

# Risicomanagement voor een meerzijdig platformbedrijf

Een risicomanagementraamwerk ontwerp voor de toekomst



<b>Deelnemer/Student</b>	Janneke Blom
<b>Studentnummer</b>	220954
<b>Datum</b>	22 juni 2022
<b>Status</b>	Masterthesis Risico Management

# Risicomanagement voor een meezijdig platformbedrijf

Een risicomanagementtraamwerk ontwerp voor de toekomst



## Samen vooruit!

<b>Deelnemer/Student</b>	Janneke Blom
<b>Studentnummer</b>	220954
<b>Datum</b>	22 juni 2022
<b>Status</b>	Masterthesis Risico Management
<b>Studie</b>	Master Risico Management
<b>Universiteit</b>	Universiteit Twente Drienerlolaan 5 7522 NB Enschede
<b>Opdrachtgever</b>	Bovemij N.V. Ageeth Bakker (Lid Raad van Bestuur) Takenhofplein 2 6538 SZ Nijmegen
<b>Begeleiders UT</b>	Jeroen Sempel (1 <sup>ste</sup> begeleider) Petra de Weerd-Nederhof (2 <sup>e</sup> begeleider)

## Voorwoord en dankwoord

Meer en meer organisaties worden geconfronteerd met een uitdagender en complexer wordende omgeving waarin zij hun bedrijfsactiviteiten uitvoeren. Om het nog ingewikkelder te maken, werd het tweede decennium van de 21e eeuw gekenmerkt door politieke instabiliteit in vele delen van de wereld en de recente pandemie covid-19 heeft de onzekerheid in de wereld nog verder vergroot. Het is in deze toenemende turbulente omgeving dat organisaties hogere verwachtingen van hun stakeholders moeten waarmaken en tegelijkertijd moeten voldoen aan strengere eisen op het gebied van corporate governance. Dit betekent voor menig bedrijf een ethische en sociale verantwoordelijkheid door het hebben van integere en beheerste bedrijfsvoering.

Het is mij daarom een groot genoegen een risicomanagementraamwerk ontwerp voor een meezijdig platform te introduceren. Terwijl de impact van digitale technologieën met verregaande omvang toeneemt, bevindt het academische veld van meezijdig platformbedrijven versus risicomanagement zich nog in de beginnende fase waar nog weinig boeken over zijn geschreven. Deze thesis vult een leemte door theorieën van bedrijfsmodellering en risicomanagement samen te brengen om zodoende een raamwerk te bieden.

Gezien al deze ontwikkelingen is de relevantie van risicomanagement voor een meezijdig platformbedrijf nog groter. Een succesvol risicomanagement-initiatief vergroot het vermogen van een organisatie om doelstellingen te bereiken, de weerbaarheid en duurzaamheid van het bedrijf te waarborgen, op basis van transparant, ethisch en integer gedrag.

Het vakgebied risicomanagement is in de laatste decennia flink ontwikkelt en in mijn optiek is het vakgebied daarom ook steeds interessanter geworden. Dit en alle masterclasses, seminars, sparring momenten met studiegenoten, collega's en alle andere bijeenkomsten, alsmede de één-op-één gesprekken met mijn management coach (van Bovemij) hebben bijgedragen in de ontwikkeling van deze thesis.

De grootste uitdaging bij het maken van deze thesis is geweest om het materiaal zo op elkaar af te stemmen dat het één geheel werd. Mijn begeleiders hebben mij echter niet alleen begeleid op inhoud en structuur. De thesis leidde namelijk ook tot een worsteling met mijzelf en ik ben daarom dankbaar voor de persoonlijke begeleiding.

