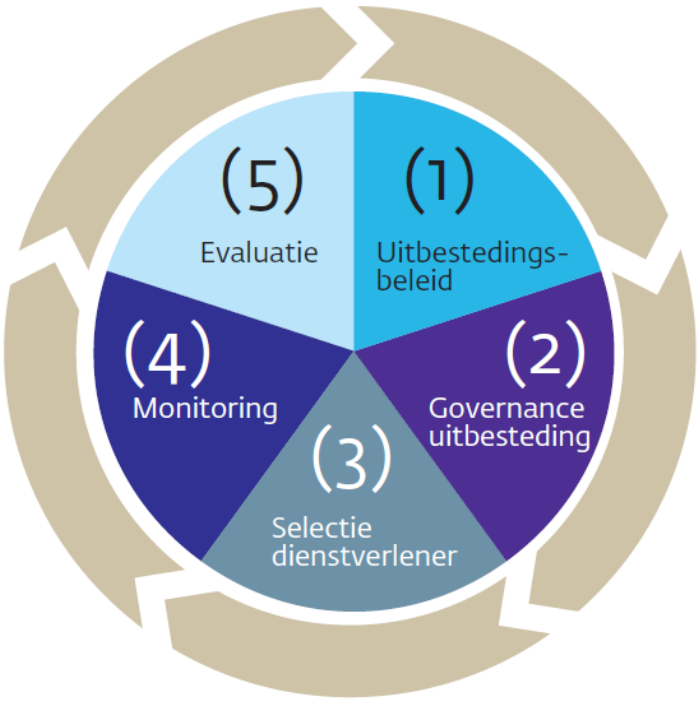
Figuur 6: Uitbestedingscyclus (bron: DNB Guidance: uitbesteding door pensioenfondsen, 2014)

Toelichting op de vijfstappen in de uitbestedingscyclus (DNB, 2014):

- **Stap 1 - Uitbestedingsbeleid:** Een pensioenfonds begint met het uitvoeren van een systematische risicoanalyse en het vastleggen welke randvoorwaarden zij belangrijk vindt voor de beheerste uitvoering van alle kernactiviteiten. De uitkomsten worden opgenomen in het uitbestedingsbeleid. In dit beleid worden onder ander opgenomen: doelstelling van uitbesteding, reikwijdte van uitbesteding, voorwaarden / selectiecriteria voor de uitbestedingspartij, prestatieafspraken en -meting en evaluatie van de partij en het beleid. Het goedgekeurde beleid moet vervolgens uitgewerkt worden in de AO/IC.
- **Stap 2 – Keuze van de uitvoerder:** omvat de voorbereiding op basis van de randvoorwaarden in het uitbestedingsbeleid, een risicoanalyse van de uitbestedingspartij waarbij rekening gehouden wordt met kenmerken die specifieke risico's kunnen identificeren en of het risicoprofiel van de uitbestedingspartij past bij die van het pensioenfonds. Andere stappen in het keuze proces zijn 'request for information', 'request for proposal', 'onderhandelen' en het 'kiezen van de uitbestedingspartij'.
- **Stap 3 – Governance uitbesteding:** omvat de governance van de uitbestedingsrelatie, uitbestedingscontract en Service Level Agreement ('SLA'). Belangrijk is dat het bestuur altijd eindverantwoordelijk is, het pensioenfonds over voldoende deskundigheid en 'countervailing power' beschikt om de regie te kunnen houden, werkzaamheden (incl. risico's en beheersing) adequaat te beoordelen en tijdig bij te sturen. In het uitbestedingscontract en SLA zijn de wettelijke vereisten opgenomen.
- **Stap 4 – Monitoring uitbesteding:** vindt plaats aan de hand van informatieverstrekking die is afgesproken met de uitbestedingspartij. Relevant zijn hierbij de periodiciteit van de rapportages, zoals: SLA-rapportages en assurance rapportages (incl. reikwijdte en betrouwbaarheid), de beoordeling van de rapportages en de toepassing van deze rapportages als sturingsmechanisme.
- **Stap 5 – Evaluatie uitbesteding:** omvat de evaluatie van de uitbestedingspartij en het uitbestedingsbeleid. De evaluatie van de uitbestedingspartij vindt plaats aan de hand van de randvoorwaarden en eisen in het uitbestedingsbeleid. Ook wordt beoordeeld of de uitbestedingspartij bijdraagt aan het behalen van doelen. Het resultaat van de evaluatie kan zijn continueren of de dienst beëindigen. Het uitbestedingsbeleid moet periodiek geëvalueerd worden of deze nog in lijn is met de strategie van het fonds.

4.3.4 Uitbestedingscyclus voor verzekeraars

De DNB *Good practice uitbesteding verzekeraars* (2019) is een leidraad en bevat handvatten voor verzekeraars om uitbestedingsrisico's te beheersen en het voldoen aan wet- en regelgeving. Deze wet- en regelgeving heeft onder meer betrekking op de Wet financieel toezicht, Besluit prudentiële regels Wft, Solvency II richtlijn en EIOPA *Richtsnoeren voor het governancesysteem*. De *Good practice uitbesteding verzekeraars* is van mei 2019. Het is de afweging van verzekeraars of de good practice wordt toegepast. De *Good practice uitbesteding verzekeraars* lijkt qua structuur op de *Guidance uitbesteding door pensioenfondsen* (2014). Het bevat onder meer een vijf fasen uitbestedingscyclus (zie Figuur 7) die grotendeels overeenkomt met de uitbestedingscyclus in de *Guidance: uitbesteding door pensioenfondsen*. De fasen twee en drie zijn echter omgewisseld. Verder is het 'Business Continuity Management' nadrukkelijker opgenomen in de *Good practice uitbesteding verzekeraars*. De verzekeraar dient namelijk op basis van de Solvency II richtlijn te beschikken over een BCM beleid en -strategie en business continuity plan met daarin alle uitbestedingen opgenomen. De uitbestedingspartijen dienen vervolgens eigen business continuity plannen te hebben.



Figuur 7: Uitbestedingscyclus (bron: DNB Good practice uitbesteding verzekeraars, 2019)

4.3.5 Overeenkomsten en verschillen in modellen

De cloudlevenscyclus- en uitbestedingscyclusmodellen vertonen overeenkomsten, maar ook kenmerkende verschillen. Hieronder zijn de belangrijkste overeenkomsten en verschillen weergegeven:

- Alle vier de modellen zijn gebaseerd op een cyclisch en iteratief karakter. In drie van de vier modellen blijkt dit ook uit het figuur (zie figuren 5, 6 en 7). Alleen bij het model van Schneider & Sunyaev (2015) blijkt dit alleen uit de onderbouwing van het model in de fasen 2, 3, 4 en 6.
- Alle vier de modellen bestaan uit 4 tot 6 fasen, die op hoofdlijnen in meer of mindere mate zijn onderscheiden in:
    - Keuze voor wel / niet uitbesteden en doel van de (cloud)uitbesteding;
    - Risicoanalyse en vereisten & selectiecriteria;
    - Inrichting en aansturing van (cloud)uitbesteding door de organisatie en voldoende kennis en kunde bij medewerkers;
    - Selectie van de aanbieder en onderhandeling met de aanbieder van (cloud)diensten;
    - Monitoring van de uitvoering van de (cloud)diensten door de aanbieder van (cloud)diensten;
    - Evaluatie van de dienstverlening van de aanbieder van (cloud)diensten.
- Kenmerkend voor de modellen van Schneider & Sunyaev (2015) en Conway & Curry (2012) is dat zij specifiek gericht op de levenscyclus van het afnemen van clouddiensten. De modellen van DNB zijn gericht op uitbesteding in bredere zin.
- Kenmerkend voor de modellen van Schneider & Sunyaev (2015) en Conway & Curry (2012) is dat zij veel specifieker ingaan op de uitrol en/of implementatie van de clouddienst in het IT-landschap. De modellen van DNB zijn vooral gericht op de monitoring van de resultaten van de IT-performance van de cloudaanbieder.
- Kenmerkend voor het model van Schneider & Sunyaev (2015) is dat de nadruk ligt op zowel de cloudaanbieder als de klant. De andere modellen zijn alleen gericht op de klant.

5 Wet- en regelgeving

Dit hoofdstuk beschrijft de voor het onderzoek gebruikte relevante wet- en regelgeving op het gebied van cloudcomputing voor Nederlandse financiële instellingen.

5.1 (Cloud)uitbesteding algemeen

5.1.1 Regulering financiële sector

De financiële sector is sterk gereguleerd. Dit is noodzakelijk omdat de Nederlandse financiële sector de stuwende kracht is van de Nederlandse economie (DNB, 2022) en ervoor zorgt dat consumenten kunnen betalen, sparen, lenen en verzekeren (Rijksoverheid, 2022). Het is daarom belangrijk dat consumenten vertrouwen hebben in de financiële sector (DNB, 2022).

De Nederlandse financiële sector staat onder toezicht van nationale en internationale toezichthouders. Nederlandse toezichthouders zijn onder andere De Nederlandsche Bank ('DNB'), Autoriteit Financiële Markten ('AFM') en Autoriteit Persoonsgegevens ('AP'). DNB voert prudentieel toezicht uit en ziet er op toe dat partijen op de financiële markten aan hun verplichtingen kunnen voldoen. De AFM voert gedragstoezicht uit en houdt toezicht op het omgaan met klanten door financiële instellingen en de manier waarop financiële instellingen onderling met elkaar omgaan. De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens (AP, 2022). Financiële ondernemingen, zoals banken, verzekeraars en pensioenfondsen gebruiken veel persoonsgegevens. Financiële ondernemingen moeten er dan ook voor zorgen dat de privacy van klanten gewaarborgd is (AP, 2022).

Een bekende Europese toezichthouder is de Europese Centrale Bank ('ECB'). Specifiek voor de financiële sector zijn ook andere Europese toezichthouders belangrijk. Dit zijn bijvoorbeeld de European Banking Authority ('EBA') en European Insurance and Occupational Pensions Authority ('EIOPA'). Voor dit onderzoek zijn de belangrijkste toezichthouders 'EBA', 'EIOPA' en 'DNB'.

Het is banken, verzekeraars en pensioenfondsen op grond van financiële wetgeving onder voorwaarden toegestaan om werkzaamheden uit te besteden aan een dienstverlener. De voorwaarden zijn er op gericht de risico's van uitbesteding te beheersen en de uitbesteding geen belemmering te laten vormen voor het toezicht van de toezichthouders (DNB, 2020).

5.1.2 Geraadpleegde wet- en regelgeving

In dit onderzoek zijn verschillende Nederlandse en Europese wet- en regelgeving, richtsnoeren en good practices (hierna tezamen: wet- en regelgeving) geraadpleegd om te onderzoeken wat de wettelijke verplichtingen en verwachtingen van toezichthouders zijn bij het gebruik van clouddiensten door een bank, verzekeraar of pensioenfonds. In Tabel 5 is deze wet- en regelgeving per soort financiële instelling ('FI') of sector breed opgenomen. In de voetnoten zijn de wettelijke verankering van een aantal bronnen toegelicht.

Soort FI:	Geraadpleegde wet- en regelgeving:
Sector breed	• Burgerlijk wetboek • Algemene verordening gegevensbescherming • CLOUD-act • Toelichting bij meldingsformulier uitbestedingen (DNB, 2020)
Bank	• Wet op het financieel toezicht • Besluit prudentiële regels Wft • Richtsnoeren inzake uitbesteding (EBA, 2019)[6]
Verzekeraar	• Wet op het financieel toezicht • Besluit prudentiële regels Wft • Richtlijn solvency II (2009/138/EG) • Gedelegeerde Verordening Solvency II (2015/35/EU) • Richtsnoeren uitbesteding aan aanbieders van clouddiensten (EIOPA, 2020)[7] • Richtsnoeren voor het governancesysteem (EIOPA, 2015)[8] • Good practice uitbesteding verzekeraars (DNB, 2019)[9]
Pensioen-fonds	• Pensioenwet • Besluit uitvoering Pensioenwet (en Wet verplichte beroepspensioenregeling) • Besluit financieel toetsingskader pensioenfondsen • Richtlijn Institutions for Occupational Retirement Provision (2016/2341) (IORP II) • Code Pensioenfondsen (2018)[10] • Guidance uitbesteding door pensioenfondsen (DNB, 2014)[6]

Tabel 5: Overzicht geraadpleegde wet- en regelgeving

[6] De EBA *Richtsnoeren inzake uitbesteding* zijn via art. 3:18 Wft en H5 Bpr verankerd in Nederlandse wetgeving.
[7] De EIOPA *Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten* zijn via art. 3:18 Wft, 27(1), 27d en 27e Bpr verankerd in Nederlandse wetgeving.
[8] De EIOPA *Richtsnoeren voor het governancesysteem* zijn o.a. via art. 3:17 en 3:18 Wft en H5 Bpr verankerd in Nederlandse wetgeving.
[9] De DNB *Good practice uitbesteding verzekeraars* en DNB *Guidance uitbesteding door pensioenfondsen* bevatten handvatten voor het kunnen voldoen aan wet- en regelgeving.
[10] De Code Pensioenfondsen is via art. 33 Pw en art. 11 B Pw verankerd in Nederlandse wetgeving.

In de volgende sub-paragrafen wordt ingegaan op (cloud)uitbesteding en sectorbrede wet- en regelgeving.

5.1.3 Cloudcomputing: een vorm van uitbesteding

In het onderzoek is specifiek onderzocht of de termen 'cloud' en 'computing' expliciet voorkomen in de Nederlandse wet- en regelgeving via de wettenbank 'wetten.overheid.nl'. Dit is vrijwel niet het geval en als het voorkomt dan heeft het niet betrekking op financiële wetgeving. Dit houdt echter niet in dat Nederlandse toezichthouders geen wettelijke eisen stellen aan cloudcomputing of het gebruik van clouddiensten door Nederlandse financiële instellingen. Toezichthouder DNB beschouwt dit namelijk als een vorm van uitbesteding. Het wordt dan ook expliciet benoemd in de documenten *Good practice uitbesteding verzekeraars* (DNB, 2019) en *Toelichting bij meldingsformulier uitbestedingen* (DNB, 2020). Wordt de blik verbreed naar ook Europese toezichthouders EIOPA en EBA, dan zijn ook de documenten *Richtsnoeren inzake uitbesteding* (EBA, 2019) en *Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten* (EIOPA, 2020) relevant. Beide documenten omvatten uitbesteding aan aanbieders van clouddiensten. Op basis hiervan kan geconcludeerd worden dat cloudcomputing of het gebruik van clouddiensten een vorm van uitbesteding is. Bovendien bleek al eerder (zie paragraaf 4.1.2) dat de drie toezichthouders DNB, EBA en EIOPA ook de NIST-definitie (Mell & Grance, 2011) voor cloudcomputing hanteren.

5.1.4 Definitie uitbesteding

In de wetenschappelijke literatuur zijn verschillende definities van 'uitbesteding' of 'IT-uitbesteding' opgenomen. Bijvoorbeeld:

- "Uitbesteding is het doen verrichten van werkzaamheden, die betrekking hebben op het eigen product of productieproces, in een ander bedrijf dan het eigen." (Hennepe, 1954).
- "Outsourcing is een benadering waarbij een organisatie een aantal niet-kernfuncties delegeert aan gespecialiseerde en efficiënte dienstverleners." (Franceschini, et al., 2003)
- "IT-uitbesteding is een vorm van uitbesteding waarbij IT-activiteiten van een bedrijf worden uitbesteed aan een ander bedrijf." (Wikipedia, 2017).

Uit de drie voornoemde definities blijkt dat bij uitbesteding de werkzaamheden (of functies of activiteiten) door anderen worden verricht. Dit blijkt hierna ook uit de definitie van 'uitbesteden' en 'uitbesteding', zoals is opgenomen in de Wet op het financieel toezicht ('Wft'), Pensioenwet ('Pw') en het document *Richtsnoeren inzake uitbesteding* (EBA, 2019).

- "Uitbesteden: Het door een financiële onderneming verlenen van een opdracht aan een derde (of uitvoerder, in de B Pw) tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:
    - die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of
    - die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan." (Wft, art. 1:1; B Pw, art. 1)
- "Uitbesteding: een overeenkomst van om het even welke vorm tussen een instelling, een betalingsinstelling of een instelling voor elektronisch geld en een dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit verricht die anders door de instelling, betalingsinstelling of instelling voor elektronisch geld zelf zou worden verricht." (EBA, 2019)

5.1.5 Voeren administratie, bewaarplicht en geautomatiseerde gegevensverwerking

Het Burgerlijk wetboek 2 gaat over rechtspersonen. Het wetboek 2 behandelt de oprichting en ontbinding van rechtspersonen, en de interne gang van zaken (Gubbels, 2014). Voor dit onderzoek zijn twee artikelen relevant, namelijk: 2:10 en 2:293. Volgens art. 2:10 lid 1 van het Burgerlijk wetboek hebben rechtspersonen een administratie- en bewaarverplichting voor alle werkzaamheden en eisen die hieruit voortvloeien zodat de rechten en verplichtingen te allen tijde kunnen worden gekend. Alle boeken, bescheiden en andere gegevensdragers worden gedurende 7 jaar bewaard (art. 2:10 lid 3). De gegevens dienen binnen een redelijke termijn leesbaar kunnen worden gemaakt (art. 2:10 lid 4). Volgens art. 2:293 brengt de accountant verslag uit aan de raad van commissarissen en het bestuur over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

5.1.6 Gegevensbescherming

De Algemene Verordening Gegevensbescherming ('AVG') is sinds 25 mei 2018 van toepassing (AP, 2018). De AP geeft aan dat er door de komst van de AVG nog maar één privacywet geldt in de hele Europese Unie in plaats van 28 verschillende nationale wetten en dat de AVG meer is toegespitst op de gedigitaliseerde samenleving. In vergelijking met de vorige privacywet de 'Wet bescherming persoonsgegevens' hebben organisaties meer verplichtingen bij het verwerken van persoonsgegevens. Voorbeelden van veranderingen zijn dat verwerkingen niet meer bij de AP meer moeten worden gemeld, een Data Protection Impact Assessment ('DPIA') moet worden uitgevoerd indien sprake is van een 'hoog' risico voor de mensen van wie persoonsgegevens worden verwerkt en de mogelijke verplichting om een functionaris gegevensbescherming aan te stellen.

In het kader van dit onderzoek is het van belang dat bij verwerking van persoonsgegevens door de aanbieder van clouddiensten een verwerkingsovereenkomst wordt gesloten. In de verwerkersovereenkomst worden in ieder geval opgenomen (Talen, 2019):

- "welke persoonsgegevens u gaat verwerken;
- op welke manier en voor welke doelen u de persoonsgegevens gaat verwerken;
- aan welke partijen u de persoonsgegevens mag verstrekken en dat die partijen dezelfde plichten opgelegd krijgen als de verwerker;
- welke beveiligingsmaatregelen u heeft genomen (of gaat nemen) om de opgeslagen gegevens te beveiligen;
- dat de verwerkingsverantwoordelijke audits mag uitvoeren;
- hoe aan de rechten van de betrokkene, bijvoorbeeld op inzage en correctie, wordt voldaan;
- dat de verwerker ondersteunt bij het melden van eventuele datalekken;
- wanneer en op welke manier de gegevens weer verwijderd worden."

Een risico van het niet naleven van de AVG is dat het kan leiden tot lekken van persoons-gegevens. Daarnaast kan het niet naleven van de AVG leiden tot boetes variërend van 2-4% van de wereldwijde jaarlijkse omzet met een maximum van EUR 20 miljoen (AP, 2018).

5.1.7 Datawetgeving met extraterritoriale werking

De meeste wet- en regelgeving die voor dit onderzoek is geraadpleegd heeft betrekking op Nederland en Europa. Maar ook bepaalde andere buitenlandse wet- en regelgeving kan relevant zijn voor de beheersing van het gebruik van clouddiensten. Uit een onderzoek dat in opdracht van het NCSC in 2022 is uitgevoerd door het advocatenkantoor GreenbergTraurig, blijkt dat Europese bedrijven met dataverwerkingen in Europa onder de werking van de Amerikaanse CLOUD-act kunnen vallen (NCSC, 2022). CLOUD-act betekent voluit 'Clarifying Lawful Overseas Use of Data Act' (Wikipedia, 2022). De CLOUD-act heeft daarmee een extraterritoriale werking. Aldus het NCSC (2022) is de CLOUD-act niet de enige wetgeving met extraterritoriale werking. De GDPR (in Nederland bekend als de 'AVG', zie paragraaf 5.1.6) geldt ook buiten Europa en bijvoorbeeld China heeft de Data Security Law ('DSL') met extraterritoriale werking. De DSL regelt de verwerking van data in China, maar ook daarbuiten. Mits deze relevant is voor de nationale veiligheid of andere maatschappelijke belangen van China.

5.1.8 Beheerste en integere bedrijfsvoering

Volgens het artikel 3:17 van de Wet op het financieel toezicht ('Wft') en artikel 143 van de Pensioenwet ('Pw') moeten banken, verzekeraars en pensioenfondsen waarborgen treffen voor een beheerste en integere bedrijfsvoering. De genoemde wetsartikelen komen op hoofdlijnen met elkaar overeen en per soort financiële instelling kunnen specifieke eisen aanwezig zijn. De overeenkomstige eisen voor beheerste en integere bedrijfsvoering hebben onder meer betrekking op het beheersen van bedrijfsprocessen en bedrijfsrisico's, integriteit en soliditeit (dit is o.a. de beheersing van financiële risico's). Specifieke eisen hebben bijvoorbeeld betrekking op de goede en veilige werking van het betalingsverkeer (banken) en het beheersen van de financiële positie op de lange termijn (pensioenfondsen). In dit onderzoek ligt de nadruk op het beheersen van processen en niet-financiële bedrijfsrisico's. Aanvullend zijn in het Besluit prudentiële regels Wft (*alleen banken en verzekeraars*), Richtlijn Solvency II en Gedelegeerde Verordening (*alleen verzekeraars*), Besluit financieel toetsingskader, Code Pensioenfondsen en Richtlijn IORP II (*alleen pensioenfondsen*) nadere uitwerkingen opgenomen voor de inrichting en uitvoering van de beheerste en integere bedrijfsvoering.

Voorbeelden van nadere uitwerkingen zijn de uitvoering van een systematische (integriteits-) risicoanalyse, omgaan met incidenten, deskundigheid, een goede administratie met interne controle mechanismes, functiescheiding, risicobeheersing en een ten minste jaarlijkse onafhankelijke toetsing van de effectiviteit van de organisatie-inrichting, procedures en maatregelen.

Beheerste en integere bedrijfsvoering omvat het gehele traject van plannen, sturen, monitoren en bijsturen, van de doelstellingen, processen en risico's (DNB, 2019). De adviesorganisatie Sprenkels & Verschuren (2022) schrijft dat de kern van beheerste en integere bedrijfsvoering is het hebben van goed beleid, deskundigheid en betrouwbaarheid. En dat het gaat om het beheerst hebben én houden van processen, structuren en systemen in de bedrijfsvoering.

5.1.9 Uitbesteding van werkzaamheden

Volgens het artikel 3:18 van de Wet op het financieel toezicht ('Wft') en artikel 34 van de Pensioenwet ('Pw') moeten banken, verzekeraars en pensioenfondsen bij de uitbesteding van werkzaamheden aan een derde ('de dienstverlener) er voor zorgdragen dat deze dienstverlener de regels die van toepassing zijn op de financiële instelling naleeft. In deze artikelen en ook in de nadere uitwerking in het Besluit prudentiële regels Wft (*alleen banken en verzekeraars*), Richtlijn Solvency II (*alleen verzekeraars*) en het Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling en IORP II (*alleen pensioenfondsen*) zijn bepalingen opgenomen over bijvoorbeeld werkzaamheden die niet mogen worden uitbesteed, vereisten waar de financiële instelling aan moet voldoen, het tijdig in kennis stellen van de toezichthouder over het voornemen van uitbesteding, beheersing van risico's bij uitbesteding en de overeenkomst tussen de financiële instelling en de dienstverlener.

De financiële instelling moet voorafgaand aan het gebruik maken van clouddiensten bepalen of sprake is van uitbesteding (zie paragraaf 5.3.1). Indien een partij waaraan wordt uitbesteed zelf geen clouddiensten aanbiedt, maar sterk afhankelijk is van cloudinfrastructuren dan kunnen hiervoor dezelfde eisen gelden alsof aan een aanbieder van clouddiensten zou worden uitbesteed (EIOPA, 2020). Bepaalde functies of diensten worden niet geschaard onder de definitie van uitbesteding (EBA, 2019). Voorbeelden hiervan zijn: uitvoering van wettelijke audits, diensten van correspondentbanken en aankopen van diensten, zoals: verstrekken van juridisch advies en nutsvoorzieningen.

5.2 (Cloud)uitbesteding beleid & governance

In deze paragraaf is beschreven welke eisen worden gesteld aan het uitbestedingsbeleid en de governance van de organisatie. Achtereenvolgend worden de volgende onderwerpen behandeld: uitbestedingsbeleid & -procedures, kritieke of belangrijke functies, deskundigheid, schriftelijke kennisgeving aan toezichthouders, bedrijfscontinuïteitsplannen en uitbestedings-register. In Bijlage 2a zijn de bronnen voor deze paragraaf per sub-paragraaf weergegeven. In Bijlage 3 zijn (indien aanwezig) per sub-paragraaf voorbeelden opgenomen. Dit laatste is expliciet beschreven per sub-paragraaf.

5.2.1 Uitbestedingsbeleid & -procedures

Toezichthouder DNB verwacht dat verzekeraars (DNB, 2019) en pensioenfondsen (DNB, 2014) starten met het uitvoeren van een systematische risicoanalyse en het definiëren van een doelstelling en reikwijdte van uitbesteding. De doelstelling, reikwijdte en randvoorwaarden worden vastgelegd in het schriftelijke uitbesteding beleid dat wordt goedgekeurd door het bestuur van de financiële instelling. Het bestuur blijft altijd eindverantwoordelijk voor alle activiteiten van de financiële instelling.

In het uitbestedingsbeleid worden de overwegingen opgenomen op grond waarvan tot uitbesteding kan worden besloten en de randvoorwaarden waaronder dit plaatsvindt (DNB, 2019). Dat is uitgewerkt in administratieve en organisatorische procedures die worden uitgedragen naar de medewerkers van de financiële instelling (DNB, 2014). Het uitbestedingsbeleid omvat alle aspecten van uitbesteding (zie paragrafen 5.2.2 t/m 5.6.2) en wordt ten minste eenmaal per drie jaar geëvalueerd of deze nog in lijn is met de strategie van de financiële instelling. In Bijlage 3 is een overzicht met vereisten, voorwaarden en overige informatie voor in het uitbestedingsbeleid opgenomen.

5.2.2 Kritieke of belangrijke functies

Voor de uitbesteding is het belangrijk om vast te stellen of sprake is van “Kritieke of belangrijke functies” (EBA, 2019) of “Kritieke of belangrijke operationele functies of activiteiten” (DNB, 2019; EIOPA, 2020). Hiermee wordt bedoeld dat een uitbesteding materieel of van wezenlijk belang is voor de financiële instelling (DNB, 2019).

Een gebrekkige of tekortschietende uitvoering van de diensten leidt tot materiële nadelige gevolgen voor het voldoen aan wet- en regelgeving, financiële resultaten en soliditeit of continuïteit van de financiële instelling (EBA, 2019). Of anders gezegd, dat de uitbestede functie of activiteit van essentieel belang is voor de bedrijfsvoering van de onderneming in de zin dat de onderneming zonder deze functie niet in staat is om haar diensten te verlenen (EIOPA, 2020). In Bijlage 3 is een overzicht met voorbeelden van voorwaarden opgenomen voor het beoordelen of sprake is van kritieke of belangrijke uitbesteding.

Opmerking: *In het vervolg van het onderzoek wordt voor het aanduiden van "Kritieke of belangrijke functies" of "Kritieke of belangrijke operationele functies of activiteiten", gemakshalve alleen gesproken over "Kritieke of belangrijke functies", tenzij anders aangeduid.*

5.2.3 Deskundigheid

De financiële instelling beschikt over voldoende 'countervailing power' / 'tegenwicht' ten opzichte van de dienstverlener (DNB, 2014). Dat wil zeggen dat het bestuur (eventueel ondersteunt door een bestuursbureau of regieorganisatie) beschikt over de benodigde kennis en competenties voor het houden van regie op de uitbesteding, de uitbestede werkzaamheden adequaat te beoordelen en tijdig bij te sturen. Voorstellen van de dienstverlener worden beargumenteerd met voor- en nadelen en waar mogelijk met alternatieven. Daarnaast beschikt de financiële instelling over voldoende deskundigheid (bijv. ICT en bedrijfskennis) die nodig is om risico's en de beheersing van de uitbestedingsrelatie te beoordelen.

5.2.4 Schriftelijke kennisgeving aan toezichthouders

Een financiële instelling stelt toezichthouders in kennis van voorgenomen uitbestedingen van "kritieke of belangrijke functies". Ook informeert een financiële instelling de toezichthouder(s) tijdig over materiële wijzigingen en/of ernstige gebeurtenissen bij dienstverleners die grote gevolgen kunnen hebben op het voortzetten van de bedrijfsactiviteiten van de financiële instelling. In Bijlage 3 is een overzicht met voorbeelden van informatie die moet worden gemeld aan de toezichthouder opgenomen.

5.2.5 Bedrijfscontinuïteitsplannen

Financiële instellingen hebben passende bedrijfscontinuïteitsplannen met betrekking tot kritieke of belangrijke functies, onderhouden deze en testen deze plannen periodiek. In de bedrijfscontinuïteitsplannen wordt rekening gehouden dat de kwaliteit van de kritieke of belangrijke functies verslechterd of niet meer wordt uitgevoerd. In de bedrijfscontinuïteits-plannen wordt rekening gehouden met mogelijke gevolgen van insolventie of andere vormen van falen van de dienstverlener en, waar relevant, politieke risico's in het rechtsgebied van de dienstverlener.

5.2.6 Uitbestedingsregister

De financiële instelling moet zicht houden op de keten van uitbesteding (Code Pensioenfondsen, 2018) en moet als onderdeel van haar governance- en risicobeheer-systeem haar (cloud)uitbestedingen documenteren in bijvoorbeeld een uitbestedingsregister (EIOPA, 2020; EBA, 2019). Dit register wordt regelmatig bijgewerkt. In Bijlage 3 is een overzicht met voorbeelden van informatie opgenomen die in het uitbestedingsregister voor kritieke of belangrijke functies moet worden opgenomen.

Voor niet kritieke of belangrijke functies moet de financiële instelling op basis van aard, omvang en de complexiteit van de inherente risico's bepalen welke informatie wordt bijgehouden in het uitbestedingsregister.

5.3 (Cloud)uitbesteding selectie dienstverlener

In deze paragraaf is beschreven welke eisen worden gesteld aan het selecteren van een dienstverlener. Voorafgaand aan de uitbesteding voert een financiële instelling een analyse uit. Hieronder begrepen de beoordeling of sprake is van kritieke of belangrijke functies, de risicobeoordeling vóór uitbesteding en de uitvoering van het due diligence onderzoek ten aanzien van de toekomstige dienstverlener. Indien een partij waaraan wordt uitbesteed zelf geen clouddiensten aanbiedt, maar sterk afhankelijk is van cloudinfrastructuren dan kunnen hiervoor dezelfde eisen gelden alsof aan een aanbieder van clouddiensten zou worden uitbesteed (EIOPA, 2020). In Bijlage 2a zijn de bronnen voor deze paragraaf per sub-paragraaf weergegeven.

5.3.1 Beoordeling kritieke of belangrijke functies

De financiële instelling moet voorafgaand aan het gebruik maken van clouddiensten of sprake is van de uitbesteding van “Kritieke of belangrijke functies” (zie paragraaf 5.2.2).

5.3.2 Risicobeoordeling vóór uitbesteding

De financiële instelling moet vóór de uitbesteding een risicobeoordeling uitvoeren. Hierbij moet een benadering worden gehanteerd die in verhouding staat tot de aard, de omvang en complexiteit van de inherente risico’s van de uitbestede clouddiensten. Hierbij moet rekening gehouden worden met de operationele en reputatie risico’s.

In het geval van uitbesteding van kritieke of belangrijke functies moet een financiële instelling (indien van toepassing en waar nodig) de juridische-, ICT-, naleving- en reputatierisico’s en toezichtbeperkingen beoordelen die het gevolg kunnen zijn van het soort clouddienst, migratie en/of implementatie, de gevoeligheid van gegevens, systemen en de beveiligingsmaatregelen, politieke stabiliteit en beveiligingssituatie waar de activiteiten worden uitgevoerd en de gegevens worden opgeslagen, onderuitbesteding (incl. lange en complexe ketens van onderuitbesteding) en concentratierisico. Voorafgaand aan uitbesteding van “Kritieke of belangrijke operationele functies of activiteiten” wordt een grondige risicobeoordeling uitgevoerd (EIOPA, 2020). Hierin worden onder meer opgenomen: ICT-risico, bedrijfscontinuïteit, naleving van wet- en regelgeving, concentratie risico, operationeel risico en indien van toepassing risico’s met betrekking tot gegevensmigratie en/of de implementatie (EIOPA, 2020).

5.3.3 Due diligence onderzoek

De financiële instelling voert voorafgaand aan een uitbesteding een due diligence onderzoek (= selectie- en beoordelingsonderzoek) uit. Het doel is om vast te stellen dat de dienstverlener kan voldoen aan de vereisten in het uitbestedingsbeleid. In het geval van uitbesteding van kritieke of belangrijke functies moet een evaluatie van geschiktheid van de dienstverlener worden opgenomen ten aanzien van bijvoorbeeld: vaardigheden, infrastructuur, economische situatie en bedrijfs- en juridische status. In het due diligence onderzoek kan gebruik worden gemaakt van certificeringen op basis van internationale normen en interne of externe audit rapportages.

De volgende aspecten komen onder meer aan bod in het due diligence onderzoek bij uitbesteding van een kritieke of belangrijke functie: bedrijfsreputatie, passende en toereikende bekwaamheden, deskundigheid, capaciteit, middelen (bijv. personeel, IT en financieel), beloningsbeleid, organisatiestructuur en bedrijfsmodel (incl. karakter, omvang, complexiteit, financiële situatie, eigendoms- en groepsstructuur). Indien de uitbesteding ook het verwerken van persoonsgegevens of vertrouwelijke gegevens betreft, dan moeten ook passende technische en organisatorische maatregelen worden getroffen om deze persoonsgegevens of vertrouwelijke gegevens te beschermen.

De financiële instellingen moeten ook de nodige stappen zetten om ervoor te zorgen dat dienstverleners handelen op een wijze die strookt met hun waarden en gedragscode, met name wat betreft dienstverleners in derde landen en hun onderaannemers, zoals: ethische en maatschappelijke verantwoorde handelswijze, internationale normen op het gebied van mensenrechten, milieubescherming en passende arbeidsomstandigheden (incl. verbod op kinderarbeid).

5.4 (Cloud)uitbesteding overeenkomst

In deze paragraaf is beschreven welke eisen worden gesteld aan de uitbestedings-overeenkomst. Achtereenvolgend worden de volgende onderwerpen behandeld: uitbestedingsovereenkomst (algemeen), beveiliging van gegevens en systemen, toegangs-, informatie- en auditrechten, onderuitbesteding en beëindigingsrechten.
In Bijlage 2a zijn de bronnen voor deze paragraaf per sub-paragraaf weergegeven. In Bijlage 3 zijn (indien aanwezig) per sub-paragraaf voorbeelden opgenomen. Dit laatste wordt expliciet vermeld per sub-paragraaf.

5.4.1 Uitbestedingsovereenkomst (algemeen)

De rechten en plichten van de financiële instelling en de dienstverlener worden opgenomen in een schriftelijke overeenkomst. In Bijlage 3 is een overzicht met rechten en plichten voor in de uitbestedingsovereenkomst opgenomen.

5.4.2 Beveiliging van gegevens en systemen

De financiële instelling neemt in de uitbestedingsovereenkomst eisen voor beveiliging van gegevens en systemen op en ziet er op toe dat deze eisen worden nageleefd. In Bijlage 3 zijn voorbeelden van de vereisten voor de beveiliging van gegevens en systemen opgenomen.

5.4.3 Toegangs-, informatie- en auditrechten

Een belangrijke voorwaarde aan uitbesteding is dat deze geen belemmering mag vormen voor de effectieve uitoefening van over toegangs-, informatie- en auditrecht van de financiële instelling en haar toezichthouder(s). De financiële instelling neemt voor uitbesteding van kritieke of belangrijke functies in de uitbestedingsovereenkomst voorwaarden op over toegangs-, informatie- en auditrechten. In Bijlage 3 is een overzicht met voorwaarden over toegangs-, informatie- en auditrechten opgenomen.

De financiële instellingen mogen gebruik maken van door de dienstverlener verstrekte externe certificeringen en externe of interne auditverslagen. De financiële instelling zijn verantwoordelijk om te beoordelen of deze certificeringen en auditverslagen voldoende zijn om aan hun regelgevingsverplichtingen te voldoen. Hierbij moet onder meer rekening worden gehouden met de reikwijdte en uitvoering van de audit volgens gepaste normen. Bovendien mogen ze op termijn niet uitsluitend vertrouwen op deze certificeringen en auditverslagen.

De financiële instelling moet het recht hebben om uitbreiding van de reikwijdte van de certificeringen of auditrapportages mits dit naar redelijkheid is. Daarnaast moet de financiële instelling het recht behouden om naar eigen inzicht individuele audits op locatie uit te voeren. Aangezien cloudoplossingen technisch bijzonder complex zijn, moet de financiële instelling er voor zorgdragen dat de door haar aangestelde auditors over de juiste vaardigheden beschikken. Indien de uitoefening van het toegangs- of auditrecht een risico oplevert voor de omgeving van de aanbieder van clouddiensten en/of andere klanten van de aanbieder van clouddiensten, dan moeten de financiële instelling en aanbieder van clouddiensten een alternatieve manier overeenkomen om een vergelijkbaar niveau van betrouwbaarheid en dienstverlening te verwezenlijken (bijvoorbeeld een verslag of specifieke certificering).

5.4.4 Onderuitbesteding

De financiële instelling neemt in de uitbestedingsovereenkomst op onder welke voorwaarden onderuitbesteding is toegestaan (of niet). In Bijlage 3 is een overzicht met eisen opgenomen met betrekking tot onderuitbesteding opgenomen.

5.4.5 Beëindigingsrechten

De financiële instelling neemt (bijvoorbeeld door middel van een ‘exitstrategie clausule’) in de uitbestedingsovereenkomst op onder welke (wettelijke) voorwaarden de uitbestedings-overeenkomst moet worden beëindigd. In Bijlage 3 is een overzicht met voorwaarden waarbij de uitbestedingsovereenkomst moet worden beëindigd opgenomen.

5.5 (Cloud)uitbesteding monitoring dienstverlener

In deze paragraaf is beschreven welke eisen worden gesteld aan de monitoring van de dienstverlener. Achtereenvolgend worden de volgende onderwerpen behandeld: monitoring- & controlemechanisme, bewaken prestaties & informatiebeveiliging dienstverlener, beoordelen assurance rapportage & opvolging bevindingen en bijwerken risicobeoordeling. In Bijlage 2a zijn de bronnen voor deze paragraaf per sub-paragraaf weergegeven. In Bijlage 3 zijn (indien aanwezig) per sub-paragraaf voorbeelden opgenomen. Dit laatste wordt expliciet vermeld per sub-paragraaf.

5.5.1 Monitoring- & controlemechanisme

Voor de monitoring moet de financiële instelling monitoring- en controlemechanisme inrichten en zorgen voor voldoende personeel dat over voldoende vaardigheden en kennis (zie paragraaf 5.2.3) beschikt om het gebruik van clouddiensten te monitoren.

5.5.2 Bewaken prestaties & informatiebeveiliging dienstverlener

De financiële instelling monitort risk-based voortdurend de prestaties van activiteiten, de beveiligingsmaatregelen en naleving van de overeengekomen afspraken via een risico gebaseerde aanpak in de zin dat de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en informatie wordt gewaarborgd. De nadruk moet hierbij liggen op kritieke of belangrijke functies. In Bijlage 3 zijn voorbeelden van rapportages opgenomen.

5.5.3 Beoordelen assurance rapportage & opvolging bevindingen

De financiële instelling beoordeelt assurance rapportages, waarbij aandacht is voor onder meer de reikwijdte, aansluiting met de uitbestede dienst en periode waarover assurance is afgegeven. De financiële instelling monitort de opvolging van bevindingen in assurance rapportages actief en treft maatregelen als tekortkomingen (bijv. het niet voldoen aan wet- en regelgeving) worden geconstateerd. Passende corrigerende of herstelmaatregelen moeten worden getroffen. Indien dit niet mogelijk is, dan wordt de uitbestedingsovereenkomst met onmiddellijke ingang beëindigd. In Bijlage 3 zijn voorbeelden van rapportages opgenomen.

5.5.4 Bijwerken risicobeoordeling

Onderdeel van de monitoring betreft ook het regelmatig bijwerken van de risicobeoordeling die in het selectieproces is uitgevoerd (zie paragraaf 5.3.2). Hieronder begrepen de monitoring van het concentratierisico die door meerdere cloud uitbestedingen kunnen ontstaan. Over de uitkomsten van de risicobeoordeling wordt gerapporteerd aan het bestuur.

5.6 (Cloud)uitbesteding evaluatie dienstverlener

In deze paragraaf is beschreven welke eisen worden gesteld aan de evaluatie van uitbesteding. De volgende onderwerpen worden behandeld: evaluatie dienstverlener en exitstrategie. In Bijlage 2a zijn de bronnen voor deze paragraaf per sub-paragraaf weergegeven. In Bijlage 3 zijn (indien aanwezig) per sub-paragraaf voorbeelden opgenomen. Dit laatste wordt expliciet vermeld per sub-paragraaf.

5.6.1 Periodieke evaluatie

De evaluatie van de dienstverlener vindt plaats aan de hand van de randvoorwaarden en eisen in het uitbestedingsbeleid (zie paragraaf 5.2.1). Ook wordt beoordeeld of de dienstverlener bijdraagt aan het behalen van doelen van de financiële instelling. De evaluatie van de dienstverlener bij een kritieke of belangrijke functie wordt minimaal jaarlijks uitgevoerd. Hierbij worden onder meer het behalen van de performance afspraken, uitkomsten van de monitoring (zie paragraaf 5.5.2) en mogelijke grote wijzigingen geëvalueerd bij de dienstverlener, zoals: wijzigingen in de strategie en de eigendomsverhoudingen. De evaluatie leidt tot een besluit om de uitbesteding te continueren of te beëindigen.

5.6.2 Exitstrategie

De financiële instelling heeft voor uitbesteding van kritieke of belangrijke functies een gedocumenteerde exitstrategie in lijn met het uitbestedingsbeleid en business continuity plannen. In de exitstrategie wordt onder meer rekening gehouden dat de uitbestedingsovereenkomst wordt beëindigd, de dienstverlener faalt en de kwaliteit van de dienst verslechterd of kan leiden tot bedrijfsverstoringen. De exitstrategieën beogen er aan te kunnen bij dragen dat financiële instellingen zich kunnen terugtrekken zonder dat dit hun bedrijfsactiviteiten onnodig verstoord, regelgevingsvereisten minder goed naleven en zonder dat dit ten koste gaat van de continuïteit en kwaliteit van hun dienstverlening aan klanten. Hiertoe worden exitplannen ontwikkeld en geïmplementeerd die volledig, gedocumenteerd en waar nodig getoetst zijn. Daarnaast onderzoeken de financiële instellingen alternatieve oplossingen, stellen zij overgangsplannen op waarmee de uitbestede functies en gegevens bij de dienstverlener kan weghalen en ervoor zorgdragen dat de kritieke of belangrijke of activiteiten kunnen worden voortgezet (intern of bij een andere dienstverlener). In Bijlage 3 zijn voorbeelden van activiteiten voor het bepalen van een exitstrategie opgenomen.