## Inhoudsopgave

1	Samenvatting .....	1
2	Inleiding .....	3
2.1	Aanleiding van het onderzoek .....	3
2.2	Bovemij .....	3
2.3	Probleemstelling, afbakening en onderzoeksdoel .....	4
2.4	Relevantie .....	4
2.5	Onderzoeksvragen en structuur .....	5
3	Methodologie .....	6
3.1	Type onderzoek .....	7
3.2	Onderzoeksmodel (Onderzoeksontwerp) .....	7
3.3	Methodische verantwoording .....	10
3.4	Validiteit en betrouwbaarheid van het onderzoek .....	14
4	Literatuuronderzoek .....	15
4.1	Digitale economie en Meerzijdig platformbedrijf .....	16
4.2	Type bedrijf en bedrijfsmodel .....	17
4.3	Risicofactor(en) en Risicoprofiel .....	18
4.4	Typische risicofactoren .....	19
4.5	Risicomanagement en Risicomanagementproces .....	20
4.6	Risicomanagementtraamwerk en het functioneren ervan .....	21
4.7	Samenstelling theoretisch ontwerp .....	23
5	Beschrijving, Analyse en Diagnose Bovemij en praktijkvoorbeelden .....	24
5.1	Externe context – Mobiliteitsbranche .....	24
5.2	Interne context - Meerzijdig platform bedrijf – organisatie .....	26
5.3	Huidig risicomanagement bij Bovemij .....	28
5.4	Equivalente bedrijven .....	30
6	Ontwerp risicomanagementtraamwerk Bovemij .....	32
6.1	Governance en risicomanagementarchitectuur .....	32
6.1.1	Three Lines of Defence .....	33
6.1.2	Risico Comités en communicatielijnen .....	35
6.2	Risicomanagement Strategie en -beleidskaders .....	36
6.3	Risicomanagementproces .....	37
6.4	Risicomanagementprotocollen .....	39
6.5	Principes .....	41
6.6	Functionerend RM – Bovemij Control Framework .....	41
6.7	Validatie van het ontwerp en bruikbaarheid .....	43
7	Conclusie, aanbeveling en discussie .....	45
7.1	Conclusie .....	45
7.2	Aanbevelingen .....	47
8	Reflectie .....	50

9	Literatuurlijst .....	52
10	Figuren en tabellenlijst .....	58
11	Bijlagen .....	60
	Bijlage A. Informatie Bovemij N.V.....	60
	Bijlage B. Aanvullende informatie over de begrippen .....	62
	Bijlage C. Aanvullende verantwoording onderzoek.....	83
	Bijlage D. Resultaten diagnose Bovemij Risicomanagement .....	87
	Bijlage E. Conceptuele ontwerpen .....	101
	Bijlage F. Resultaten Equivalente bedrijven .....	104
	Bijlage G. Gerapporteerde risicofactoren equivalente bedrijven per risicocategorie ...	107
	Bijlage H. Case 1 – Amazon.....	109
	Bijlage I. Case 2 – Alphabet.....	111
	Bijlage J. Case 3 - VNV Global .....	113
	Bijlage K. Case 4 - Newlink Technology .....	115
	Bijlage L. Begrippenlijst.....	117

## 1 Samenvatting

Bovemij N.V. ('Bovemij') bevindt zich in de mobiliteit sector met snel veranderende technologieën en globalisering van de gehele keten. Echter is, Bovemij één van de bedrijven op de wereld met een ernstig verouderde informatietechnologie. Dit in de combinatie met aanzienlijke incidenten waarbij Bovemij niet voldeed aan wet- en regelgeving die bij de toezichthouders zijn gemeld, moest Bovemij onder zeer hoge druk een risicomanagementfunctie en compliance functie inrichten. Momenteel beschikt Bovemij niet over een risicomanagementraamwerk. Op aandringen van de aandeelhouder en toezichthouders is voor de komende vijf jaar door de nieuwe Raad van Bestuur een digitaliserings-/ platformstrategie ontwikkeld, waarbij zij eveneens de door Bovemij zogenoemde 'basis op orde' brengt. Onderdeel van de basis op orde brengen is het hebben van een aantoonbaar functionerend risicomanagementraamwerk.

Het doel van dit onderzoek is het ontwerpen van een risicomanagementraamwerk voor Bovemij als meezijdig platformbedrijf binnen de mobiliteit sector. Waarbij het ontwerp is gebaseerd op basis van kaders uit wetenschappelijk onderzoek. Daarnaast zijn kaders uit literatuuronderzoek gehanteerd voor het planmatig en gestructureerd onderzoek verrichten bij equivalente bedrijven en Bovemij voor praktische aanknopingspunten. Dit onderzoek maakt gebruik van wetenschappelijke literatuuronderzoek, bestudering van beschikbare bedrijfsinformatie en data-analyse. Voor het valideren van concept ontwerpen is met verschillende interne en externe stakeholders gesproken. De onderzoeksmethodieken en -activiteiten leidde tot het beantwoorden van de volgende hoofdvraag opgesteld: *Hoe ziet een functionerend risicomanagementraamwerk eruit voor Bovemij als meezijdig platformaanbieder?*

Het resultaat van dit onderzoek is een ontwerp risicomanagementraamwerk van zeven onderling samenhangende bedrijfs- en risicomanagementcomponenten: 1) Governance, (2) Principes, (3) Architectuur, (4) Strategie en Beleid, (5) Protocollen, (6) Risicomanagementproces en (7) Bovemij Control framework. Dit biedt Bovemij een leidraad en dient als structuur zodat de organisatie risicomanagement en compliance integreert binnen de (bedrijfs)activiteiten en daarmee haar specifieke doelstellingen realiseert. Waarbij het functioneren van het raamwerk met name wordt geborgd door het hebben van het zevende component, zogenoemd het Bovemij Control Framework. Het ontwerp is een door de onderzoeker zelf ontwikkeld raamwerk op basis van kaders uit de literatuur. De kaders voor risicomanagement zijn met name van "Fundamentals of Riskmanagement" van Paul Hopkin (2018), "Risk Management Guide for Information Technology Systems" van Gary Stoneburner (2002), Cobit 5 for Risk (2013) en ISO 31000 (2019). Voor de integratie met de bedrijfscontext zijn met name 'bedrijfsarchitectuur op basis van Novius Architectuur Methode' van Guido Bayens (2015) en "Business Model Generation" van Osterwalder. De concept ontwerpen zijn op verschillende momenten bij verschillende Bovemij

medewerkers getoetst, waaronder de eindgebruikers om het raamwerk zodoende afgestemd te krijgen op de nieuwe bedrijfsinrichting van Bovemij als meezijdig platformbedrijf.

De conclusie is dat het ontwerp risicomanagementraamwerk voor Bovemij op dit moment vooral een belangrijk stuurinstrument gaat zijn om de basis voor risicomanagement op orde te krijgen, structuur aan te brengen en kaders mee te geven aan de organisatie. Ook is het een aangewezen hulpmiddel voor het begrijpen van samenhang en te hanteren terminologiën. Met de grootscheepse transformatie van de organisatie verschaft het risicomanagementraamwerk eveneens beter inzicht en overzicht, zeker op inhoud als het gaat om beperkingen (risico's) van de transformatie.

Voorts heeft Bovemij nog stappen te ondernemen om het risicomanagementraamwerk te implementeren om zodoende ook het functioneren ervan te kunnen aantonen. Het verkrijgen van een zogenoemd 'functionerend' risicomanagementraamwerk vereist nader onderzoek naar de effecten van het in deze thesis opgenomen Bovemij Control Framework. Omwille van het functioneren zijn in deze thesis al wel enkele aanbevelingen aangedragen voor de implementatie en het functioneren van het risicomanagementraamwerk. Voor de implementatie is in eerste instantie training en constructieve communicatie nodig om toe te werken naar een benodigde risicocultuur. Het verkrijgen van deze risicocultuur zal onderdeel moeten zijn van de transformatie om zodoende risicomanagement onderdeel te maken van de platformbedrijf. Omdat risicomanagement onderdeel is voor beheerst transformeren van de organisatie en de digitale wereld rondom Bovemij snel veranderd, is het advies om het risicomanagementraamwerk radicaal te implementeren en pas op lange termijn het raamwerk incrementeel mee te laten veranderen. Doordat het huidige risicomanagementraamwerk met name is gericht op de basis op orde krijgen, geeft de laatste aanbeveling aan om de volgende versie van het raamwerk te baseren op een intelligente en geautomatiseerde bedrijfsprocessen. Dit zal nog wel vervolgonderzoek en analyse behoeven.