6 Conceptueel model voor(cloud)uitbesteding

In dit hoofdstuk is de wetenschappelijke literatuur en wet- en regelgeving gebruikt voor de totstandkoming van een conceptueel model voor de beheersing van clouduitbesteding door een Nederlandse financiële instelling.

6.1 Totstandkoming conceptueel (cloud)uitbestedingsmodel

Het conceptueel (cloud)uitbestedingsmodel is tot stand gekomen op basis van onderzoek in wetenschappelijke literatuur en wet- en regelgeving voor Nederlandse financiële instellingen. Daarnaast is gebruik gemaakt van praktijkervaring van de auteur. De auteur heeft ruim negentien jaar werkervaring waarvan vier jaar in de accountancy, zes jaar in compliance & business proces outsourcing (voor de bancaire sector) en de laatste ruim negen jaar in het vakgebied operationeel riskmanagement (incl. operationeel-, uitbesteding-, IT- en juridische risico's) in de pensioensector.

6.1.1 Identificatie wettelijke vereisten – (cloud)uitbestedingscyclus

Het onderzoek is van start gegaan met een verkennend literatuuronderzoek met betrekking tot cloudcomputing en (cloud)levenscyclus modellen. Vervolgens is onderzocht welke wet- en regelgeving in Nederland en Europa van toepassing is op banken, verzekeraars en pensioenfondsen. Hiervoor is allereerst een overzicht opgesteld met Nederlandse en Europese instituten & toezichthouders met betrekking tot de financiële sector, namelijk: ECB, ESFS, ESRB, EBA, ESMA, EIOPA, DNB, AFM en AP (zie Bijlage 9 – Afkortingenlijst). Via de websites van deze instituten & toezichthouders is onderzocht welke wet- en regelgeving relevant is voor uitbesteding aan aanbieders van (cloud)diensten en welke toezichthouders het meest belangrijk zijn voor dit onderzoek (zie paragraaf 5.1.1). Vervolgens is analyse uitgevoerd om de wettelijke vereisten en toezichthouder verwachting op basis van wetgeving, richtsnoeren en good practices te identificeren. Parallel is gestart met het ordenen van onderwerpen op basis waarvan de wettelijke vereisten en verwachtingen kunnen worden geordend. Het geheel is na enkele iteraties in één groot overzicht verwerkt, zie hiervoor Bijlage 2a. In Bijlage 2b is het grote overzicht in Bijlage 2a ontrafeld voor banken, verzekeraars en pensioenfondsen. Dit kan praktisch(er) zijn voor een gebruiker van één of meerdere van de drie geselecteerde financiële instellingen (banken, verzekeraars of pensioenfondsen).

6.1.2 Concretisering wettelijke vereisten, voorwaarden en overige informatie

De geraadpleegde wetgeving, richtsnoeren en good practices in het onderzoek is behoorlijk omvangrijk. Daarom is de structuur van de paragrafen 5.1 t/m 5.6 in lijn gebracht met het overzicht met wettelijke vereisten (zie Bijlage 2a). Vervolgens zijn in Bijlage 3 deze wettelijke vereisten tezamen met voorwaarden en overige relevante informatie meer gedetailleerd uitgewerkt. Ook deze Bijlage 3 sluit aan op de paragrafen 5.1 t/m 5.6 en Bijlage 2a.

6.2 Conceptueel (cloud)uitbestedingsmodel in zes onderdelen

Het conceptueel (cloud)uitbestedingsmodel bestaat op hoofdlijnen uit zes onderdelen. Dit wordt hieronder weergegeven door middel van een tabel, figuur en checklist.

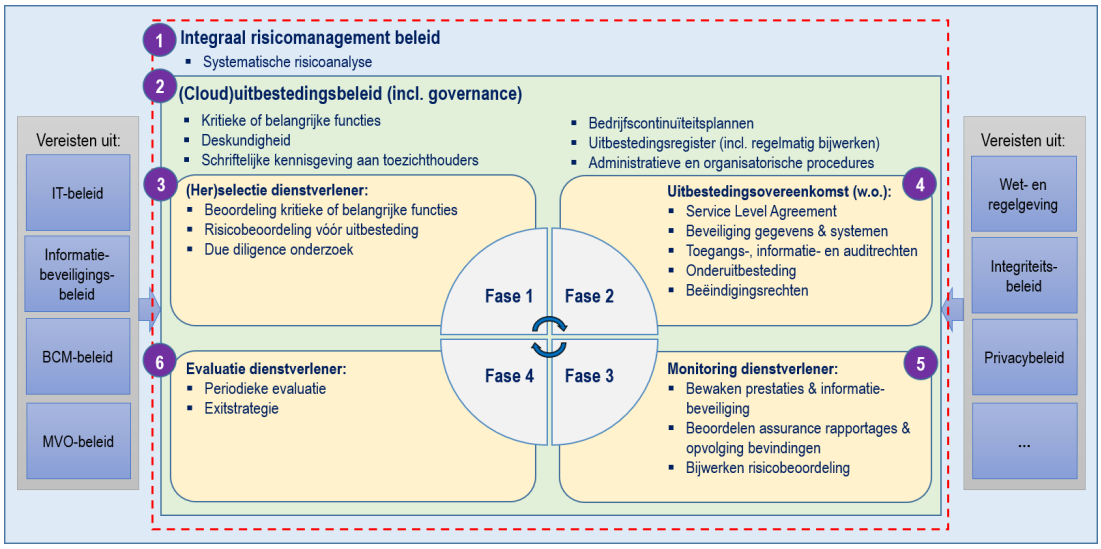
6.2.1 Concretisering conceptueel (cloud)uitbestedingsmodel - tabel

In de Tabel 6 hieronder zijn de zes onderdelen van het conceptueel (cloud)uitbestedings-model met verwijzingen naar de relevante sub-paragrafen in hoofdstukken 4 en 5 opgenomen.

#	Onderdelen conceptueel (cloud)uitbestedingsmodel op hoofdlijnen	Paragraaf
1	**Risicomanagement**	
	• Systematische risicoanalyse	• 4.2.2
	• Periodieke uitbestedingsrisicoanalyse voor KOB	• 4.2.3
2	**(Cloud)uitbestedingsbeleid & -governance**	
	• Uitbestedingsbeleid & -procedures	• 5.2.1
	• Kritieke of belangrijke functies	• 5.2.2
	• Deskundigheid	• 5.2.3
	• Schriftelijke kennisgeving aan toezichthouders	• 5.2.4
	• Bedrijfscontinuïteitsplannen	• 5.2.5
	• Uitbestedingsregister	• 5.2.6
3	**Selectie dienstverlener**	
	• Beoordeling kritieke of belangrijke functies	• 5.3.1
	• Risicobeoordeling vóór uitbesteding	• 5.3.2
	• Due diligence onderzoek	• 5.3.3
4	**Uitbestedingsovereenkomst**	
	• Uitbestedingsovereenkomst (algemeen)	• 5.4.1
	• Beveiliging van gegevens en systemen	• 5.4.2
	• Toegangs-, informatie- en auditrechten	• 5.4.3
	• Onderuitbesteding	• 5.4.4
	• Beëindigingsrechten	• 5.4.5
5	**Monitoring dienstverlener**	
	• Monitoring- & controlemechanisme	• 5.5.1
	• Bewaken prestaties & informatiebeveiliging dienstverlener	• 5.5.2
	• Beoordelen assurance rapportages & opvolging bevindingen	• 5.5.3
	• Bijwerken risicobeoordeling	• 5.5.4
6	**Evaluatie dienstverlener**	
	• Periodieke evaluatie	• 5.6.1
	• Exitstrategie	• 5.6.2

Tabel 6: Overzicht met onderdelen conceptueel (cloud)uitbestedingsmodel

6.2.2 Concretisering conceptueel (cloud)uitbestedingsmodel - figuur



Figuur 8: Conceptueel (cloud)uitbestedingsmodel

Figuur 8 presenteert het conceptueel (cloud)uitbestedingsmodel.

Het conceptueel (cloud)uitbestedingsmodel bestaat uit zes hoofdonderdelen conform Tabel 6 (zie het gebied binnen de rode stippellijn). In Bijlage 4 (checklist) zijn details voor de stappen weergegeven, waarbij op onderdelen wordt verwezen naar Bijlage 3 waarin detailvereisten zijn opgenomen. Hieronder zijn de zes onderdelen beknopt beschreven.

1. **Integraal risicomanagementbeleid**: Vormt het beleid over de wijze van inrichting van de risicobeheerfunctie en het risicobeheersingsproces. Een belangrijke risicoanalyse is de systematische risicoanalyse, waarin naast uitbestedingsrisico's ook risico's van aanpalende beleidsgebieden, zoals IT en privacy worden meegenomen. Een uitkomst hiervan kan zijn dat bepaalde kernactiviteiten kunnen worden uitbesteed.
2. **(Cloud)uitbestedingsbeleid (incl. governance):** Hierin zijn de overwegingen op grond waarvan tot uitbesteding kan worden overgegaan opgenomen en de randvoorwaarden waaronder uitbesteding plaatsvindt. De governance omvat specifieke voorwaarden en het uitbestedingsproces (zie stappen 3 t/m 6). Deze stappen in het uitbestedingsproces moeten cyclisch worden uitgevoegd.
3. **(Her)selectie dienstverlener:** In deze stap is opgenomen hoe en op basis van welke voorwaarden de financiële instelling een dienstverlener selecteert. Hieronder begrepen een beoordeling of sprake is van uitbesteding van 'kritieke of belangrijke functies' en een risicoanalyse (zie Bijlage 8 – Template RSA Clouduitbesteding).

4. **Uitbestedingsovereenkomst:** Hierin worden de afspraken met de dienstverlener opgenomen op basis van het uitbestedingsbeleid. Dit vormt de basis hoe de financiële instelling kan voldoen aan wet- en regelgeving en invulling kan geven aan haar eindverantwoordelijkheid.
5. **Monitoring dienstverlener:** de financiële instelling bewaakt dat de dienstverlener zich aan de afspraken in de uitbestedingsovereenkomst en SLA houdt. In deze stap wordt ook de risicoanalyse bijgewerkt.
6. **Evaluatie dienstverlener:** de financiële instelling evalueert periodiek het functioneren van de dienstverlener in alle stappen van het uitbestedingsproces. Afhankelijk van de uitkomsten blijft de financiële instelling bij de dienstverlener, treft zij corrigerende maatregelen (bij stap 4) of selecteert zij een andere dienstverlener (bij stap 3).

In Bijlage 4 zijn de wettelijke vereisten en verwachting van toezichthouders omgezet in een checklist door middel van beheersingsmaatregelen. Deze zijn door de auteur geformuleerd. Dit vereenvoudigt namelijk de validatie van het conceptueel (cloud)uitbestedingsmodel aan de hand van de casestudy.

6.3 Verschillen met bestaande (cloud)uitbestedingsmodellen

Het conceptueel (cloud)uitbestedingsmodel heeft raakvlak met de cloudlevenscyclus- & uitbestedingscyclus modellen zoals beschreven in paragraaf 4.3. Ons conceptueel model is echter gebaseerd op een combinatie van actuele nationale en internationale wet- en regelgeving voor banken, verzekeraars en pensioenfondsen. Hierdoor is een uniform conceptueel model ontstaan voor deze financiële instellingen, ofschoon het in de praktijk zelden tot nooit voorkomt dat een financiële instelling een combinatie is van bank, verzekeraar én pensioenfonds. Het model is daarom conceptueel. Het conceptueel model kan daarentegen wel praktische handvatten bieden voor verschillende Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse aanbieders. Het kan tevens bijdragen aan het invulling geven aan de beheerste en integere bedrijfsvoering.

7 Resultaten en analyse

Dit hoofdstuk beschrijft de resultaten van het onderzoek aan de hand van de beantwoording van de deelvragen zoals geformuleerd in paraaf 2.4. Zie de onderstaande Tabel 7.

#	Deelvraag	Antwoord
1	Wat is cloudcomputing en wie bieden clouddiensten aan?	Cloudcomputing is beschreven in de sub-paragrafen 4.1.1 t/m 4.1.6. De letterlijke definitie van cloudcomputing is opgenomen in paragraaf 4.1.2, waarbij de NIST-definitie (Mell & Grance, 2011) het meest voorkomend is. De paragraaf 4.1.7 geeft inzicht in de aanbieders van clouddiensten. De drie grootste aanbieders van clouddiensten zijn het Amerikaanse Amazon Web Services ('AWS'), Microsoft Azure en Google Cloud.
2	Wat zijn de belangrijkste risico's van het gebruik van clouddiensten door Nederlandse financiële instellingen?	In de sub-paragrafen 4.2.4 & 4.2.5 zijn de belangrijkste risico's voor het gebruik van clouddiensten uit dit onderzoek opgenomen. Hiervoor is gebruik gemaakt van een overzicht (Tabel 3; zie sub-paragraaf 4.2.4) met risico's van toezichthouder DNB (2020) aangevuld met in dit onderzoek geïdentificeerde aanvullende uitbestedingsrisico's in Tabel 4 (zie sub-paragraaf 4.2.5). In Bijlage 8 zijn deze twee tabellen opgenomen met een aanpassing, namelijk: Tabel 3 die is omgezet voor uitbesteding aan aanbieders van clouddiensten en Tabel 4 die is verrijkt op basis van antwoorden in de interviews (zie sub-paragraaf 8.3.2).
3	Welke cloudlevenscyclus-/uitbestedings-cyclusmodellen zijn beschreven in de wetenschappelijke literatuur en wat zijn de verschillen hiertussen?	In sub-paragrafen 4.3.1 t/m 4.3.4 zijn twee cloudlevenscyclus modellen en twee uitbestedingscyclusmodellen onderzocht. In sub-paragraaf 4.3.5 zijn de belangrijkste overeenkomsten en verschillen tussen de modellen weergegeven.
4	Welke wettelijke vereisten & toezichthouder verwachtingen gelden voor Nederlandse financiële instellingen bij uitbesteding en het gebruik maken van clouddiensten?	Ondanks dat de reikwijdte van Nederlandse financiële instelling beperkt was tot alleen banken, verzekeraars en pensioenfondsen was dit een omvangrijke analyse. De wettelijke vereisten voor deze financiële instellingen zijn beknopt beschreven in de paragrafen 5.1 t/m 5.6. Ter ondersteuning hiervan zijn de Bijlagen 2a, 2b en 3 aanwezig.
5	Welke maatregelen moet een Nederlandse financiële instelling nemen om haar risico's bij het gebruik maken van clouddiensten te beheersen?	In paragraaf 6.2 is het conceptueel (cloud)uitbestedingsmodel in de vorm van een tabel, figuur en checklist (zie Bijlage 4) opgenomen. De uitvoering van dit conceptueel model en de checklist zouden er aan bijdragen om de risico's bij het gebruik van clouddiensten te beheersen. Daarnaast kan het bijdragen aan het invulling geven aan de beheerste en integere bedrijfsvoering. *Een kanttekening van het conceptueel (cloud)uitbestedings-model is dat het theoretisch van aard is, omdat het in de praktijk zelden tot nooit voorkomt dat een financiële instelling een combinatie is van bank, verzekeraar én pensioenfonds.*

Tabel 7: Overzicht deelvragen en antwoorden op basis van het onderzoek

8 Resultaten validatie

Dit hoofdstuk beschrijft de validatie van het conceptueel (cloud)uitbestedingsmodel voor de beheersing van clouduitbesteding op basis van validatie door middel van een casestudy bij een pensioenfonds en een clouduitbestedingsovereenkomst, en interviews.

8.1 Resultaten casestudy – analyse vigerend pensioenfondsbeleid

De casestudy is uitgevoerd bij pensioenfonds A. Het pensioenfonds heeft het merendeel van haar bedrijfsprocessen, zoals pensioenuitvoering en vermogensbeheer uitbesteed. Hieronder begrepen ook cloud (onder)uitbesteding. In de casestudy is het conceptueel (cloud)uitbestedingsmodel getoetst aan het vigerende beleid van het pensioenfonds.

8.1.1 Vigerend beleid pensioenfonds A

In dit onderzoek zijn verschillende beleidsdocumenten van pensioenfonds A in relatie tot het conceptueel (cloud)uitbestedingsmodel onderzocht, namelijk:

- Integraal risicomanagement beleid (2020)
- Beleid Uitbesteding en Advisering (2020) & (2022)
- Informatiebeveiligingsbeleid (2021)
- IT-beleid (2021)
- Governance handboek (2019)
- Geschiktheidsbeleidskader (2022)
- Business Continuïteitsplan (2020)

Opgemerkt moet worden dat in de loop van de onderzoeksperiode een update is uitgevoerd van het Beleid Uitbesteding en Advisering (2022). Bij deze update is gebruik gemaakt van tussentijdse uitkomsten van een eerste toets van het conceptueel (cloud)uitbestedingsmodel en het Beleid Uitbesteding en Advisering (2020). Het nieuwe beleid is ook beoordeeld door twee externe partijen, namelijk een advocatenkantoor en accountantskantoor. In dit onderzoek is vervolgens een tweede toets uitgevoerd om resterende verbeterpunten voor het pensioenfonds te identificeren. Zie hiervoor de aanbevelingen in paragraaf 9.2.

8.1.2 Toetsingen vigerend beleid & conceptueel (cloud)uitbestedingsmodel

Voor het uitvoeren van de twee toetsingen zijn de checklist (zie Bijlage 4) en de Tabel 6, zoals opgenomen in paragraaf 6.2.1, van het conceptueel (cloud)uitbestedingsmodel gebruikt. Door middel van de Tabel 8 hieronder zijn de uitkomsten van de twee toetsingen weergegeven. De afwijkingen zijn genummerd en in sub-paragraaf 8.1.3 toegelicht.

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Toets 1	Toets 2
4.2	**Risicomanagement**		
4.2.2	Systematische risicoanalyse	✓	✓
4.2.3	Periodieke uitbestedingsrisicoanalyse voor kritieke op belangrijke functies	1	✓
4.4	**Uitbestedingsbeleid & -governance**		
5.2.1	Uitbestedingsbeleid	2	✓
5.2.2	Kritieke op belangrijke functies	3	✓
5.2.3	Deskundigheid	✓	✓
5.2.4	Schriftelijke kennisgeving aan toezichthouders	✓	✓
5.2.5	Bedrijfscontinuïteitsplannen	4	✓
5.2.6	Uitbestedingsregister	5	✓
5.3	**Selectie dienstverlener**		
5.3.1	Beoordeling kritieke of belangrijke functies *(zie 5.2.2, in deze tabel)*	Zie 3	✓
5.3.2	Risicobeoordeling vóór uitbesteding *(zie 4.2.3, in deze tabel)*	Zie 1	✓
5.3.3	Due diligence onderzoek	✓	✓
5.4	**Uitbestedingsovereenkomst**		
5.4.1	Uitbestedingsovereenkomst (algemeen)	6	✓
5.4.2	Beveiliging van gegevens en systemen	✓	✓
5.4.3	Toegangs-, informatie- en auditrechten	✓	✓
5.4.4	Onderuitbesteding	✓	✓
5.4.5	Beëindigingsrechten	✓	✓
5.5	**Monitoring dienstverlener**		
5.5.1	Monitoring- & controlemechanisme	✓	✓
5.5.2	Bewaken prestaties & informatiebeveiliging dienstverlener	✓	✓
5.5.3	Beoordelen assurance rapportages & opvolging bevindingen	✓	✓
5.5.4	Bijwerken risicobeoordeling *(zie 4.2.3, in deze tabel)*	Zie 1	✓
5.6	**Evaluatie dienstverlener**		
5.6.1	Evaluatie dienstverlener	✓	✓
5.6.2	Exitstrategie	7	✓
Toelichting symbolen: ✓ = sluit aan, ✓ = sluit gedeeltelijk aan.			

Tabel 8: Uitkomst toetsing conceptueel (cloud)uitbestedingsmodel met vigerend pensioenfondsbeleid.

8.1.3 Toelichting uitkomst toetsingen (samengevat i.v.m. vertrouwelijkheid)

Op basis van toets 1 zijn zeven afwijkingen van het conceptueel (cloud)uitbestedingsmodel geconstateerd. De nummers 1, 2, 3, 5 en 6 hebben betrekking op het beter verankeren van de onderwerpen in het Beleid Uitbesteding en Advisering. Dit is reeds gerealiseerd bij de update van dit beleid in november 2022. De nummers 4 en 7 hebben met elkaar te maken. Op onderdelen wordt invulling gegeven aan de criteria, maar een overkoepelend formeel Business Continuity Beleid is niet beschreven. Beide punten zijn ten dele opgenomen in het nieuwe Beleid Uitbesteding en Advisering (2022). Zie hiervoor de aanbevelingen in paragraaf 9.2.

8.2 Resultaten casestudy – cloudovereenkomst

De casestudy is uitgevoerd op een cloudovereenkomst van Microsoft. Hiervoor is gebruik gemaakt van een Microsoft Cloud Mapping For Financial institutions in Europe[11] uit december 2021 en een Microsoft Customer Agreement, Financial Services Amendment (Microsoft, november 2019). Onderzocht is of de vereisten voor de uitbestedingsovereenkomst die zijn beschreven in de het conceptueel (cloud)uitbestedingsmodel adequaat worden ingevuld door Microsoft en/of aandachtspunten voor financiële instellingen aanwezig zijn.

8.2.1 Toetsing cloudovereenkomst & conceptueel (cloud)uitbestedingsmodel

Voor het uitvoeren van de toetsing is één onderdeel uit het conceptueel (cloud)uitbestedings-model gebruikt, namelijk de uitbestedingsovereenkomst. Zie voor de detailtoetsing Bijlage 5. Deze Bijlage 5 is gebaseerd op één onderdeel van de checklist in Bijlage 4 (onderdeel 5.4). De uitkomsten van de toetsing zijn hieronder weergegeven in Tabel 9. De afwijking is genummerd en in sub-paragraaf 8.2.2 toegelicht.

5.4	Uitbestedingsovereenkomst	Toets
5.4.1	Uitbestedingsovereenkomst (algemeen)	1
5.4.2	Beveiliging van gegevens en systemen	✓
5.4.3	Toegangs-, informatie- en auditrechten	✓
5.4.4	Onderuitbesteding	✓
5.4.5	Beëindigingsrechten	✓

Tabel 9: Uitkomst toetsing conceptueel (cloud)uitbestedingsmodel met cloudovereenkomst.

8.2.2 Toelichting uitkomst toetsing & vervolganalyse

Voor één onderwerp uit het conceptueel (cloud)uitbestedingsmodel, onderdeel uitbestedings-overeenkomst, was het aan de hand van de Microsoft Cloud Mapping For Financial Institutions in Europe uit december 2021 niet mogelijk om een aansluiting te maken. Dit heeft betrekking op art. 31 lid 2 sub b, Bpr Wft (voor banken en verzekeraars) en art. 13 sub e, B Pw (voor pensioenfondsen). Tekstueel lijken deze artikelen op elkaar, behalve de woorden ‘financiële onderneming of bijkantoor’ en ‘fonds’.

[11] https://servicetrust.microsoft.com/DocumentPage/2f18eb43-64df-424c-8d59-98c18b7cb9e0

Hieronder is de letterlijke wettekst van art. 31 lid 2 sub b, Bpr Wft opgenomen.

> **Wettekst:**
> "2. In de overeenkomst wordt in ieder geval het volgende geregeld:
> b. de mogelijkheid voor de financiële onderneming of het bijkantoor om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt;"

Een aanleiding voor het aanbrengen van een wijziging in de wijze waarop de uitvoering van de werkzaamheden door de derde (= aanbieder van clouddiensten in de context van dit onderzoek) geschiedt zou een aanwijzing van toezichthouder DNB kunnen zijn (art. 1:75 Wft).

Bij het nader analyseren van een Microsoft Customer Agreement, Financial Services Amendment (Microsoft, november 2019) blijkt dat een gedeeltelijke oplossing aanwezig is. Dit heeft betrekking op paragraaf 5. Customer Compliance Program, lid c. Responding to Regulatory Changes. Hierin zijn o.a. de volgende twee paragrafen opgenomen:

- "If a Member, either acting on its own behalf or upon instruction from the Regulator, requires a change to an existing services feature or control or a new services feature or control, a Member may request such feature or control from Microsoft, and Microsoft will respond within a reasonable time, so that the parties can discuss if accommodating such request is feasible and, if so, how to accommodate that Member's requirements.
- In the event Microsoft and a Member cannot come to a mutually satisfactory resolution to address concerns about regulatory changes or changes to Online Service, that Member may elect to terminate the Online Services, with no penalty, by providing reasonable notice of termination."

Via de hiervoor opgenomen twee punten biedt Microsoft contractueel de mogelijkheid om te vragen om een wijziging. Indien Microsoft en de klant ('Member') niet tot een wederzijds bevredigende oplossing kunnen komen, kan de klant ervoor kiezen om de Online Services te beëindigen, zonder boete, door een redelijke kennisgeving van de beëindiging te verstrekken.

8.3 Resultaten interviews

Naast desk research is een field research uitgevoerd met behulp van interviews om de geraadpleegde wetenschappelijke literatuur en wet- en regelgeving in dit onderzoek aan te vullen met primaire informatie (McCartan & Robson, 2016) ter verbetering van het conceptueel (cloud)uitbestedingsmodel. Daarnaast waren vragen gericht over de uitvoerbaarheid van bepaalde tussentijdse uitkomsten zoals behandeld in paragraaf 8.1.2.

8.3.1 Achtergrond geïnterviewden

De vijf geïnterviewden waren allen man en hun leeftijd ligt tussen de 34 en 64 jaar. Hun opleidingsniveau varieert van HEAO, (executive) master(s), postdoctoraal tot gepromoveerd (en/of een combinatie hiervan). Drie van hen zijn werkzaam voor pensioenfonds A in een senior management positie, één is werkzaam bij een juridisch advies kantoor en één bij een big four accounts- en adviesorganisatie.

8.3.2 Belangrijkste uitkomsten van de interviews

In Bijlagen 7 en 8 zijn de vragen en antwoorden (beknopt) uit de interviews opgenomen. De vragenlijst bestaat uit algemene vragen over de geïnterviewden en specifieke vragen in lijn met de geformuleerde doelen in paragraaf 3.2.2. In de Tabel 10 hieronder is de (gedeeltelijke) realisatie van deze doelen beschreven voor de dataverzameling en toetsing van het conceptueel (cloud)uitbestedingsmodel.

#	Omschrijving doel	Toelichting realisatie doel
1	Verificatie van de verzameling van de belangrijkste uitbesteding- en cloudrisico's.	**Doel bereikt.** De geïnterviewden herkennen de risico's die zijn behandeld in het interview en hebben geen wezenlijk nieuwe of andere (cloud) risico's benoemd dan zijn geïdentificeerd in het onderzoek. Een bijkomstigheid van de interviews is dat naast risico's ook maatregelen zijn benoemd voor het beheersen van cloudrisico's. Deze zijn opgenomen in Bijlage 8.
2	Verificatie van de verzameling van de belangrijkste relevante eisen uit wet- en regelgeving en toezichthouder verwachtingen.	**Doel ten dele bereikt.** De geïnterviewden tezamen hebben een deel van de geraadpleegde wet- en regelgeving in dit onderzoek benoemd. Geen nieuwe wet- en regelgeving is benoemd. Het onderwerp in relatie tot wet- en regelgeving lag over het algemeen te ver van hen af.
3	Verificatie van de uitvoerbaarheid van het conceptueel (cloud)uitbestedingsmodel, het voldoen aan wet- en regelgeving en het omgaan met afwijkingen bij uitbesteding aan cloud aanbieders.	**Doel bereikt.** De geïnterviewden benadrukten regelmatig het belang van risk based, of uitgedrukt in de termen van 'kritiek of belangrijk'. Dit vanwege de uitvoerbaarheid, kosten en efficiënte inzet van personeel, en het voldoen aan wet- en regelgeving. Meerdere malen is benadrukt dat cloud een vorm van uitbesteding is. Dit sluit aan op het conceptueel (cloud)uitbestedingsmodel dat risk-based is ingericht en dat cloud een vorm van uitbesteding is.

Tabel 10: Overzicht realisatie dataverzameling doelen door middel van interviews

8.4 Conclusie en implicaties voor het onderzoek

Het conceptueel (cloud)uitbestedingsmodel is in hoge mate gebaseerd op basis van wet- en regelgeving en verwachtingen van toezichthouders. Hiervoor geldt in principe dat daaraan invulling moet worden gegeven. Dit is daarom als een gegeven meegenomen in het ontwerp en de validatie van het conceptueel (cloud)uitbestedingsmodel.

Op basis van de toetsingen en interviews zoals beschreven in de paragrafen 8.1 t/m 8.3 kan het volgende worden geconcludeerd:

- Het conceptueel (cloud)uitbestedingsmodel hoeft niet te worden gewijzigd naar aanleiding van de casestudy met betrekking tot het vigerende beleid van pensioenfonds A;
    - Het model is tweemaal getoetst bij het pensioenfonds en heeft reeds bijgedragen aan de verbetering van het Beleid Uitbesteding en Advisering versie 2022. Dit beleid is ook getoetst door een advocatenkantoor en accountantskantoor.
- Het conceptueel (cloud)uitbestedingsmodel hoeft niet te worden gewijzigd naar aanleiding van de casestudy met betrekking tot de Microsoft clouduitbestedingsovereenkomst;
    - Een aandachtspunt vormt de mogelijkheid om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door Microsoft geschiedt. Dit risico moet zorgvuldig worden afgewogen bij de risicoanalyse.
- Het conceptueel (cloud)uitbestedingsmodel is niet gewijzigd naar aanleiding van de interviews.
    - In Bijlage 8 is een extra “Template RSA Cloudcomputing” opgenomen. Dit template biedt een financiële instelling mogelijk extra handvatten t.o.v. het standaard “Template RSA Uitbesteding” van DNB (zie paragraaf 4.2.4, Tabel 3). *NB. In dit template (zie Bijlage 8) zijn specifieke technische IT- en informatie-beveiliging risico’s buiten beschouwing gelaten vanwege de aard van dit onderzoek.*

Conclusie: Het conceptueel (cloud)uitbestedingsmodel wijzigt niet naar aanleiding van de validatie. Daarnaast is aangetoond dat het model toepasbaar is bij pensioenfonds A.

9 Conclusie, aanbevelingen en reflectie

In dit hoofdstuk is de conclusie opgenomen waarin een antwoord wordt gegeven op de hoofdvraag. Gevolgd door aanbevelingen en onderwerpen voor vervolgstudies. Het hoofdstuk sluit af met een reflectie op het leerproces en uitvoering van de masterthesis.

9.1 Conclusie onderzoek

De hoofdvraag van dit onderzoek luidt:

> ***Hoe kunnen financiële instellingen blijven voldoen aan de wettelijke vereisten en verwachtingen van toezichthouders bij uitbesteding van hun ICT aan grote buitenlandse aanbieders van clouddiensten?***

Het onderzoek naar wetenschappelijke literatuur en wet- en regelgeving heeft geleid tot een zevental belangrijke aanknopingspunten.

1. In de wetenschappelijke literatuur zijn cloudlevenscyclus modellen beschreven en onderzocht, maar deze zijn niet specifiek gericht op de Nederlandse financiële sector.
2. Voor Nederlandse financiële instellingen geldt dat zij hun bedrijfsvoering beheerst en integer moeten inrichten.
3. Het bestuur van een financiële instelling is te allen tijde eindverantwoordelijk voor de bedrijfsvoering van de instelling. Ook als werkzaamheden zijn uitbesteed of onderuitbesteed.
4. De term ‘cloud’ of ‘cloudcomputing’ komt niet voor in Nederlandse wet- en regelgeving voor financiële instellingen.
5. Het gebruik van clouddiensten of cloudcomputing is een vorm van uitbesteding. In Nederlandse en Europese wet- en regelgeving zijn eisen voor uitbesteding opgenomen en in bepaalde situaties ook expliciet voor uitbesteding aan aanbieders van clouddiensten.
6. De vereisten voor uitbesteding aan aanbieders van clouddiensten voor banken en verzekeraars zijn explicieter beschreven dan pensioenfondsen.
7. Verwachtingen van toezichthouder DNB over de naleving van wet- en regelgeving zijn opgenomen in ‘good practices’ specifiek voor verzekeraars en pensioenfondsen.

Op basis van wetenschappelijke literatuur, Nederlandse en Europese wet- en regelgeving en verwachtingen van toezichthouders is een conceptueel (cloud)uitbestedingsmodel voor banken, verzekeraars en pensioenfondsen ontwikkeld. Dit model bestaat uit een figuur en checklist. Het conceptueel (cloud)uitbestedingsmodel is gevalideerd op basis van casestudy met vigerend beleid van een financiële instelling en een cloudovereenkomst, en interviews. De validatie heeft niet geleid tot het aanpassen van het conceptueel (cloud)uitbestedingsmodel.

Het antwoord op de hoofdvraag kan hiermee worden gegeven. Een Nederlandse financiële instelling kan voldoen aan wettelijke vereisten en verwachtingen van toezichthouders bij uitbesteding van ICT aan grote aanbieders van clouddiensten door het (aantoonbaar) voldoen aan wet- en regelgeving voor beheerste & integere bedrijfsvoering en uitbesteding. Hieronder begrepen:

- Integraal risicomanagementbeleid, risicobeheerfunctie, risicobeheersingsproces en systematische risicoanalyse;
- (Cloud)uitbestedingsbeleid (incl. governance) met daarin specifieke voorwaarden en het uitbestedingsproces. In dit proces zijn opgenomen: de (her)selectie van een dienstverlener, uitbestedingsovereenkomst, monitoring en evaluatie van de dienstverlener.

De Nederlandse financiële instellingen kunnen hierbij mogelijk mede gebruik maken van het in dit onderzoek ontwikkelde conceptueel (cloud)uitbestedingsmodel (incl. checklist). Een kanttekening van het conceptueel (cloud)uitbestedingsmodel is dat het in de praktijk zelden tot nooit zal voorkomen dat een Nederlandse financiële instelling een combinatie is van bank, verzekeraar én pensioenfonds. Het model is daarom conceptueel van aard. Het conceptueel model kan daarentegen wel praktische handvatten bieden voor Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse aanbieders. Het kan tevens bijdragen aan het invulling geven aan de beheerste en integere bedrijfsvoering.

9.2 Aanbevelingen pensioenfonds A

Het aantal aanbevelingen als gevolg van dit onderzoek voor pensioenfonds A is beperkt, omdat bij een update van het Beleid Uitbesteding en Advisering in november 2022 reeds gebruik is gemaakt van tussentijdse uitkomsten van dit onderzoek. Deze uitkomsten hadden betrekking op het beter verankeren van bepaalde onderwerpen in het Beleid Uitbesteding en Advisering. Dit had betrekking op:

1. Veranker de terminologie 'kritiek of belangrijke functies' beter in het Beleid Uitbesteding en Advisering.
2. Neem de voorwaarden voor de inrichting en uitvoering van een uitbestedingsregister expliciet op in het Beleid Uitbesteding en Advisering.
3. Neem een template RSA Uitbesteding op in het Beleid Uitbesteding en Advisering.
4. Neem de 'exitstrategie' en 'kritieke of belangrijke functies' expliciet op in het uitbestedingsproces in het Beleid Uitbesteding en Advisering.
5. Neem de locatie van de opslag en verwerking van (persoons)gegevens expliciet op in het Beleid Uitbesteding en Advisering (en template uitbestedingsovereenkomst (in het Beleid Uitbesteding en Advisering)).

De voornoemde vijf punten zijn opgenomen in het Beleid Uitbesteding en Advisering versie 2022. Dit beleidsdocument is in november 2022 vastgesteld door het bestuur van pensioenfonds A.

Een aanbeveling resteert naar aanleiding van dit onderzoek.

1. Het verdient de aanbeveling om een formeel overkoepelend Business Continuity Management beleid te ontwikkelen om verbeterd invulling te geven aan Art. 21, lid 5 (IORP II): *"het treffen van redelijke maatregelen, waaronder de ontwikkeling van noodplannen, om voor continuïteit en regelmatigheid in de verrichting van hun werkzaamheden te zorgen. Daartoe maakt het pensioenfonds gebruik van passende en proportionele systemen, middelen en procedures"*. Ondanks dat uit het fieldresearch blijkt dat het risico beperkt wordt ingeschat, wordt het belang van dit beleid unaniem onderschreven.

9.3 Beperkingen van het onderzoek

Het onderzoek kent een aantal belangrijke beperkingen, namelijk:

- De auteur is géén jurist, maar heeft ruim negentien jaar werkervaring waarvan vier jaar in de accountancy, zes jaar in compliance & business proces outsourcing (voor de bancaire sector) en de laatste ruim negen jaar in het vakgebied operationeel riskmanagement (incl. operationeel-, uitbesteding-, IT- en juridische risico's) in de pensioensector.
- De geraadpleegde wet- en regelgeving was primair gericht op 'cloudcomputing', 'uitbesteding' en 'beheerste bedrijfsvoering'. Aanpalende wet- en regelgeving is slechts ten dele geraadpleegd. Het onderzoek streeft nadrukkelijk geen absolute compliance met wet- en regelgeving na, maar het biedt mogelijk handvatten voor verschillende Nederlandse financiële instellingen bij het gebruik van clouddiensten van grote buitenlandse cloud aanbieders.
- In Nederland zijn veel verschillende financiële instellingen. In het onderzoek zijn deze financiële instellingen beperkt tot alleen banken, verzekeraars en pensioenfondsen. In wet- en regelgeving worden deze financiële instellingen op verschillende wijze aangeduid. Bijvoorbeeld: financiële instelling, financiële onderneming, opdrachtgever, bank, verzekeraar en pensioenfonds.
- In de analyse van wet- en regelgeving is geen rekening gehouden met (uitbesteding binnen) groepsmaatschappijen.

9.4 Afbakening (cloud)uitbestedingsmodel

Het conceptueel (cloud)uitbestedingsmodel is primair gericht op de beheersing van (cloud) uitbestedingsrisico's. Dit houdt in dat niet alle onderzochte wet- en regelgeving expliciet in het model is opgenomen. Bovendien zijn technische IT- en informatiebeveiligingsrisico's in dit onderzoek buiten beschouwing gelaten.

9.5 Suggesties voor vervolgonderzoek

Dit onderzoek is specifiek gericht op de beheersing van uitbestedingsrisico's voor uitbesteding naar cloudaanbieders. Gedurende het onderzoek zijn verschillende onderwerpen voor vervolgonderzoek geïdentificeerd, namelijk:

- De IT- en informatiebeveiligingsrisico's van cloudcomputing in relatie tot een uitbreiding van het DNB template RSA Uitbesteding.
- De organisatorische inrichting van financiële instellingen met betrekking tot verschillende functies, zoals: interne controle, risicomanagement, interne audit, business continuity, IT en IT-security op basis van Nederlandse en Europese wet- en regelgeving.
- De werking van datawetgeving met extraterritoriale werking, waarbij niet alleen de 'bekende' AVG en CLOUD-act worden onderzocht, maar ook bijvoorbeeld datawetgeving uit China (Data Security Law).
- De wijze waarop een Business Continuity Beleid in de keten van (cloud)uitbesteding kan worden ontworpen (en geïmplementeerd) bij een financiële instelling.

9.6 Reflectie

De reflectie maakt geen onderdeel uit van de gepubliceerde versie van deze masterthesis.

Bijlage 1 – Bronvermelding

Autoriteit Persoonsgegevens. (2018). *Boetes en andere sancties.* Geraadpleegd op 14 augustus 2022, van *https://autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties*

Autoriteit Persoonsgegevens. (2022). *Taken en bevoegdheden.* Geraadpleegd op 14 augustus 2022, van https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/taken-en-bevoegdheden

Brudenall, P. (2005). *The Outsourcing Contract: Structure and Tactics.* In: Brudenall, P. (eds) Technology and Offshore Outsourcing Strategies. Palgrave Macmillan, London. Geraadpleegd van https://doi.org/10.1057/9780230518568_12

Conway, G. & Curry, E. (2012). *MANAGING CLOUD COMPUTING - A Life Cycle Approach.* Proceedings of the 2nd International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0003928401980207

Daniëls, K. & Kits, P. (2015). *Contracteren in de cloud – ken uw risico's.* Contracteren, 17(1), 2–16. Geraadpleegd op 16 augustus 2022, van https://doi.org/10.5553/contr/156608932015017001002

De Nederlandsche Bank. (2011). *Wat is integraal risicomanagement (IRM) en waar kijkt DNB hierbij naar?* Geraadpleegd op 25 september 2022, van https://www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/pensioenfondsen/prudentieel-toezicht/beleggingen/wat-is-integraal-risicomanagement-irm-en-waar-kijkt-dnb-hierbij-naar/

De Nederlandsche Bank. (2019). *Q&A Melding uitbesteding van werkzaamheden bij De Nederlandsche Bank door pensioenfondsen en premiepensioeninstellingen.* Geraadpleegd op 25 september 2022, van https://www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/pensioenfondsen/prudentieel-toezicht/uitbesteding-pensioenfondsen/q-a-melding-uitbesteding-van-werkzaamheden-bij-de-nederlandsche-bank-door-pensioenfondsen-en-premiepensioeninstellingen/

De Nederlandsche Bank. (2020). *Governance: Uitbesteding.* Geraadpleegd op 25 september 2022, van2022, van https://www.dnb.nl/voor-de-sector/open-boek-toezicht-fasen/lopend-toezicht/prudentieel-toezicht/governance/governance-uitbesteding/

De Nederlandsche Bank. (2022) *Toezicht op financiële instellingen.* Geraadpleegd op 15 augustus 2022, van https://www.dnb.nl/betrouwbare-financiele-sector/toezicht-op-financiele-instellingen/

ENISA. (2009). Geraadpleegd op 15 augustus 2022, van https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

Ferreira Pires. (2011), Wat is Cloud computing? Geraadpleegd op 24 juli 2022, van https://ris.utwente.nl/ws/portalfiles/portal/6868995/Computerrecht-2011-lfp.pdf

Franceschini, F. et al,. (2003). Outsourcing: guidelines for a structured approach | Emerald Insight. Geraadpleegd op 21 september 2019, van https://www.emerald.com/insight/content/doi/10.1108/14635770310477771/full/html

Gartner. (2022). *Gartner Forecasts Worldwide Public Cloud End-User Spending to reach Nearly $500 Billion in 2022.* Geraadpleegd op 27 augustus 2022, van https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022#:%7E:text=Worldwide%20end%2Duser%20spending%20on,to%20reach%20nearly%20%24600%20billion.

Gubbels, B.G.N. (2014). *Burgerlijk Wetboek | Wet & Recht*. Geraadpleegd op 16 augustus 2022, van https://www.wetrecht.nl/burgerlijk-wetboek/

Hennepe, A. T. G. (1954). *Uitbesteding van werk en toelevering.* SpringerLink. Geraadpleegd op 27 augustus 2022, https://link.springer.com/article/10.1007/BF02206035?error=cookies_not_supported&code=933d676e-caa5-47b1-ab93-28160824c2f4

LaFlamme (2020). *The Big -aaS List of As-a-Service Offerings*. Geraadpleegd op 1 augustus 2022, van https://www.auvik.com/franklyit/blog/aas-as-a-service-list/

Linthicum, D. S. (2009). Cloud Computing and SOA Convergence in Your Enterprise (1ste editie). Addison-Wesley Professional.

McCartan, K., & Robson, C. (2016). Real World Research (4de editie). Wiley.

Mell, P. & Grance, T. (2011), *The NIST Definition of Cloud Computing*, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, Geraadpleegd op 14 augustus 2022, https://doi.org/10.6028/NIST.SP.800-145

Microsoft. (2022). *Wat is SaaS?* Geraadpleegd op 1 augustus 2022, van https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-saas/

Ministerie van Veiligheid en Justitie. (2012, januari). *Whitepaper NCSC Cloudcomputing & Security.* Nationaal Cyber Security Centrum. Den Haag.