## 2 Inleiding

### 2.1 Aanleiding van het onderzoek

Tegenwoordig kenmerkt menig bedrijfsomgeving zich als een complexe omgeving met snel veranderende technologieën en globalisering. Internationaal gezien opereren de grootste en de meest invloedrijke bedrijven in de huidige economie via digitale wegen en middels een platform. Daar waar twee- en meezijdige marktbediening eerder nog uitzonderlijk waren, is dit tegenwoordig niet meer weg te denken. Opkomende en snelle veranderingen in de bedrijfsomgeving zijn voor menig bedrijf dan ook complex. De zogenoemde opkomende digitale transformatie is op dit moment een zogenoemde “Key challenge” voor bedrijven (Brunner & Wolfartsberger, 2020). Desalniettemin zijn de uitdagingen een megatrend die gepaard gaan met zowel risico's als kansen dat vooral naar voren komt bij productie- en procesoptimalisatie, data-gedreven bedrijfsmodellen en nieuwe perspectieven voor de interactie met klanten (Brunner & Wolfartsberger, 2020).

De aanleiding voor het onderwerp *Risicomanagementraamwerk voor een meezijdig platformbedrijf* is ontstaan door het veranderen van de voorgaande strategie naar een digitalisering- en platformstrategie. en de vraag hoe ziet een risicomanagementraamwerk er dan uit voor een platformbedrijf. Doordat tegenwoordig verschillende “best practices” voor risicomanagement raamwerken aanwezig zijn, zal in dit onderzoek vanuit wetenschappelijk perspectief beargumenteerd worden wat de “best practice” voor Bovemij kan zijn. Dit onderzoek is dan ook gebaseerd op een praktijkcase die samen met de opdrachtgever vanuit Bovemij is samengesteld.

### 2.2 Bovemij

De BOVAG werd in 6 mei 1930 binnen de mobiliteit sector opgericht. De leden van de BOVAG, de Bond Van Automobielhandelaren en Garagehouders richtte in 1963 de verzekeraar NV Schadeverzekering-Maatschappij Bovemij (hierna ‘SVM’) opgericht voor het aanbieden van verzekeringen aan bedrijven in de mobiliteit sector met verzekeringsvoorwaarden die specifiek bedoeld waren voor de door Bovemij genoemde niche sector. Inmiddels is de organisatie door aankoop en het zelf opzetten van verschillende bedrijfsentiteiten uitgegroeid tot Bovemij N.V. (hierna ‘Bovemij’). De verzekeraar SVM is nu onderdeel van de groep





Bovemij N.V. naast de andere grote organisatieonderdelen Bovemij Financieringsmaatschappij BV (hierna 'BFM') en RDC Group BV. (hierna 'RDC'<sup>1</sup>). Zie organigram in Bijlage A.

### 2.3 Probleemstelling, afbakening en onderzoeksdoel

Hoewel verschillende literatuur bestaat over het type bedrijf 'meezijdige platformbedrijf en platformen', is weinig literatuur voorhanden over het risicomanagement of risicobeheersing bij een meezijdig platformbedrijf. Terwijl eigenlijk, al het toetreden tot een bepaalde markt/sector een risico kan zijn omdat het potentiële succes afhankelijk is van de beschikbaarheid van producten en/ of diensten die het platform aantrekkelijk moeten maken voor afnemers/ gebruikers (Alt & Zimmermann, 2019; D. P. McIntyre & Srinivasan, 2017; Veisdal, 2020).

Verschillende onderzoekers hebben artikelen gepubliceerd en boeken geschreven waar wordt gesproken over 'de aanwezigheid' van bepaalde type risico's, of uitleg over waarom risicomanagement belangrijk is, of specifieke risico's binnen een bepaald type bedrijfsmodel. Een geconsolideerd en eenduidig risicomanagementtraamwerk specifiek toegepast op een meezijdig platformbedrijf (inclusief verschillende type bedrijfsentiteiten als Bovemij) lijkt als zodanig te ontbreken. Het onderzoek in deze thesis is daarom een aanzet naar een ontwerp, waarbij sprake van een theoretisch en praktische probleem.