Nationaal Cyber Security Centrum. (2022, 18 augustus). *Cloud Act Memo.* Publicatie Nationaal Cyber Security Centrum. Geraadpleegd op 27 augustus 2022, van https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo

Oracle. (z.d.). *What is cloud computing?* Geraadpleegd op 27 augustus 2022, van https://www.oracle.com/nl/cloud/what-is-cloud-computing/#cloud-computing-defined

Rijksoverheid. (2022). *Financiële sector.* Geraadpleegd op 1 augustus 2022, van https://www.rijksoverheid.nl/onderwerpen/financiele-sector

Rijksoverheid (2022). *Stabiele financiële sector*. Financiële sector | Rijksoverheid.nl. Geraadpleegd op 15 augustus 2022, van https://www.rijksoverheid.nl/onderwerpen/financiele-sector/gezonde-financiele-sector

Schneider, S. & Sunyaev, A. (2015). CloudLive: a life cycle framework for cloud services. Electronic Markets, 25(4), 299–311. https://doi.org/10.1007/s12525-015-0205-y

Scott, et al. (2019). *Cloud computing in the Financial Sector: A Global Perspective.* Social Science Research Network. Geraadpleegd op 17 november 2022, van https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427220

Sprenkels & Verschuren. (2022). *Beheerste en integere bedrijfsvoering.* Geraadpleegd op 4 september 2022, van https://www.sprenkelsenverschuren.nl/beheerste-en-integere-bedrijfsvoering/

Synergy Research Group. (2022). *Huge Cloud Market Still Growing at 34% Per Year.* Geraadpleegd op 1 augustus 2022, van https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

Tapestry Networks. (2021). Hoe *technologie leidt tot concurrentievoordeel in de financiële dienstverlening*. EY - Nederland. Geraadpleegd op 27 augustus 2022, van https://www.ey.com/nl_nl/financial-services/how-technology-is-driving-competitive-advantage-in-fs

Talen, R. (2019). De verwerkersovereenkomst: wanneer wel, wanneer niet en wat zet je erin? ictrecht.nl. Geraadpleegd op 16 augustus 2022, van https://www.ictrecht.nl/blog/de-verwerkersovereenkomst-wanneer-wel-wanneer-niet-en-wat-zet-je-erin

Universiteit Twente. (2019). *Beschrijving masterthesis voor master risicomanagement.*

Wikipedia. (2017). *IT-outsourcing.* Geraadpleegd op 21 september 2021, van https://nl.wikipedia.org/wiki/IT-outsourcing

Wikipedia. (2018). *Cloudcomputing*. Geraadpleegd op 27 augustus 2022, van https://nl.wikipedia.org/wiki/Cloudcomputing

Wikipedia. (2022). *CLOUD Act.* Geraadpleegd op 21 september 2021, van https://nl.wikipedia.org/wiki/CLOUD_Act

Toezichthouder documenten:

Good practice uitbesteding verzekeraars. (2019). https://www.dnb.nl. Geraadpleegd op 14 augustus 2022, van https://www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/verzekeraars/prudentieel-toezicht/governance/good-practice-uitbesteding-verzekeraars/

Guidance uitbesteding pensioenfondsen. (2014). https://www.dnb.nl. Geraadpleegd op 14 augustus 2022, van https://www.dnb.nl/media/un1fz452/guidance-uitbesteding-pensioenfondsen.pdf

Guidelines on outsourcing arrangements. (2019). European Banking Authority. Geraadpleegd op 14 augustus 2022, van https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

Guidelines on outsourcing to cloud service providers - Eiopa European Commission. (2020). Eiopa - European Commission. Geraadpleegd op 14 augustus 2022, van https://www.eiopa.europa.eu/document-library/guidelines/guidelines-outsourcing-cloud-service-providers_en?source=search

Guidelines on system of governance. (2015). Geraadpleegd op 14 augustus 2022, van https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa_guidelines_on_system_of_governance_nl.pdf

Toelichting bij meldingsformulier uitbestedingen. (z.d.). De Nederlandsche Bank. Geraadpleegd op 14 augustus 2022, van https://www.dnb.nl/media/djcpgosh/toelichting-uitbesteding.pdf

Wet- en regelgeving:

Besluit financieel toetsingskader, geraadpleegd op 7 augustus 2022 van https://wetten.overheid.nl/BWBR0020871/2022-07-01/0#Paragraaf1

Besluit prudentiële regels Wft, geraadpleegd op 7 augustus 2022 van https://wetten.overheid.nl/BWBR0020420/2020-01-01

Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling, geraadpleegd op 7 augustus 2022 van https://wetten.overheid.nl/BWBR0020892/2020-01-01

Gedelegeerde Verordening Solvency II (2015/35EU), geraadpleegd op 7 augustus 2022 van http://publications.europa.eu/resource/cellar/e0c803af-9e0f-11e4-872e-01aa75ed71a1.0016.03/DOC_477

Pensioenwet, geraadpleegd op 7 augustus 2022 van https://wetten.overheid.nl/BWBR0020809/2022-07-07

Richtlijn Institutions for Occupational Retirement Provision (2016/2341), geraadpleegd op 29 september van https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016L2341&from=EN

Richtlijn solvabiliteit II, geraadpleegd op 7 augustus 2022 van https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/?uri=CELEX%3A02009L0138-20140523

Staatscourant van het Koninkrijk der Nederlanden. (2018) Code Pensioenfondsen geraadpleegd op 29 september 2022 van https://zoek.officielebekendmakingen.nl/stcrt-2018-55140.html

Wet op het financieel toezicht, geraadpleegd op 7 augustus 2022 van https://wetten.overheid.nl/BWBR0020368/2022-07-08

Bijlage 2a – Detailanalyse wet- en regelgeving (totaal)

In deze is een detailanalyse opgenomen van wet- en regelgeving met betrekking tot uitbesteding van werkzaamheden en/of het gebruik maken van clouddiensten door Nederlandse banken, verzekeraars en pensioenfondsen.

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
			Bank / Verzekeraar	Bank / Verzekeraar	Pensioenfonds	Pensioenfonds	Pensioenfonds	Verzekeraar	Verzekeraar	Pensioenfonds	Pensioenfonds	Bank	Verzekeraar	Verzekeraar	Verzekeraar	Pensioenfonds	Sectorbreed
Par.	Titel (/sub-titel)	Zoekwoorden	Wet op het financieel toezicht	Besluit prudentiële regels Wft	Pensioenwet	Besluit uitvoering Pensioenwet (en Wet verplichte beroepspensioenregeling)	Besluit financieel toetsingskader pensioenfondsen	Richtlijn Solvency II (2009/138/EG)	Gedelegeerde Verordening Solvency II (2015/35EU)	Richtlijn Institutions for Occupational Retirement Provision (2016/2341)	Code pensioenfondsen (2018)	EBA: Richtsnoeren inzake uitbesteding (2019)	EIOPA: Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten (2020)	EIOPA: Richtsnoeren voor het governance systeem (2014)	DNB: Good practice uitbesteding verzekeraars (2019)	Guidance uitbesteding door pensioenfondsen (DNB, 2014)	Toelichting bij meldings-formulier uitbestedingen (DNB, 2020)
4.2.2	Risicomanagement: - (onafhankelijke) risicobeheerfunctie - systematische risicoanalyse	Risicobeheerfunctie, systematisch(e), risicoanalyse	Art. 3:17 Beheerste en integere bedrijfsvoering (lid 2a)	Art. 23 Risicomanagement (lid 6 en 7)	Art. 143 lid 2a en 143a lid 1	Art. 14 Beheersing van de risico's (lid 1)	Art. 18 Beheerste bedrijfsvoering (lid 5)	Art. 44 Risk management	Art. 259 Risicomanagement-systeem Art. 269 Risicomanagement-functie	Art. 25 Risicobeheer	Thema 1, art. 8	Richtsnoer 5: Solide governanceregelingen en risico's die samenhangen met derden	Richtsnoer 2: Algemene beginselen van governance inzake uitbesteding van clouddiensten	Inleiding (art. 1.8)	H1: Uitbestedingsbeleid	H1: Uitbestedingsbeleid	-
4.2.3	Risicomanagement: - periodieke risicoanalyse voor uitbesteding van kritieke of belangrijke functies	Vóór, voor, vooraf gaand, risicoanalyse	-	-	-	Art. 14 Beheersing van de risico's	-	-	-	Art. 25 Risicobeheer	-	Richtsnoer 5: Solide governanceregelingen en risico's die samenhangen met derden Richtsnoer 12.2: Beoordeling van risico's van uitbestedingsregelingen	Richtsnoer 8: Beoordeling van risico's van uitbesteding van clouddiensten	-	H3: Selectieproces	H2: Keuze van de pensioenuitvoerder	6. Risicoanalyse
5.1.3	Cloudcomputing: een vorm van uitbesteding	Cloud, cloudcomputing, clouddiensten	-	-	-	-	-	-	-	-	-	Art. 12 Definities	Art. 12 Definities	-	-	-	4. Algemene gegevens uitbesteding
5.1.4	Definitie uitbesteding	Uitbesteding, uitbesteden	Art. 1:1 Definties	-	-	Art. 1 Definties	-	Art. 13 Definities	-	-	-	Art. 12 Definities	Art. 9 Definities	-	Inleiding	Voorwoord (indirect)	1. Algemeen
5.1.8	Beheerste en integere bedrijfsvoering	Beheerste, bedrijfsvoering	Art. 3:17 Beheerste en integere bedrijfsvoering	Hoofdstuk 4. Beheerste uitbelening van het bedrijf	Art. 143 Beheerste en integere bedrijfsvoering	-	Art. 18 Beheerste bedrijfsvoering	Art. 41: Algemene governance vereisten	Art. 258 Algemene governance vereisten	Art 21 lid 5, Algemene governance voorschriften	Thema 7, art. 46	Richtsnoer 6: Solide governanceregelingen en uitbesteding (art. 40, sub b)	-	Hele document	Inleiding	Inleiding	-
5.1.9	Uitbesteding van werkzaamheden	Uitbesteding, uitbesteden	Art. 3:18 Uitbesteding	Hoofdstuk 5. Uitbesteden van werkzaamheden	Art. 34 Uitbesteding	Hoofdstuk 4. Uitbesteding	-	Art. 49: Uitbesteding	Art. 274: Uitbesteding	Art. 31 Uitbesteding	Thema 2	Hele document Richtsnoer 3: Uitbesteding	Hele document Richtsnoer 1: Clouddiensten en uitbesteding	Afdeling 11: Uitbesteding	Hele document	Hele document	Hele document
5.2.1	Uitbestedingsbeleid & -governance - Uitbestedingsbeleid & -procedures	Uitbestedingsbeleid, beleid, beleidslijn	-	Art. 29 Uitbestedingsbeleid	-	Art. 14 Beheersing van de risico's (lid 2 en 3)	-	Art. 41: Algemene governance vereisten Art. 49: Uitbesteding	Art. 274: Uitbesteding	Art. 31 Uitbesteding	Thema 1, art. 3 Thema 2, toelichting & art. 10	Richtsnoer 6: Solide governanceregelingen en uitbesteding Richtsnoer 7: Uitbestedingsbeleid	Richtsnoer 2: Algemene beginselen van governance inzake uitbesteding van clouddiensten Richtsnoer 3: Actualisering van de schriftelijke beleidslijn inzake uitbesteding	Richtsnoer 63: Schriftelijke beleidslijn inzake uitbesteding	H1: Uitbestedingsbeleid	H1: Uitbestedingsbeleid	-
5.2.2	Uitbestedingsbeleid & -governance - Kritieke of belangrijke uitbesteding	Kritiek, belangrijk, uitbesteding, functies, activiteiten	-	-	-	-	-	-	Art. 274: Uitbesteding	-	-	Richtsnoer 4: Kritieke of belangrijke functies	Richtsnoer 7: Beoordeling van kritieke of belangrijke operationele functies en activiteiten	Richtsnoer 60: Kritieke of belangrijke operationele functies of activiteiten	H1: Uitbestedingsbeleid	-	1. Algemeen
5.2.3	Uitbestedingsbeleid & -governance - Deskundigheid	Deskundigheid, countervailing power, geschiktheid	Art. 3:8 Geschiktheid	Art. 21 lid 3 Art. 30	Art. 106 Geschiktheid en betrouwbaarheid	Art. 14: Beheersing van risico's (w.o. lid 5, m.b.t. deskundigheid)	-	-	Art. 273 Deskundigheids- en betrouwbaarheidsvereisten	Art. 22 Vereisten voor een deskundig en betrouwbaar bestuur	-	-	-	Richtsnoer 11: Deskundigheidsvereisten	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	-
5.2.4	Uitbestedingsbeleid & -governance - Schriftelijke kennisgeving aan toezichthouders	Kennis, kennisgeving, toezichthouder, toezichthoudende, autoriteit	-	Art. 27a	-	Art. 14.0a. Kennisgeving uitbesteding	-	Art. 49: Uitbesteding	Verwijzing naar art. 49 Solvency II	Art. 31 Uitbesteding Art. 50 Aan de bevoegde autoriteiten te verstrekken informatie	-	Richtsnoer 11: Documentatievereisten (art. 59)	Richtsnoer 4: Schriftelijke kennisgeving aan toezichthouders	Richtsnoer 64: Schriftelijke kennisgeving aan de toezichthoudende autoriteit	H2: Governance uitbesteding en uitbestedingsovereenkomst	-	1. Algemeen
5.2.5	Uitbestedingsbeleid & -governance - Bedrijfscontinuïteitsplannen	Bedrijfscontinuïteit, continuïteit, noodplan, nood, BCP	-	Art. 26d	-	-	-	-	Art. 274: Uitbesteding	Art 21 lid 5, Algemene governance voorschriften	-	Richtsnoer 9: Bedrijfscontinuïteitsplannen	Richtsnoer 10: Contractuele bepalingen	Richtsnoer 63: Schriftelijke beleidslijn inzake uitbesteding	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	6. Risicoanalyse
5.2.6	Uitbestedingsbeleid & -governance - Uitbestedingsregister	Register, uitbestedingsregister, documentatievereisten	-	-	-	-	-	-	-	-	Thema 2, art. 12	Richtsnoer 11: Documentatievereisten	Richtsnoer 5: documentatievereisten	-	H4: Monitoring van de uitbestedingsrelatie	-	-
5.3.1	Selectie dienstverlener - Beoordeling kritieke of belangrijke functies (zie ook 5.5.2)	Kritiek, belangrijk, uitbesteding, functies, activiteiten	-	-	-	Art. 14 Beheersing van de risico's	-	-	Art. 274: Uitbesteding	-	-	Richtsnoer 12: Analyse vóór uitbesteding	Richtsnoer 6: Analyse voorafgaand aan uitbesteding	-	H3: Selectieproces	H2: Keuze van de pensioenuitvoerder	-
5.3.2	Selectie dienstverlener - Risicobeoordeling vóór uitbesteding (zie ook 4.2.3)	Vóór, voor, vooraf gaand, risicoanalyse	-	-	-	Art. 14 Beheersing van de risico's	-	-	-	Art. 25 Risicobeheer	-	Richtsnoer 5: Solide governanceregelingen en risico's die samenhangen met derden Richtsnoer 12.2: Beoordeling van risico's van uitbestedingsregelingen	Richtsnoer 8: Beoordeling van risico's van uitbesteding van clouddiensten	-	H3: Selectieproces	H2: Keuze van de pensioenuitvoerder	6. Risicoanalyse
5.3.3	Selectie dienstverlener - Due diligence onderzoek	Due diligence, selectie, selectieproces, onderzoek	-	-	-	Art. 14 Beheersing van de risico's	-	-	Art. 274: Uitbesteding	Art. 31 Uitbesteding	-	Richtsnoer 12.3: Due diligence	Richtsnoer 9: Due diligence-onderzoek t.a.v. aanbieder van clouddiensten	-	H3: Selectieproces	H2: Keuze van de pensioenuitvoerder	-
5.4.1	Uitbestedingsovereenkomst - Uitbestedingsovereenkomst (algemeen)	Uitbestedingsovereenkomst, uitbestedingsregeling, contract	-	Art. 31	-	Art. 13 Overeenkomst tot uitbesteding	-	-	Art. 274: Uitbesteding	Art. 31 Uitbesteding	Thema 2, art. 11 & 13	Richtsnoer 13: Contractfase	Richtsnoer 10: Contractuele bepalingen	-	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	5. Contract
5.4.2	Uitbestedingsovereenkomst - Beveiliging van gegevens en systemen	Beveiliging, bescherming	-	Art. 20	-	-	-	-	Art. 274: Uitbesteding Verwijzing naar AVG	-	-	Richtsnoer 13.2: Beveiliging van gegevens en systemen	Richtsnoer 12: Beveiliging van gegevens en systemen	-	H2: Governance uitbesteding en uitbestedingsovereenkomst	-	4. Algemene gegevens uitbesteding
5.4.3	Uitbestedingsovereenkomst - Toegangs-, informatie- en auditrechten	Toegang(srecht), audit(recht), right to audit, richt to examine, onderzoeksrecht	-	Art. 31	-	Art. 13 Overeenkomst tot uitbesteding	-	-	Art. 274: Uitbesteding	Art. 31 Uitbesteding	-	Richtsnoer 13.3: Toegangs-, informatie- en auditrechten	Richtsnoer 11: Toegangs- en auditrecht	-	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	5. Contract
5.4.4	Uitbestedingsovereenkomst - Onderuitbesteding	Onderuitbesteding, derden, aannemer, onderaannemer	-	-	-	-	-	-	Art. 274: Uitbesteding	Art. 50 Aan de bevoegde autoriteiten te verstrekken informatie (deels)	Thema 2, toelichting & art. 10	Richtsnoer 13.1: Onderuitbesteding van kritieke of belangrijke functies	Richtsnoer 13: Onderuitbesteding van kritieke of belangrijke operationele functies en activiteiten.	-	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	5. Contract
5.4.5	Uitbestedingsovereenkomst - Beëindigingsrechten	Beëindiging, exit, exitstrategieën	-	Art. 31	-	Art. 13 Overeenkomst tot uitbesteding	-	-	Art. 274: Uitbesteding	-	-	Richtsnoer 13.4: Beëindigingsrechten	Richtsnoer 15: Beëindigingsrecht en exitstrategieën	-	H2: Governance uitbesteding en uitbestedingsovereenkomst	H3: Governance van de uitbestedingsrelatie	5. Contract
5.5.1 5.5.2 5.5.3 5.5.4	Monitoring dienstverlener - Monitoring- & controle mechanisme - Bewaken prestaties & IB dienstverlener - Beoordelen assurance rapportages - Bijwerken risicobeoordeling (4.2.3 & 5.3.2)	Monitoring, prestaties, regelmatig, werkzaamheden, beoordelen	-	Art. 30	-	Art. 14 Beheersing van de risico's	-	-	Art. 274: Uitbesteding	-	-	Richtsnoer 14: Toezicht op uitbestede functies	Richtsnoer 14: Monitoring van en controle op uitbestedingsovereenkomsten betreffende clouddiensten	-	H4: Monitoring	H4: Monitoring van de uitbestedingsrelatie	-
5.6.1 5.6.2	Evaluatie dienstverlener - Evaluatie dienstverlener - Exitstrategie	Evaluatie, evaluatieproces, exitstrategieën, beëindigingsrecht	-	Art. 30	-	Art. 14 Beheersing van de risico's	-	Art. 41: Algemene governance vereisten	Art. 258: Algemene governance vereisten	-	Thema 1, art. 1 toelichting	Richtsnoer 15: Exitstrategieën	Richtsnoer 15: Beëindigingsrecht en exitstrategieën	-	H5: Evaluatieproces	H5: Evaluatie van de uitbestedingsrelatie	-

Bijlage 2b – Detailanalyse wet- en regelgeving (uitgesplitst)

In bijlage 2b is de detailanalyse van bijlage 2a uitgesplitst naar Nederlandse banken, verzekeraars en pensioenfondsen.

Verwijzing naar paragraaf en onderwerpen		De nummers corresponderen met bijlage 2a.		
Par.	**Titel (/sub-titel)**	**Bank**	**Verzekeraar**	**Pensioenfonds**
4.2.2	Risicomanagement: - (onafhankelijke) risicobeheerfunctie - systematische risicoanalyse	1, 2 en 10	1, 2, 6, 7, 11, 12 en 13	3, 4, 5, 8, 9 en 14
4.2.3	Risicomanagement: - periodieke risicoanalyse voor uitbesteding van kritieke of belangrijke functies	10 en 15	11, 13 en 15	4, 8, 14 en 15
5.1.3	Cloudcomputing: een vorm van uitbesteding	10 en 15	11 en 15	15
5.1.4	Definitie uitbesteding	1, 10 en 15	1, 6, 11, 13 en 15	4, 14 en 15
5.1.8	Beheerste en integere bedrijfsvoering	1, 2 en 10	1, 2, 6, 7, 12 en 13	3, 5, 8, 9 en 14
5.1.9	Uitbesteding van werkzaamheden	1, 2, 10 en 15	1, 2, 6, 7, 11, 12, 13 en 15	3, 4, 8, 9, 14 en 15
5.2.1	Uitbestedingsbeleid & -governance - Uitbestedingsbeleid & -procedures	2 en 10	2, 6, 7, 11, 12 en 13	4, 8, 9 en 14
5.2.2	Uitbestedingsbeleid & -governance - Kritieke of belangrijke uitbesteding	10 en 15	7, 11, 12, 13 en 15	15 + voetnoot[12]
5.2.3	Uitbestedingsbeleid & -governance - Deskundigheid	1 en 2	1, 2, 7, 12 en 13	3, 4, 8 en 14
5.2.4	Uitbestedingsbeleid & -governance - Schriftelijke kennisgeving aan toezichthouders	2, 10 en 15	2, 6, 7, 11, 12, 13 en 15	4, 8 en 15 + voetnoot[13]
5.2.5	Uitbestedingsbeleid & -governance - Bedrijfscontinuïteitsplannen	2, 10 en 15	2, 7, 11, 12, 13 en 15	8, 14 en 15
5.2.6	Uitbestedingsbeleid & -governance - Uitbestedingsregister	10	11 en 13	9
5.3.1	Selectie dienstverlener - Beoordeling kritieke of belangrijke functies (zie ook 5.5.2)	10	7, 11 en 13	4 en 14
5.3.2	Selectie dienstverlener - Risicobeoordeling vóór uitbesteding (zie ook 4.2.3)	10 en 15	11, 13 en 15	4, 8, 14 en 15
5.3.3	Selectie dienstverlener - Due diligence onderzoek	10	7, 11 en 13	4, 8 en 14
5.4.1	Uitbestedingsovereenkomst - Uitbestedingsovereenkomst (algemeen)	2, 10 en 15	2, 7, 11, 13 en 15	4, 8, 9, 14 en 15
5.4.2	Uitbestedingsovereenkomst - Beveiliging van gegevens en systemen	2, 10 en 15	2, 7, 11, 13 en 15	8 en 15
5.4.3	Uitbestedingsovereenkomst - Toegangs-, informatie- en auditrechten	2, 10 en 15	2, 7, 11, 13 en 15	4, 8, 14 en 15
5.4.4	Uitbestedingsovereenkomst - Onderuitbesteding	10 en 15	7, 11, 13 en 15	8, 9, 14 en 15
5.4.5	Uitbestedingsovereenkomst - Beëindigingsrechten	2, 10 en 15	2, 7, 11, 13 en 15	4, 14 en 15

[12] Toezichthouder DNB geeft op haar website aan dat o.a. pensioenfondsen sinds 13 januari 2019 wettelijk verplicht zijn om uitbesteding van werkzaamheden aan derde bij DNB te melden. Voor een aantal kritieke of belangrijke functies ('(onder)uitbestedingen') geldt dat DNB vooraf geïnformeerd moet worden.
[13] Idem.

Verwijzing naar paragraaf en onderwerpen		De nummers corresponderen met bijlage 2a.		
Par.	**Titel (/sub-titel)**	**Bank**	**Verzekeraar**	**Pensioenfonds**
5.5.1 **5.5.2** **5.5.3** **5.5.4**	Monitoring dienstverlener - Monitoring- & controle mechanisme - Bewaken prestaties & IB dienstverlener - Beoordelen assurance rapportages - Bijwerken risicobeoordeling (4.2.3 & 5.3.2)	2 en 10	2, 7, 11 en 13	4 en 14
5.6.1 **5.6.2**	Evaluatie dienstverlener - Evaluatie dienstverlener - Exitstrategie	2 en 10	2, 6, 7, 11 en 13	4, 9 en 14

Bijlage 3 – Overzicht detaillering vereisten, voorwaarden en overige informatie

In deze bijlage zijn per sub-paragraaf van hoofdstuk 5 (indien aanwezig) voorbeelden van vereisten, voorwaarden en overige informatie opgenomen.

Par.	Omschrijving wettelijke vereisten/voorwaarden/overige informatie
5.2.1	**(cloud)uitbesteding uitbestedingsbeleid & -governance – onderdeel: uitbestedingsbeleid & -procedures**
	Voorbeelden van onderwerpen in het uitbestedingsbeleid & -procedures: • De doelstellingen van uitbesteding door de financiële instellingen; • De reikwijdte van uitbesteding, waarbij expliciet wordt aangegeven wat niet mag worden uitbesteed; • De verantwoordelijkheden en betrokkenheid van het bestuur van de financiële instelling bij de besluitvorming over het uitbesteden van kritieke of belangrijke functies; • De betrokkenheid van bedrijfsonderdelen (bijv. ICT en informatiebeveiliging) en interne controle functies (bijv. compliance, risicobeheer en interne audits); • Het gebruik van clouddiensten moet in overeenstemming zijn de strategieën van de financiële instelling (zoals: bedrijfsstrategie, ICT-strategie en informatiebeveiligingsstrategie) en in lijn met interne beleidslijnen en processen; • Een duidelijk onderscheid tussen “Kritieke of belangrijke functies” en andere uitbestedingen. Bij “Kritieke of belangrijke functies” wordt rekening gehouden met mogelijke effecten op het risicoprofiel van de instelling, het monitoren van de (cloud)dienstverlener, het beheersen van risico’s, het monitoren van bedrijfscontinuïteit en de uitoefening van de bedrijfsactiviteiten; • De uitbestedingsvoorwaarden (zie paragrafen 5.3 en 5.4), zoals: de beoordeling van risico’s, de frequentie van de beoordeling van de prestaties en resultaten (bijv. SLA), het omgaan met belangen conflicten, business continuity en de goedkeuring van uitbestedingsovereenkomsten; • De wijze waarop de monitoring (zie paragraaf 5.5) van de dienstverlener plaatsvindt met in achtneming van de omvang en complexiteit van de inherente risico’s van de geleverde (cloud)diensten. Hieronder begrepen de monitoring van de naleving van de uitbestedingsovereenkomst, SLA, beveiligingsnormen en wet- en regelgeving. Alsook in relatie tot de uitkomsten van het due diligence en uitgevoerde risico analyses; • De wijze waarop en wanneer evaluatie (zie paragraaf 5.6) van de dienstverlener en het uitbestedingsbeleid in alle stappen van het uitbestedingsproces plaatsvindt; • Voor uitbesteding van kritieke of belangrijke functies betreffende clouddiensten dient een gedocumenteerde en (evt. geteste) “exitstrategie” die in verhouding staat tot de aard, omvang en complexiteit van de inherente risico’s van de geleverde, diensten te worden beschreven.
5.2.2	**(cloud)uitbesteding uitbestedingsbeleid & -governance – onderdeel: kritieke of belangrijke functies**
	Voorbeelden van voorwaarden voor het beoordelen of sprake is van kritieke of belangrijke functies: • De mogelijke gevolgen van een wezenlijke verstoring van de uitbestede functie of activiteit met impact op de naleving van wet- en regelgeving, bedrijfscontinuïteit, operationele veerkracht, operationele risico’s (w.o. gedrag, ICT en juridische risico’s) en reputatierisico; • De mogelijke gevolgen van de uitbestedingsovereenkomst betreffende clouddiensten om alle risico’s vast te stellen, te bewaken en te beheren, het voldoen aan wettelijke vereisten en het kunnen uitvoeren van gepaste audits op de uitbestede functie of activiteiten; • De mogelijke gevolgen voor de diensten aan klanten van de financiële instelling; • De geaggregeerde blootstelling van de financiële instelling aan dezelfde cloud aanbieder; • De mogelijkheid om op te schalen zonder de onderliggende overeenkomst te vervangen of te herzien; • De mate waarin het mogelijk is om de clouddienst aan een andere dienstverlener over te dragen of te herintegreren bij de financiële instelling;

Par.	Omschrijving wettelijke vereisten/voorwaarden/overige informatie
	• De bescherming van persoons- en niet-persoonsgebonden gegevens en de mogelijke gevolgen voor de financiële instelling, haar klanten en andere betrokken van een schending van vertrouwelijkheid of het niet-waarborgen van beschikbaarheid en integriteit van gegevens op grond van ondermeer de privacywetgeving ('AVG'). In het bijzonder moet rekening gehouden worden met bedrijfsgeheimen en/of gevoelige persoonsgegevens.
5.2.4	**(cloud)uitbesteding uitbestedingsbeleid & -governance – onderdeel: Schriftelijke kennisgeving aan toezichthouders**
	Voorbeelden van informatie die moet worden gemeld aan de toezichthouder: • Een korte omschrijving van de operationele functie of activiteit en de reden waarom de uitbesteding als kritieke of belangrijke functies wordt beschouwd; • De aanvangsdatum, einddatum en/of opzegtermijnen voor de dienstverlener en de financiële instelling; • Contractuele afspraken, zoals: exit-clausule, toegangs-, informatie- en auditrecht voor de toezichthouder en financiële instelling, voorwaarden voor onderuitbesteding en risicoanalyse op basis van een template van toezichthouder DNB; • Het recht dat van toepassing is op de uitbestedingsovereenkomst met de dienstverlener; • De naam en contactgegevens van de dienstverlener; • De cloud service- en implementatie model (zie sub-paragrafen 4.1.3 en 4.1.4) en de specifieke aard van de te bewaren gegevens en locaties (landen of regio's) waar de gegevens worden opgeslagen.
5.2.6	**(cloud)uitbesteding uitbestedingsbeleid & -governance – onderdeel: Uitbestedingsregister**
	Voorbeelden van informatie voor het uitbestedingsregister: • De informatie zoals opgenomen bij "Schriftelijke kennisgeving aan toezichthouders"; • De datum waarop de laatste risicobeoordeling heeft plaatsgevonden en een korte samenvatting met de belangrijkste uitkomsten; • Het besluitvormingsorgaan (of persoon) dat de (cloud)uitbestedingsovereenkomst heeft goedgekeurd; • De data van de meest recente en volgende geplande audits (indien van toepassing) • De datum waarop het kritieke of belangrijke functies voor laatst is beoordeeld; • De namen van onderuitbestedingspartijen waaraan materiele onderdelen van kritieke of belangrijke functies worden onderuitbesteed (incl. landen waarvandaan de diensten worden uitgevoerd en locatie waar de gegevens worden opgeslagen); • Het resultaat van de beoordeling van de vervangbaarheid van de dienstverlener (bijvoorbeeld eenvoudig, moeilijk of onmogelijk), de mogelijkheid om de uitbesteding opnieuw bij de financiële instelling te integreren en het effect van de beëindiging van de kritieke of belangrijke functies; • Alternatieve dienstverleners in relatie tot het vorige punt; • De gegevens met betrekking tot de kritieke of belangrijke functies tijdgevoelige bedrijfsactiviteiten ondersteunt; • De geraamde jaarlijkse begrotingskosten; • De gegevens met betrekking tot de exitstrategie (bij beëindiging van de diensten van de dienstverlener of verstoringen bij de dienstverlener).
5.4.1	**(cloud)uitbesteding overeenkomst - onderdeel: uitbestedingsovereenkomst**
	Voorbeelden van rechten en plichten in de uitbestedingsovereenkomst: • Een duidelijke omschrijving van de werkzaamheden (incl. soort clouddiensten) en onder welke voorwaarden deze worden uitbesteed; • De aanvangsdatum, einddatum en/of opzegtermijnen voor de dienstverlener en de financiële instelling; • De bevoegde rechtbank en wetgeving die van toepassing is op de overeenkomst;

Par.	Omschrijving wettelijke vereisten/voorwaarden/overige informatie
	• De financiële verplichtingen van partijen; • De vermelding of onderuitbesteding van kritieke of belangrijke functies is toegestaan, en zo ja, onder welke voorwaarden; • De locatie van waar de gegevens worden bewaard en verwerkt in datacenters (incl. voorwaarden waar aan moet worden voldaan en hoe de financiële instellingen in kennis gesteld moet worden bij voorstellen om de locatie te wijzigen); • De bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, privacy en veiligheid van de relevante gegevens; • Het recht om de prestaties van de dienstverlener doorlopend te bewaken; • De overeengekomen niveaus van dienstverlening met kwantitatieve en kwalitatieve prestatiedoelen in een SLA om tijdige controle mogelijk te maken; • De verplichting van de dienstverlener om te rapporteren aan de financiële instelling door middel van bijvoorbeeld een SLA-rapportage, informatiebeveiligingsrapportage en auditrapportages; • De vermelding of de dienstverlener zich moet verzekeren tegen bepaalde risico's en indien van toepassing de vereiste hoogte van de verzekeringsdekking; • De vereiste inzake de invoering en het testen van bedrijfscontinuïteitsplannen; • De wijze waarop informatie uitwisseling tussen de financiële instelling en de dienstverlener plaatsvindt (bijvoorbeeld: het geven van instructie en het rapporteren door middel van een SLA-rapportage); • De afspraken over toegangs-, informatie- en auditrechten voor de toezichthouder en financiële instelling; • De mogelijkheid om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de dienstverlener geschiedt (bijvoorbeeld als gevolg van een instructie of aanwijzing van een toezichthouder); • De verplichting dat de dienstverlener de financiële instelling instaat stelt om blijvend te voldoen aan wet- en regelgeving; • De wijze waarop de overeenkomst eindigt en wordt gewaarborgd dat de financiële instelling de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere dienstverlener kan laten uitvoeren.
5.4.2	**(cloud)uitbesteding overeenkomst - onderdeel: Beveiliging van gegevens en systemen**
	Voorbeelden van eisen voor beveiliging van gegevens en systemen in de uitbestedingsovereenkomst: • Een duidelijke verdeling van taken en verantwoordelijkheden tussen de aanbieder van clouddiensten en haar zelf met betrekking tot operationele functies of activiteiten die door de uitbesteding van clouddiensten worden beïnvloed; • Een passend beschermingsniveau voor de vertrouwelijkheid van gegevens, de continuïteit van de uitbestede activiteiten en de integriteit en herleidbaarheid van gegevens en systemen; • Nagaan of specifieke maatregelen nodig zijn voor gegevens in transit, opgeslagen gegevens in het geheugen en gegevens in ruststand (bijvoorbeeld de toepassing van encryptie in combinatie met een passend sleutelbeheer; • De beschikbaarheid van netwerkverkeer en verwachte capaciteit; • Gepaste continuïteitsvereisten op ieder niveau van de technologische keten; • Een gedegen en goed gedocumenteerd incidentenbeheerproces (incl. verantwoordelijkheden van beide partijen); • Een risico gebaseerde aanpak gehanteerd met betrekking tot de locatie(s) van gegevensopslag en -verwerking en beveiliging.

Par.	Omschrijving wettelijke vereisten/voorwaarden/overige informatie
5.4.3	**(cloud)uitbesteding overeenkomst - onderdeel: toegangs-, informatie- en auditrechten**
	Overzicht met voorwaarden over toegangs-, informatie- en auditrechten in de uitbestedingsovereenkomst: • Volledige toegang verleent tot alle relevante bedrijfslocaties inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestede functie te verrichten, waaronder bijbehorende financiële informatie, personeel en de externe auditors van de dienstverlener ("toegangs- en informatierechten"); en • Een onbeperkt recht van inspectie en audits verleent met betrekking tot de uitbestedingsovereenkomst ("auditrechten") om hen in staat te stellen de uitbestedingsovereenkomst te bewaken en er voor te zorgen dat aan alle toepasselijke wet- en regelgeving en contractuele voorschriften wordt voldaan.
5.4.4	**(cloud)uitbesteding overeenkomst - onderdeel: onderuitbesteding**
	Voorbeelden van voorwaarden met betrekking tot onderuitbesteding in de uitbestedingsovereenkomst: • Alle soorten activiteiten die van onderuitbesteding zijn uitgesloten; • De voorwaarden waaraan moet worden voldaan bij onderuitbesteding (bijvoorbeeld dat de onderuitbestedingspartij de relevante verplichtingen van de dienstverlener ook volledig moet naleven, zoals: toegangs-, informatie- en auditrechten, voldoen aan wet- en regelgeving en de beveiliging van gegevens en systemen); • De dienstverlener blijft volledig aansprakelijk en de onderuitbestede diensten moet monitoren en controleren; • De dienstverlener moet de financiële instelling tijdig in kennis stellen van de voorgenomen belangrijke wijziging van onderuitbesteding die ertoe zouden kunnen leiden dat de dienstverlener minder goed in staat is de verplichtingen uit hoofde van de uitbestedingsovereenkomst na te komen. • De financiële instelling moet het recht hebben om bewaar te maken tegen de voorgenomen belangrijke wijziging van onderuitbesteding als dit nadelig is voor het risicoprofiel van de financiële instelling en/of de overeenkomst te beëindigen. • Het bestuur blijft eindverantwoordelijk voor de hele keten van uitbesteding.
5.4.5	**(Cloud)uitbesteding overeenkomst - onderdeel: beëindigingsrechten**
	Voorbeelden van voorwaarden waarbij de uitbestedingsovereenkomst moet worden beëindigd: • De dienstverlener overtreedt geldende wet- en regelgeving of contractuele bepalingen; • De dienstverlener voert materiële wijzigingen door die gevolgen hebben voor de uitvoering van de uitbestedingsovereenkomst (bijv. onderuitbesteding of wijziging in onderuitbestedingspartijen) • De dienstverlener treft onvoldoende maatregelen met betrekking tot het beheer en beveiliging van vertrouwelijke, persoonlijke of anderszins gevoelige gegevens of informatie waardoor zwakke punten ontstaan. • De toezichthouder geeft instructies aan de financiële instelling (bijvoorbeeld doordat de toezichthouder niet in staat is om haar taken effectief uit te voeren).
5.5.2	**(cloud)uitbesteding monitoring – onderdeel: bewaken prestaties & informatiebeveiliging dienstverlener**
	Voorbeelden van monitoring rapportages & relevante informatie zijn: • Service level rapportages met daarin kritische performance indicatoren over beschikbaarheid (in %), aantallen en aard (cyber)securityincidenten en oplostijden van incidenten; • Service level rapportages met daarin kritische risico indicatoren (voorbeelden zijn: aantal verstoring met direct operationeel effect op de dienstverlening, aantal data-incidenten, mate van compliance aan wet- en regelgeving en concentraties op dienstverleners) • Andere relevante informatie (w.o. verslagen over maatregelen en testen op het gebied van bedrijfscontinuïteit).

Par.	Omschrijving wettelijke vereisten/voorwaarden/overige informatie
5.5.3	**(cloud)uitbesteding monitoring – onderdeel: beoordelen assurance rapportage & opvolging bevindingen**
	Voorbeelden van assurance rapportages zijn: • Certificeringen en onafhankelijke (externe) audit rapportages, zoals: ISAE 3402, SOC2 of ISAE 3000 verklaring.
5.6.2	**(cloud)uitbesteding monitoring – onderdeel: exitstrategie**
	Voorbeelden van activiteiten voor het bepalen van een exitstrategie: • Vaststellen doelen van de exitstrategie; • Uitvoeren van een bedrijfsimpactanalyse in verhouding tot het risico van de uitbestede processen, diensten of activiteiten met als doel om na te gaan welke personele of financiële middelen nodig zijn om het exitplan uit te voeren en hoe lang dat zou duren; • Toewijzen van taken, verantwoordelijkheden en middelen voor het beheer van exitplannen en het overbrengen van activiteiten; • Bepalen criteria of de overdracht van uitbestede functies en gegevens geslaagd is; • Vaststellen indicatoren voor de monitoring van de uitvoering van de uitbestedingsovereenkomst (zie “Fase 4: Monitoring”) en indicatoren die zijn gebaseerd op onaanvaardbare niveaus van dienstverlening niet tot een exit moeten leiden; • Het bestuur beoordeelt periodiek of de uitvoerder zodanig functioneert dat het bestuur door wil gaan met de uitbesteding.

Bijlage 4 – Checklist beheersing (cloud)uitbesteding

Deze checklist is opgesteld op basis van het onderzoek in de literatuur en wet- en regelgeving. De beheersmaatregelen zijn geformuleerd op basis van de geïdentificeerde wettelijke vereisten. De checklist is van toepassing op uitbesteding en het gebruik maken van clouddiensten.

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Beheersmaatregelen (o.b.v. wettelijke vereisten)	Check
4.2	**Risicomanagement**		
4.2.2	Systematische risicoanalyse	• De FI beschikt over een risicobeheerfunctie die op systematische wijze onafhankelijk risicobeheer uitvoert dat gericht is op het identificeren, meten en evalueren van (uitbestedings)risico's; • De FI voert periodiek een systematische risicoanalyse met als uitgangspunt de missie, visie en strategie. • De FI legt de randvoorwaarden voor de beheerste uitvoering van alle kernactiviteiten vast.	
4.2.3	Periodieke uitbestedingsrisicoanalyse voor KOB *Dit onderdeel heeft ook betrekking op 'Selectie dienstverlener' en 'Monitoring dienstverlener'.*	• De FI voert voorafgaand aan uitbesteding een risicoanalyse uit o.b.v. de in sub-paragrafen 4.2.4 en 4.2.5 benoemde uitbesteding- en cloudrisico's. • De FI werkt de uitbestedingsrisicoanalyse voor 'Kritieke of belangrijk functies' periodiek bij (zie sub-paragraaf 5.5.4). • De FI beoordeelt bij uitbesteding van 'Kritieke of belangrijke functies' (indien van toepassing en waar nodig) de juridische-, ICT-, naleving- en reputatierisico's en toezichtbeperkingen die het gevolg kunnen zijn van het soort clouddienst, migratie en/of implementatie, de gevoeligheid van gegevens, systemen en de beveiligingsmaatregelen, politieke stabiliteit en beveiligingssituatie waar de activiteiten worden uitgevoerd en de gegevens worden opgeslagen, onderuitbesteding (incl. lange en complexe ketens van onderuitbesteding) en concentratierisico (zie sub-paragrafen 5.3.2 en 5.5.4). • Over de uitkomsten van de risicobeoordeling wordt gerapporteerd aan het bestuur.	
5.2	**Uitbestedingsbeleid & -governance**		
5.2.1	Uitbestedingsbeleid & -procedures	• De FI legt de doelstelling, reikwijdte en randvoorwaarden vast in een schriftelijk uitbestedingsbeleid dat wordt goedgekeurd door het bestuur. Het bestuur blijft altijd eindverantwoordelijk voor alle activiteiten van de financiële instelling. • De FI werkt het beleid uit in administratieve en organisatorische procedures die worden uitgedragen aan de medewerkers. • De FI evalueert het uitbestedingsbeleid ten minste eenmaal per drie jaar. • De FI neemt in haar uitbestedingsbeleid op de onderwerpen, zoals beschreven in bijlage 3, bij paragraaf 5.2.1.	
5.2.2	Kritieke op belangrijke functies *NB. Dit is relevant voor de intensiteit van de beheersing van de (cloud)uitbesteding.*	• De FI bepaalt voorafgaand aan uitbesteding of sprake is van 'Kritieke of belangrijke functies'. Om te bepalen of sprake is van 'Kritieke of belangrijke functies' kan de FI gebruik maken van de voorwaarden, zoals opgenomen in bijlage 3, bij sub-paragraaf 5.2.2.	

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Beheersmaatregelen (o.b.v. wettelijke vereisten)	Check
5.2.3	Deskundigheid	• De FI beschikt over voldoende kennis, competenties en 'counter vailing power' voor het houden van regie op de uitbesteding, de uitbestede werkzaamheden adequaat te beoordelen en tijdig bij te sturen. • De FI kan voorstellen van de dienstverlener beargumenteren met voor- en nadelen en waar mogelijk met alternatieven. • De FI beschikt over voldoende deskundigheid (bijv. ICT en bedrijfskennis) die nodig is om risico's en de beheersing van de uitbestedingsrelatie te beoordelen.	
5.2.4	Schriftelijke kennisgeving aan toezichthouders	• De FI stelt haar toezichthouder(s) schriftelijk in kennis van voorgenomen uitbesteding van een 'Kritieke of belangrijke functie'. In bijlage 3, bij sub-paragraaf 5.2.4, zijn voorbeelden van informatie die aan de toezichthouder moet worden gemeld beschreven. • De FI informeert haar toezichthouder(s) tijdig over materiële wijzigingen en/of ernstige gebeurtenissen bij dienstverleners die grote gevolgen kunnen hebben op het voortzetten van de bedrijfsactiviteiten van de FI.	
5.2.5	Bedrijfscontinuïteitsplannen	• De FI heeft passende bedrijfscontinuïteitsplannen m.b.t. 'Kritieke of belangrijke functies'. Hierin wordt o.a. rekening gehouden met mogelijke gevolgen van insolventie of andere vormen van falen van de dienstverlener en, waar relevant, politieke risico's in het rechtsgebied van de dienstverlener. • De FI onderhoud de bedrijfscontinuïteitsplannen en test deze plannen periodiek.	
5.2.6	Uitbestedingsregister	• De FI documenteert haar uitbestedingen in een uitbestedingsregister. In bijlage 3, bij sub-paragraaf 5.2.6, zijn voorbeelden van informatie voor in het uitbestedingsregister opgenomen voor 'Kritieke of belangrijke functies'. • De FI documenteert haar niet-kritieke of belangrijke functies in een uitbestedingsregister. O.b.v. de aard, omvang en complexiteit van de inherente risico's wordt bepaald welke informatie relevant is voor het uitbestedingsregister. • De FI onderhoudt het uitbestedingsregister regelmatig (minimaal eenmaal per jaar).	
5.3	**Selectie dienstverlener**		
5.3.1	Beoordeling kritieke of belangrijke functies	• Zie sub-paragraaf 5.2.2 (in deze checklist).	
5.3.2	Risicobeoordeling vóór uitbesteding	• Zie sub-paragraaf 4.2.3 (in deze checklist).	
5.3.3	Due diligence onderzoek	• De FI voert voorafgaand aan een uitbesteding een due diligence onderzoek uit. Het doel is om vast te stellen dat de dienstverlener kan voldoen aan de vereisten in het uitbestedingsbeleid. • De FI voert bij uitbesteding van 'Kritieke of belangrijke functies' een evaluatie van geschiktheid van de dienstverlener uit. Hierin worden bijvoorbeeld opgenomen: vaardigheden, infrastructuur, economische situatie en bedrijfs- en juridische status. In het due diligence onderzoek kan gebruik worden gemaakt van certificeringen op basis van internationale normen en interne of externe audit rapportages. • De FI beoordeelt onder meer de volgende aspecten in het due diligence onderzoek bij uitbesteding van een 'Kritieke of belangrijke functie': bedrijfsreputatie, passende en toereikende bekwaamheden, deskundigheid, capaciteit, middelen (bijv.	

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Beheersmaatregelen (o.b.v. wettelijke vereisten)	Check
		personeel, IT en financieel), beloningsbeleid, organisatiestructuur en bedrijfsmodel (incl. karakter, omvang, complexiteit, financiële situatie, eigendoms- en groepsstructuur). • De FI beoordeelt indien de uitbesteding het verwerken van persoonsgegevens of vertrouwelijke gegevens omvat, de passende technische en organisatorische maatregelen om deze gegevens te beschermen. (zie ook sub-paragrafen 5.1.6 'Gegevensbescherming' en 5.1.7 'Datawetgeving met extraterritoriale werking') • De FI zet de nodige stappen om ervoor te zorgen dat dienstverleners handelen op een wijze die strookt met hun waarden en gedragscode, met name wat betreft dienstverleners in derde landen en hun onderaannemers, zoals: ethische en maatschappelijke verantwoorde handelswijze, internationale normen op het gebied van mensenrechten, milieubescherming en passende arbeidsomstandigheden (incl. verbod op kinderarbeid).	
5.4	**Uitbestedingsovereenkomst**		
5.4.1	Uitbestedingsovereenkomst (algemeen)	• De FI neemt de rechten en plichten op in de uitbestedingsovereenkomst. In bijlage 3, bij sub-paragraaf 5.4.1 zijn voorbeelden van deze rechten en plichten opgenomen.	
5.4.2	Beveiliging van gegevens en systemen	• De FI neemt in de uitbestedingsovereenkomst eisen voor beveiliging van gegevens en systemen op. In bijlage 3, sub-paragraaf 5.4.2, zijn voorbeelden van vereisten voor beveiliging van gegevens en systemen opgenomen. • De FI ziet er op toe dat de eisen voor beveiliging van gegevens en systemen worden nageleefd.	
5.4.3	Toegangs-, informatie- en auditrechten	• De FI neemt voor uitbesteding van 'Kritieke of belangrijke functies' in de uitbestedingsovereenkomst voorwaarden over toegangs-, informatie- en auditrechten op. In Bijlage 3, sub-paragraaf 5.4.3, is een overzicht met voorwaarden over toegangs-, informatie- en auditrechten opgenomen. • De FI ziet er op toe dat uitbesteding geen belemmering vormt voor de effectieve uitoefening van toegangs-, informatie- en auditrecht van de FI en haar toezichthouder(s). • De FI mag gebruik maken van de door de dienstverlener versterkte externe certificeringen en (externe of interne) auditverslagen. De FI moet beoordelen of deze certificeringen of auditverslagen voldoende zijn om aan regelgevingsverplichtingen te voldoen. Idem voor de reikwijdte en uitvoering van de audit volgens gepaste normen. Bovendien mag de FI niet uitsluitend vertrouwen op deze certificeringen en auditverslagen. • De FI moet het recht hebben om naar redelijkheid de reikwijdte van de certificeringen of auditrapportages uit te breiden. • De FI moet het recht behouden om naar eigen inzicht audits op locatie uit te voeren. Aangezien cloudoplossingen technisch bijzonder complex zijn, moet de FI er voor zorgdragen dat de door haar aangestelde auditors over de juiste vaardigheden beschikken. Indien de uitoefening van het toegangs- of auditrecht een risico oplevert voor de omgeving van de aanbieder van clouddiensten en/of andere klanten van de aanbieder van clouddiensten, dan moeten de FI en aanbieder van clouddiensten een alternatieve manier overeenkomen om een vergelijkbaar niveau van betrouwbaarheid en dienstverlening te verwezenlijken (bijvoorbeeld een verslag of specifieke certificering).	

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Beheersmaatregelen (o.b.v. wettelijke vereisten)	Check
5.4.4	Onderuitbesteding	• De FI neemt in de uitbestedingsovereenkomst op onder welke voorwaarden onderuitbesteding is toegestaan (of niet). In bijlage 3, bij sub-paragraaf 5.4.4, is een overzicht met voorwaarden met betrekking tot onderuitbesteding opgenomen.	
5.4.5	Beëindigingsrechten	• De FI neemt in de uitbestedingsovereenkomst op onder welke voorwaarden de uitbestedingsovereenkomst moet worden beëindigd. In bijlage 3, sub-bij paragraaf 5.4.5, is een overzicht met voorwaarden waarbij de uitbestedingsovereenkomst moet worden beëindigd opgenomen.	
5.5	**Monitoring dienstverlener**		
5.5.1	Monitoring- & controlemechanisme	• De FI richt voor de monitoring van dienstverleners monitoring- en controlemechanisme in. • De FI zorgt voor voldoende personeel dat over voldoende vaardigheden en kennis beschikt om de naar de cloud uitbestede diensten te monitoren.	
5.5.2	Bewaken prestaties & informatiebeveiliging dienstverlener	• De FI monitort risk-based voortdurend de prestaties van activiteiten, de beveiligingsmaatregelen en naleving van de overeengekomen afspraken via een risico gebaseerde aanpak in de zin dat de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en informatie. De nadruk ligt hierbij op 'Kritieke of belangrijke functies'. In bijlage 3, sub-paragraaf 5.5.2, zijn voorbeelden van monitoring rapportages & overige informatie opgenomen.	
5.5.3	Beoordelen assurance rapportages & opvolging bevindingen	• De FI beoordeelt assurance rapportages, waarbij aandacht is voor onder meer de reikwijdte, aansluiting met de uitbestede dienst en periode waarover assurance is afgegeven. • De FI monitort de opvolging van bevindingen in assurance rapportages actief. De FI treft maatregelen als tekortkomingen worden geconstateerd. Passende corrigerende of herstelmaatregelen moeten worden getroffen. Indien dit niet mogelijk is, dan wordt de uitbestedingsovereenkomst met onmiddellijke ingang beëindigd. In Bijlage 3, sub-paragraaf 5.5.3, zijn voorbeelden van assurance rapportages opgenomen.	
5.5.4	Bijwerken risicobeoordeling	• Zie paragraaf 4.2.3 (in deze checklist).	
5.6	**Evaluatie dienstverlener**		
5.6.1	Periodieke evaluatie	• De FI voert jaarlijks een evaluatie uit van de dienstverlener bij een 'Kritieke of belangrijke functie'. Hierbij worden onder meer het behalen van de performance afspraken, uitkomsten van de monitoring (zie paragraaf 5.5.2) en mogelijke grote wijzigingen bij de dienstverlener geëvalueerd, zoals: wijziging in de strategie, de winstgevendheid en eigendomsverhoudingen. • De FI voert periodiek een evaluatie van de dienstverlener uit aan de hand van de randvoorwaarden en eisen in het uitbestedingsbeleid. Zie sub-paragraaf 5.2.1 (in deze checklist). • De FI beoordeelt of de dienstverlener bijdraagt aan het behalen van de doelen van de FI. • De evaluatie leidt tot een besluit om de dienstverlening te continueren of te beëindigen.	
5.6.2	Exitstrategie	• De FI heeft voor uitbesteding van kritieke of belangrijke functies een gedocumenteerde exitstrategie in lijn met het uitbestedingsbeleid en business continuity plannen. In de exitstrategie wordt onder meer rekening gehouden dat de uitbestedingsovereenkomst wordt beëindigd, de dienstverlener faalt en de kwaliteit van de dienst verslechterd of kan leiden	

Par.	Onderdelen conceptueel (cloud)uitbestedingsmodel	Beheersmaatregelen (o.b.v. wettelijke vereisten)	Check
		tot bedrijfsverstoringen. De exitstrategieën beogen er aan te kunnen bij dragen dat financiële instellingen zich kunnen terugtrekken zonder dat dit hun bedrijfsactiviteiten onnodig verstoord, regelgevingsvereisten minder goed naleven en zonder dat dit ten koste gaat van de continuïteit en kwaliteit van hun dienstverlening aan klanten. In bijlage 3, bij sub-paragraaf 5.6.2, zijn voorbeelden van activiteiten voor het bepalen van een exitstrategie opgenomen. • De FI ontwikkelt en implementeert exitplannen die volledig, gedocumenteerd en waar nodig getoetst zijn. • De FI onderzoekt alternatieve oplossingen, stelt overgangsplannen op waarmee de uitbestede functies en gegevens bij een dienstverlener kan weghalen en draagt ervoor zorg dat de 'Kritieke of belangrijke functies' kunnen worden voortgezet (intern of bij een andere dienstverlener).	

Bijlage 5 – Casestudy Microsoft Agreement

In deze bijlage is een toetsing ('match') uitgevoerd conceptueel (cloud)uitbestedingsmodel m.b.t. de checklist (zie Bijlage 4). De toetsing is gericht op één onderdeel uit het conceptueel (cloud)uitbestedingsmodel en checklist, namelijk de 'Uitbestedingsovereenkomst' (zie paragraaf 5.4). Hierbij is vervolgens getoetst in hoeverre dit onderdeel kan worden vergeleken met een Microsoft Cloud Mapping For Financial institutions in Europe[14]. In het kader van de focus van dit onderzoek op banken, verzekeraars en pensioenfondsen is de toetsing voor zowel de EBA *Richtsnoeren inzake uitbesteding* (2019) als de EIOPA *Richtsnoeren uitbesteding aan aanbieders van clouddiensten* (2020).

Legenda beoordelingscriteria		
	=	Match t.o.v. conceptueel (cloud)uitbestedingsmodel
	=	Mismatch t.o.v. conceptueel (cloud)uitbestedingsmodel

			EBA		EIOPA		Microsoft	
5.4	**Uitbestedings-overeenkomst**	**Conceptueel (cloud)uitbestedingsmodel (gebaseerd op bijlage 4, paragraaf 5.4)**	**Richt-snoer**	**Art.**	**Richt-snoer**	**Art.**	**Mapping**	**Match**
5.4.1	Uitbestedings-overeenkomst (algemeen)	• De FI neemt de rechten en plichten op in de uitbestedingsovereenkomst.	13	74	10	36	1	
		• Een duidelijke omschrijving van de werkzaamheden (incl. soort clouddiensten) en onder welke voorwaarden deze worden uitbesteed;	13	75a	10	37a	2	
		• De aanvangsdatum, einddatum en/of opzegtermijnen voor de dienstverlener en de financiële instelling;	13	75b	10	37b	3	
		• De bevoegde rechtbank en wetgeving die van toepassing is op de overeenkomst;	13	75c	10	37c	4	
		• De financiële verplichtingen van partijen;	13	75d	10	37d	5	
		• De vermelding of onderuitbesteding van kritieke of belangrijke functies is toegestaan, en zo ja, onder welke voorwaarden;	13	75e 76	10	37e	7	

[14] https://servicetrust.microsoft.com/DocumentPage/2f18eb43-64df-424c-8d59-98c18b7cb9e0

			EBA		EIOPA		Microsoft	
5.4	**Uitbestedings-overeenkomst**	**Conceptueel (cloud)uitbestedingsmodel (gebaseerd op bijlage 4, paragraaf 5.4)**	**Richt-snoer**	**Art.**	**Richt-snoer**	**Art.**	**Mapping**	**Match**
		• De locatie van waar de gegevens worden bewaard en verwerkt in datacenters (incl. voorwaarden waar aan moet worden voldaan en hoe de financiële instellingen in kennis gesteld moet worden bij voorstellen om de locatie te wijzigen);	13	75f	10	37f	17	
		• De bepalingen inzake toegankelijkheid, beschikbaarheid, integriteit, privacy en veiligheid van de relevante gegevens;	6 6 12.3 13.2	40d 40g 72 84	10	37g	21	
		• Het recht om de prestaties van de dienstverlener doorlopend te bewaken;	13 14 14	75h 100 104	10	37h	22	
		• De overeengekomen niveaus van dienstverlening met kwantitatieve en kwalitatieve prestatiedoelen in een SLA om tijdige controle mogelijk te maken;	13	75i	10	37i	23	
		• De verplichting van de dienstverlener om te rapporteren aan de financiële instelling door middel van bijvoorbeeld een SLA-rapportage, informatiebeveiligingsrapportage en auditrapportages;	6 11 13	40e 59 75j	10	37j	24	
		• De vermelding of de dienstverlener zich moet verzekeren tegen bepaalde risico's en indien van toepassing de vereiste hoogte van de verzekeringsdekking;	13	75k	10	37k	6	
		• De vereiste inzake de invoering en het testen van bedrijfscontinuïteitsplannen;	9 9 14 13	48 49 104c 75l	10	37l	25	
		• De wijze waarop informatie uitwisseling tussen de financiële instelling en de dienstverlener plaatsvindt (bijvoorbeeld: het geven van instructie en het rapporteren door middel van een SLA-rapportage);	13	75i	10	37i	23	
		• De afspraken over toegangs-, informatie- en auditrechten voor de toezichthouder en financiële instelling;	Zie 5.4.2 (verderop in deze tabel)				29 t/m 33	
		• De mogelijkheid om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de dienstverlener geschiedt (bijvoorbeeld als gevolg van een instructie of aanwijzing van een toezichthouder). *(bron: art. 31 lid 2d Bpr Wft)*	-	-	-	-	-	

			EBA		EIOPA		Microsoft	
5.4	**Uitbestedings-overeenkomst**	**Conceptueel (cloud)uitbestedingsmodel (gebaseerd op bijlage 4, paragraaf 5.4)**	**Richt-snoer**	**Art.**	**Richt-snoer**	**Art.**	**Mapping**	**Match**
		• De verplichting dat de dienstverlener de financiële instelling instaat stelt om blijvend te voldoen aan wet- en regelgeving;	13.1	79a	-	-	15	
		• De wijze waarop de overeenkomst eindigt en wordt gewaarborgd dat de financiële instelling de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere dienstverlener kan laten uitvoeren.	6 7 13.4 15	40f 42f 99a-c 106-108	3	20f	40 41 42 43	
5.4.2	Beveiliging van gegevens en systemen	• Een duidelijke verdeling van taken en verantwoordelijkheden tussen de aanbieder van clouddiensten en haar zelf met betrekking tot operationele functies of activiteiten die door de uitbesteding van clouddiensten worden beïnvloed;	13.2 13.3	82 94	3 12	20a 48 49	20	
		• Een passend beschermingsniveau voor de vertrouwelijkheid van gegevens, de continuïteit van de uitbestede activiteiten en de integriteit en herleidbaarheid van gegevens en systemen;	12.3 13 13.2	72 75g 81	10 12	37g 47	18 19	
		• Nagaan of specifieke maatregelen nodig zijn voor gegevens in transit, opgeslagen gegevens in het geheugen en gegevens in ruststand (bijvoorbeeld de toepassing van encryptie in combinatie met een passend sleutelbeheer;	13.2 13.3	82 94	3 12	20a 48 49	20	
		• De beschikbaarheid van netwerkverkeer en verwachte capaciteit;						
		• Gepaste continuïteitsvereisten op ieder niveau van de technologische keten;						
		• Een gedegen en goed gedocumenteerd incidentenbeheerproces (incl. verantwoordelijkheden van beide partijen);						
		• Een risico gebaseerde aanpak gehanteerd met betrekking tot de locatie(s) van gegevensopslag en -verwerking en beveiliging.						
5.4.3	Toegangs-, informatie- en auditrechten	• De FI neemt voor uitbesteding van 'Kritieke of belangrijke functies' in de uitbestedingsovereenkomst voorwaarden over toegangs-, informatie- en auditrechten op.	13 13 13.3 13.3	75n 75o 86 94	-	-	27 28 33	
		• De FI ziet er op toe dat uitbesteding geen belemmering vormt voor de effectieve uitoefening van toegangs-, informatie- en auditrecht van de FI en haar toezichthouder(s).	13 13.1	75p 79b	10 11	37 m 38	29 16	
		• De FI mag gebruik maken van de door de dienstverlener versterkte externe certificeringen en (externe of interne) auditverslagen. De FI moet beoordelen of	13 14	75h 100	10	37h	22	

			EBA		EIOPA		Microsoft	
5.4	**Uitbestedings-overeenkomst**	**Conceptueel (cloud)uitbestedingsmodel (gebaseerd op bijlage 4, paragraaf 5.4)**	**Richt-snoer**	**Art.**	**Richt-snoer**	**Art.**	**Mapping**	**Match**
		deze certificeringen of auditverslagen voldoende zijn om aan regelgevingsverplichtingen te voldoen. Idem voor de reikwijdte en uitvoering van de audit volgens gepaste normen. Bovendien mag de FI niet uitsluitend vertrouwen op deze certificeringen en auditverslagen.	14	104				
		• De FI moet het recht hebben om naar redelijkheid de reikwijdte van de certificeringen of auditrapportages uit te breiden.	13.3	85	-	-	30	
		• De FI moet het recht behouden om naar eigen inzicht audits op locatie uit te voeren. Aangezien cloudoplossingen technisch bijzonder complex zijn, moet de FI er voor zorgdragen dat de door haar aangestelde auditors over de juiste vaardigheden beschikken. Indien de uitoefening van het toegangs- of auditrecht een risico oplevert voor de omgeving van de aanbieder van clouddiensten en/of andere klanten van de aanbieder van clouddiensten, dan moeten de FI en aanbieder van clouddiensten een alternatieve manier overeenkomen om een vergelijkbaar niveau van betrouwbaarheid en dienstverlening te verwezenlijken (bijvoorbeeld een verslag of specifieke certificering).	13.3 13.3	87 89	- 11	- 38	31 32	
		• Volledige toegang verleent tot alle relevante bedrijfslocaties inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestede functie te verrichten, waaronder bijbehorende financiële informatie, personeel en de externe auditors van de dienstverlener (“toegangs- en informatierechten”); en						
		• Een onbeperkt recht van inspectie en audits verleent met betrekking tot de uitbestedingsovereenkomst (“auditrechten”) om hen in staat te stellen de uitbestedingsovereenkomst te bewaken en er voor te zorgen dat aan alle toepasselijke wet- en regelgeving en contractuele voorschriften wordt voldaan.						
5.4.4	Onder-uitbesteding	• De FI neemt in de uitbestedingsovereenkomst op onder welke voorwaarden onderuitbesteding is toegestaan (of niet). In bijlage 3, bij paragraaf 5.4.4, is een overzicht met voorwaarden met betrekking tot onderuitbesteding opgenomen.	13	75e 76	10	37e	7	
		• Alle soorten activiteiten die van onderuitbesteding zijn uitgesloten;	13.1	78a	13	50a	8	
		• De voorwaarden waaraan moet worden voldaan bij onderuitbesteding (bijvoorbeeld dat de onderuitbestedingspartij de relevante verplichtingen van de dienstverlener	13.1	78b	13	50b	9	

			EBA		EIOPA		Microsoft	
5.4	**Uitbestedings-overeenkomst**	**Conceptueel (cloud)uitbestedingsmodel (gebaseerd op bijlage 4, paragraaf 5.4)**	**Richt-snoer**	**Art.**	**Richt-snoer**	**Art.**	**Mapping**	**Match**
		ook volledig moet naleven, zoals: toegangs-, informatie- en auditrechten, voldoen aan wet- en regelgeving en de beveiliging van gegevens en systemen);						
		• De dienstverlener blijft volledig aansprakelijk en de onderuitbestede diensten moet monitoren en controleren;	13.1	78c 80	13	50c	10	
		• De dienstverlener moet de financiële instelling tijdig in kennis stellen van de voorgenomen belangrijke wijziging van onderuitbesteding die ertoe zouden kunnen leiden dat de dienstverlener minder goed in staat is de verplichtingen uit hoofde van de uitbestedingsovereenkomst na te komen.	13.1 13.1	78d 78e	- 13	- 50d	11 12	
		• De financiële instelling moet het recht hebben om bewaar te maken tegen de voorgenomen belangrijke wijziging van onderuitbesteding als dit nadelig is voor het risicoprofiel van de financiële instelling en/of de overeenkomst te beëindigen.	13.1	78f 7g	13	50e	13 14	
5.4.5	Beëindigings-rechten	• De FI neemt in de uitbestedingsovereenkomst op onder welke voorwaarden de uitbestedingsovereenkomst moet worden beëindigd. In bijlage 3, bij paragraaf 5.4.5, is een overzicht met voorwaarden waarbij de uitbestedingsovereenkomst moet worden beëindigd opgenomen.	13	75q	15	55	34	
		• De dienstverlener overtreed geldende wet- en regelgeving of contractuele bepalingen;	13.4	98a	-	-	35	
		• De dienstverlener voert materiële wijzigingen door die gevolgen hebben voor de uitvoering van de uitbestedingsovereenkomst (bijv. onderuitbesteding of wijziging in onderuitbestedingspartijen)	13.1 13.4 13.4	78g 98b 98c	13	50e	37 36	
		• De dienstverlener treft onvoldoende maatregelen met betrekking tot het beheer en beveiliging van vertrouwelijke, persoonlijke of anderszins gevoelige gegevens of informatie waardoor zwakke punten ontstaan.	13.4	98d	-	-	38	
		• De toezichthouder geeft instructies aan de financiële instelling (bijvoorbeeld doordat de toezichthouder niet in staat is om haar taken effectief uit te voeren).	13.4	98e	-	-	39	

Bijlage 6 – Voorbereiding & vragen interviews

Algemene vragen	
#	**Vragen:**
1	Gaat u akkoord met het opnemen van dit gesprek in Teams? Na het succesvol afronden van de scriptie zal de opname worden verwijderd.
2	Geeft u de antwoorden op persoonlijke titel?
2	Wat is u naam?
3	Wat is uw leeftijd?
4	Welke opleidingen heeft u gevolgd?
5	Hoeveel jaar werkervaring heeft u en in welke sectoren?
6	Wat is uw huidige functie bij uw organisatie?
7	Wat is uw werkrelatie met pensioenfonds A? (intern / extern)
8	Kunt u kort toelichten wat uw rol is in relatie tot de werkrelatie met pensioenfonds A?

Specifieke vragen		
#	**Onderwerp:**	**Vragen:**
1	**Clouddiensten algemeen**	▪ Wat is uw visie op het gebruik maken van clouddiensten door NL-financiële instellingen? (heden & over 5-10 jaar) Is dit verschillend voor banken, verzekeraars en/of pensioenfondsen?
2		▪ Ziet u cloudcomputing als een kans of een bedreiging? Of allebei?
3		▪ Kunt u een drietal voordelen van cloudcomputing benoemen?
4	**Cloud risico (-beheersing)**	▪ Kunt u een drietal risico's noemen van cloudcomputing?
5		▪ Bent u bekent met de DNB template risico analyse uitbesteding?
6		▪ Denkt u ook dat het een goed idee is om het DNB template risico analyse uitbesteding op te nemen in het Beleid Uitbesteding van pensioenfonds A?
7	**Wijzigingen door aanbieder clouddiensten**	▪ Ziet u het als een risico dat aanbieders van clouddiensten eenzijdige wijzigingsbedingen opnemen in de overeenkomst en leverings-voorwaarden? - Zo nee, waarom niet? - Zo ja, welke maatregelen zou een financiële instelling kunnen treffen?
8	**Wijzigingen door financiële instelling**	▪ Ziet u het als risico dat een financiële instelling geen wijzigingen kan aanbrengen in de wijze waarop de uitvoering van de werkzaamheden door de dienstverlener geschiedt? - Zo nee, waarom niet? - Zo ja, welke maatregelen zou een financiële instelling kunnen treffen?
9	**Countervailing power**	▪ Kunt u beknopt verwoorden of countervailing power bij reguliere uitbesteding en bij het gebruik van clouddiensten verschilt? - Wat is de belangrijkste reden voor dit verschil? - Welke maatregelen zou een financiële instelling kunnen treffen?
10	**Keten-management**	▪ Kunt u beknopt verwoorden hoe u zicht houdt (of kunt houden) op de keten van uitbesteding? Denk hierbij aan uitbesteding en onderuitbesteding (naar de cloud).
11		▪ Een vereiste voor een pensioenfonds is dat zij zicht houdt op de keten van uitbesteding (maar niet hoe?). Zou het een praktische werkwijze kunnen zijn om ook voor pensioenfonds A een uitbestedingsregister bij te houden op basis van eisen voor banken en verzekeraars?

Specifieke vragen		
#	**Onderwerp:**	**Vragen:**
12		▪ Kunt u beknopt in uw eigen woorden formuleren wat er verandert in de beheersing van uitbesteding als een uitbestedingspartij gaat onder uitbesteden (naar de cloud)?
13	**Vernietiging data in de cloud**	▪ Ziet u het als een risico dat geen absolute zekerheid kan worden verkregen dat data is vernietigd na het geven tot een opdracht hiertoe? - Zo nee, waarom niet? - Zo ja, welke maatregelen zou een financiële instelling kunnen treffen?
14	**Business Continuity**	▪ Ziet u het als een risico dat pensioenfonds A niet beschikt over een formeel BCM-beleid? Wel zijn verschillende business continuity maatregelen aanwezig. De uitbestedingspartijen hebben dit beleid wel. - Zo ja, hoe zou dit risico zich kunnen effectueren?
15	**Wet- en regelgeving**	▪ Bent u bekent met wet- en regelgeving voor (cloud) uitbesteding voor financiële instellingen? Kunt u deze onderscheiden voor banken, verzekeraars en pensioenfondsen?
16		▪ Bent u bekent met verwachtingen van toezichthouders m.b.t. het gebruik van clouddiensten door NL-financiële instellingen? Zo ja, kunt u deze beknopt toelichten.
17		▪ Voor NL-financiële instellingen is geen uniform kader aanwezig voor het gebruik van clouddiensten. Wat vindt u hiervan?
18		▪ Bent u bekent met datawetgeving met extraterritoriale werking? - Hoe groot acht u het risico dat buitenlandse veiligheidsdiensten informatie van Nederlanders zullen opvragen bij aanbieders van clouddiensten? - En van klanten van NL-financiële instellingen? - En van deelnemers van pensioenfonds A? - Welke maatregelen zou een financiële instelling kunnen treffen?
19		▪ Kunt u voorbeelden noemen van toekomstige wet- en regelgeving voor de beheersing van (cloud)uitbesteding? Bijv. DORA.
20	**Afronding**	▪ Zijn er nog vragen n.a.v. dit interview?
21		▪ Is het mogelijk om u achteraf te benaderen voor aanvullende vragen?

Bijlage 7 – Samenvatting antwoorden interviews

In deze bijlage zijn de antwoorden op de interviewvragen samengevat per aandachtsgebied.

#	Aandachtgebieden interview vragen	Belangrijkste uitkomsten (samengevat)
1	Clouddiensten algemeen	De interviews zijn gestart met een vraag over de visie. De vijf geïnterviewden (hierna: 'zij') zien clouddiensten als een logische ontwikkeling / keuze, iets dat gebeurt en daarmee een organisatie kunnen helpen in het efficiënt inrichten, de nieuwe wereld, veel bedrijven zullen de komende jaren de stap naar de cloud maken en de cloud is onontkoombaar. Zij zien clouddiensten (overwegend) als kans. "Alles heeft voor- en nadelen dat geldt natuurlijk ook voor cloudcomputing". De risico's moet je wel beheersen. De meest genoemde voordelen van clouddiensten zijn: veiligheid / informatiebeveiliging, beschikbaarheid/stabiliteit, schaalbaarheid en kosten/pay-per-use.
2	Cloudrisico(-beheersing)	Alle vijf de geïnterviewden zijn bekend met de DNB template RSA uitbesteding. Zij kunnen zich vinden in het voorstel om dit template op te nemen in het nieuwe Beleid Uitbesteding van pensioenfonds A. Nadrukkelijk wordt opgemerkt om deze wel risk-based toe te passen in combinatie met dat de organisatie wel moet blijven nadenken over andere risico's. Qua risico's van clouddiensten benoemen zij het vaakst: data grensoverschrijdend, privacy & veiligheidsdiensten, vendor lock-in & exit, geen invloed op keuzes & arrogantie van de macht.
3	Wijzigingen door aanbieder clouddiensten of financiële instelling	Alle vijf de geïnterviewden zien het als een risico dat een aanbieder van clouddiensten eenzijdig wijzigingen kan maken in de overeenkomst en leveringsvoorwaarden. Een van hen merkt op dat hierbij wel een onderscheid tussen kleine en grote wijzigingen mag worden gemaakt, omdat het niet reëel is om alle klanten te raadplegen bij kleine wijzigingen. Het niet kunnen aanpassen van wijzigingen in de standaardovereenkomst door de financiële instelling wordt als risico gezien. Als maatregelen worden genoemd: • Verenigen met andere organisatie en/of lobby via NL-overheid of EU. • Volgen van informatieverstrekking door de aanbieder van clouddiensten en van kritische partijen zoals 'Follow The Money' • Alternatief scenario achter de hand houden.
4	Countervailing power	De vijf geïnterviewden merken op dat countervailing power bij reguliere uitbesteding of het gebruik van clouddiensten samengevat in theorie vergelijkbaar is, maar dat het in de praktijk verschillen aanwezig zijn door bijvoorbeeld de marktdominantie van de drie grote aanbieders van clouddiensten, omvang (waarde) van de afgenomen clouddiensten en (te) beperkte kennis over clouddiensten. Een geïnterviewde merkt op dat uitbesteding altijd kennis vergt en dat een organisatie deze moet organiseren, waardoor het gebruik van clouddiensten in feite niet afwijkt van een reguliere uitbesteding. Twee andere geïnterviewde merken op dat bij kleinere IT-uitbestedingen of Europese IT-uitbesteding de financiële instelling meer macht kan behouden. De consequentie hiervan is dat de financiële instelling minder veeleisend moet zijn ten aanzien van bijvoorbeeld: uptime, connectiviteit en kosten. Een kanttekening hierbij is dat vaak wel lijntjes naar de drie grote aanbieders van clouddiensten lopen, merkt een van deze twee geïnterviewden op.

#	Aandachtgebieden interview vragen	Belangrijkste uitkomsten (samengevat)
5	Ketenmanagement	De vijf geïnterviewden benadrukken het belang contractuele afspraken over onderuitbesteding te maken. Zij kunnen zich vinden in het voorstel om het uitbestedingsregister op te nemen in het nieuwe Beleid Uitbesteding van pensioenfonds A. De inrichting moet dan wel risk based zijn, waarbij de normen voor banken en verzekeraars in beginsel niet leidend zijn. Eén geïnterviewde merkt op dat het niet alleen van belang is om naar de verwerking van (persoons)gegevens te kijken, maar ook naar bijvoorbeeld de leverancier van SMS-authenticatie of connectiviteit; “De keten is zo sterk als de zwakste schakel”. In juridische zin leidt (onder)uitbesteding niet tot een wijziging, mits hierover afspraken zijn gemaakt. Vanuit een interne beheersing perspectief kan het impact hebben op de countervailing power van de financiële instelling en aan de zijde van de uitbestedingspartij leiden tot een “gamechanger” (die leidt tot een reorganisatie) en wijziging in het beheersingsraamwerk van de uitbestedingspartij (die beoordeelt moet worden door de financiële instelling).
6	Vernietiging data in de cloud	De vijf geïnterviewden beschouwen het risico dat geen absolute zekerheid kan worden verkregen van de vernietiging van data in de cloud als een klein risico. Maatregelen die worden genoemd zijn: encryptie, sleutelbeheer, assurance verklaring en contractueel afspreken (bijv. voor de exit). Ook merkt een drietal op dat de aanbieder van clouddiensten geen enkel commercieel belang heeft om de data te bewaren. De ruimte kan immers maar eenmaal worden verkocht.
7	Business continuity	De vijf geïnterviewden beschouwen het risico dat pensioenfonds A geen formeel BCM-beleid heeft als een beperkt of (heel) klein risico. De verwachting is dat processen grotendeels doorlopen bij onderbrekingen, ook zonder beleid. Eenmaal wordt opgemerkt dat de COVID-periode ook goed is verlopen. Alle vijf merken op dat een BCM-beleid wel kan bijdragen aan het preventief formuleren van uitgangspunten. Enerzijds kan je voorbereid zijn op verschillende omstandigheden en anderzijds kan worden getoetst of uitbestedingspartijen hun BCM-beleid in lijn met het pensioenfonds A hebben opgesteld. Vanuit de uitvoerbaarheid wordt opgemerkt om er niet een te lijvig document van te maken.
8	Wet- en regelgeving	De vijf geïnterviewden zijn tezamen bekend met diverse Nederlandse en Europese wet- en regelgeving. Hieronder begrepen de EBA-richtsnoeren, DNB Good practices, Wft, Pw en DORA. Een drietal merkt op dat cloud een vorm van uitbesteding is en dat daarvoor de wet- en regelgeving & toezichthouder verwachtingen gelden. Op het ontbreken van een uniform kader voor het gebruik maken van clouddiensten door financiële instellingen wordt verschillend gereageerd van ‘goed idee’ tot ‘het is wel goed zoals het is’. Redenen hiervoor zijn: niet ieder het wiel uitvinden, ondersteuning bij bewustwording & risicobeoordelingen en partijen zijn niet hetzelfde. Allen zijn bekend met datawetging met extraterritoriale werking, zoals de AVG en Cloud Act. De benoemde risico’s van toegang door buitenlandse veiligheidsdiensten m.b.t. Nederlanders, klanten van financiële instellingen en deelnemers van pensioenfonds A varieert. Zoals: geen verschil, alleen impact vanuit antiterrorisme, geen illusies dat veiligheidsdiensten vanuit het belang van veiligheid ver gaan, en voor een gewone Nederlander of deelnemer van pensioenfonds A is totaal

#	Aandachtgebieden interview vragen	Belangrijkste uitkomsten (samengevat)
		geen interesse. Gegevens van OneDrive of banktransacties kunnen veel interessanter zijn. Als maatregelen tegen buitenlandse veiligheidsdiensten worden genoemd: encryptie, sleutelmanagement en locatie verwerking & opslag persoonsgegevens. De bekendheid met toekomstige wet- en regelgeving voor dit aandachtsgebied is beperkt. Een drietal Europese wet- en regelgeving wordt benoemd: DORA, Digital Services Act en Digital Markets Act.

Bijlage 8 – Template RSA Cloudcomputing

In deze bijlage zijn twee tabellen opgenomen, namelijk:

- Tabel 3 (zie paragraaf 4.2.4) met risico's volgens de DNB Template uitbesteding die is omgezet naar uitbesteding aan aanbieders van clouddiensten.
- Tabel 4 (zie paragraaf 4.2.5) met aanvullende (cloud)risico's geïdentificeerd in dit onderzoek en verrijkt met maatregelen op basis van de interviews.

#	Omschrijving risico
1	**Vendor lock-in:** Dit risico omvat dat niet of niet eenvoudig kan worden overgestapt naar een andere aanbieder van clouddiensten door technische beperkingen, te weinig andere aanbieders van clouddiensten, of geen of onvoldoende ondersteuning van deze aanbieder bij de overstap naar een andere aanbieder van clouddiensten.
2	**Onvoldoende middelen voor managen en monitoren uitbesteding:** Dit risico omvat dat de financiële instelling te weinig kennis en personeel heeft om uit te besteden en de presentaties, interne beheersing en IT-risico's van de aanbieder van clouddiensten te monitoren.
3	**Concentratie:** Dit risico omvat dat de aanbieder van clouddiensten meerdere clouddiensten levert (in de keten van uitbesteding) aan de financiële instelling. De totale impact van een eventuele uitval neemt toe bij iedere volgende uitbesteding aan deze aanbieder.
4	**Aanbieder van clouddiensten staakt activiteiten:** Dit risico omvat dat gegevens, systemen en diensten (direct) niet langer beschikbaar zijn zodra een aanbieder van clouddiensten zijn activiteiten staakt. Bijv. als gevolg van faillissement.
5	**Naleving wet- en regelgeving:** De instelling behoudt de verantwoordelijkheid over de uitbestede activiteiten en dient er zorg voor te dragen dat de aanbieder van clouddiensten (en mogelijk onderaannemers) voldoen aan toepasselijke wet- en regelgeving.
6	**Onvoldoende performance / resultaten:** Dit risico omvat dat de aanbieder van clouddiensten zich niet houdt aan de kwaliteitsnormen en afspraken, terwijl service levels wel worden gehaald. Het gaat hierbij om bijvoorbeeld certificering en assurance rapporten.
7	**Scheiding van omgevingen:** Dit risico omvat dat verstoringen in clouddiensten kunnen leiden tot het (tijdelijk) wegvallen van de scheiding van opslag, geheugen en routing van gedeelde infrastructuur. Eventueel zelfs met impact op de reputatie van de verschillende klanten van de gedeelde infrastructuur.
8	**Gegevenslocatie:** Dit risico omvat de locatie van opslag en doorgifte van gegevens, waarbij mogelijk verschillende (lokale) wetgeving van toepassing is die verschilt van de Nederlandse wetgeving.
9	**Gegevenstoegang:** Dit risico omvat de toegang tot gegevens en dat hiermee op een wettelijk juiste manier wordt omgegaan. Hierbij gaat het om de naleving van de regelgeving, zoals over encryptiestandaarden, beheer van encryptiesleutels, het vierogenbeginsel en authenticatie.
10	**Cyberaanvallen:** Alle risico's die verband houden met cyberaanvallen, zoals DDoS-aanvallen, het onderscheppen of uitlekken van gegevens, social engineering, ongeoorloofde toegang, het ongeoorloofd verkrijgen van rechten en ransomware

#	Risico	Maatregelen o.b.v. interviews & onderzoek
11	**Wijzigingen (1):** De financiële instelling kan (mogelijk) geen wijzigingen aanbrengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt.	▪ Aanbieder van clouddiensten verzoeken[15] om aanpassing te maken; ▪ Volgen kritische partijen zoals 'Follow the Money'; ▪ Verenigen, lobby via NL-overheid of EU; ▪ Alternatief scenario achter de hand houden.
12	**Wijzigingen (2):** De aanbieder van clouddiensten voert eenzijdige wijzigingsbedingen op in de overeenkomst en gestandaardiseerde cloud leveringsvoorwaarden.	▪ Volgen informatieverstrekking aanbieder van clouddiensten; ▪ Volgen kritische partijen zoals 'Follow the Money'; ▪ Verenigen, lobby via NL-overheid of EU; ▪ Alternatief scenario achter de hand houden.
13	**Deskundigheid:** De financiële instelling kan onvoldoende 'countervailing power' / 'tegenwicht' bieden tegen een grote aanbieder van clouddiensten.	▪ Zorgdragen voor voldoende kennis over de uit te besteden activiteiten; ▪ Kiezen voor een andere partij (niet-Big-tech) ▪ Verenigen, lobby via NL-overheid of EU; ▪ Alternatief scenario achter de hand houden.
14	**Ketenmanagement (1):** De financiële instelling heeft onvoldoende zicht op de keten van uitbesteding van kritieke of belangrijke functies.	▪ Contractuele afspraken over onderuitbesteding; ▪ Opstellen en onderhouden uitbestedings-register (incl. alle kritieke of belangrijke functies in de keten van uitbesteding); ▪ (Her)beoordelen wijziging(en) organisatie en beheersingsraamwerk bij uitbesteding in de keten.
15	**Ketenmanagement (2):** De financiële instelling kan onvoldoende haar risico's beheersen en haar verantwoordelijkheid nemen door onderuitbesteding naar een aanbieder van clouddiensten.	
16	**Toegang door buitenlandse overheidsdiensten:** Een aanbieder van clouddiensten kan door wetgeving met een extra-territoriale werking door een buitenlandse overheid worden gedwongen om gegevens te verstrekken. Ook als de gegevens in Europa worden verwerkt en opgeslagen.	▪ Encryptie; ▪ Sleutelmanagement (in eigen beheer of externe locatie (niet bij aanbieder van clouddiensten)); ▪ Locatie opslag en verwerking persoonsgegevens.
17	**Vernietiging data:** De onzekerheid van het verwijderen van data na het geven van een opdracht tot verwijdering van deze data. Een harde schijf kan bijvoorbeeld niet worden vernietigd als deze door meerdere partijen wordt gebruikt.	▪ Contractuele afspraken over data vernietiging bij bijvoorbeeld een exit; ▪ Encryptie; ▪ Sleutelmanagement (in eigen beheer of externe locatie (niet bij aanbieder van clouddiensten)); ▪ Assurance verklaring.

[15] In sub-paragraaf 8.2.2 is beschreven welke contractuele ruimte door Microsoft wordt geboden via de Microsoft Customer Agreement, Financial Services Amendment (november 2019).

Bijlage 9 – Afkortingenlijst

AFM	Autoriteit Financiële Markten
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BCM	Business Continuity Management
Besluit FTK	Besluit financieel toetsingskader pensioenfondsen
Besluit Pw	Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling
Bpr	Besluit prudentiële regels
BW	Burgerlijk Wetboek
DNB	De Nederlandse Bank
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ESFS	European System of Financial Supervision
ESMA	Europese Autoriteit voor effecten en markten
ESRB	European Systemic Risk Board
Financiële instelling	Alle ondernemingen in de financiële sector
Financiële onderneming	Dit is een term die wordt gebruikt in de Wet op het financieel toezicht. Dit heeft onder meer betrekking op banken en verzekeraars.
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
KOB	kritieke of belangrijke operationele functies en activiteiten
NCSC	Nationaal Cyber Security Centrum
PaaS	Platform as a Service
Pw	Pensioenwet
SaaS	Software as a Service
Wft	Wet op het financieel Toezicht
Wvp	Wet verplichte beroepspensioenregeling