Op dit moment beschikt Bovemij niet over een risicomanagementtraamwerk. Dit onderzoek heeft daarom tot doel om een risicomanagementtraamwerk te ontwerpen voor Bovemij als meezijdig platformbedrijf op basis van kaders uit wetenschappelijk onderzoek, aangevuld met de praktijk vanuit equivalente bedrijven. Om te komen tot een risicomanagementtraamwerk dat past bij het specifieke bedrijfsmodel is onderzoek nodig naar het bedrijfsmodel en naar de verwachte risico's die er op bedrijfsniveau aan verbonden zijn (Halman et al., 2003). Het doel in het onderzoek is te onderzoeken 'hoe', 'waarom' en onder 'welke randvoorwaarden' een meezijdig platformbedrijf een risicomanagementtraamwerk kan inrichten.

### 2.4 Relevantie

Bij ontwerpwetenschap gaat het daarom dat generieke wetenschappelijke kennis wordt opgedaan ter ondersteuning aan het ontwerpen van specifieke oplossingen voor het veldprobleem (Verdonschot & Kessels, 2011). Anders dan wetenschap waarbij belangeloos wordt geobserveerd en begrepen van het bestaande, zorgt ontwerpgericht wetenschap middels een creatief proces voor oplossingen (en de wijzen

---

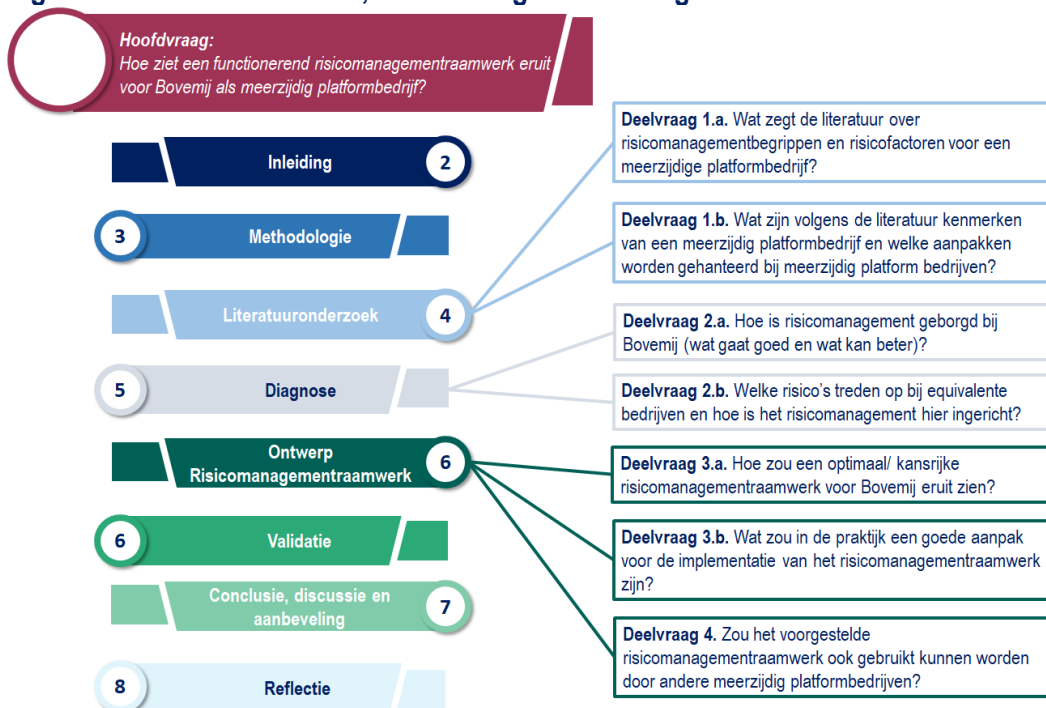
<sup>1</sup> Gedurende het onderzoek is de interne naam van RDC veranderd naar 'Data & Analytics'. De juridische naam is richting klanten en toezichthouder nog onveranderd gebleven.

van invoeren) door de oplossing zelf te ontwerpen (Verdonschot & Kessels, 2011). Dit onderzoek is wetenschappelijk relevant omdat het onderzoek een theoretische bijdraagt in de combinatie bestaande wetenschap en een praktische bijdrage levert aan de toekomstige bedrijfsvoering van Bovemij. Ook levert het onderzoek een bijdrage aan de theorievorming in het vakgebied van risicomanagement voor een meezijdig platformbedrijf. Een raamwerk voor risicomanagement is praktisch relevant omdat dit de Raad van Bestuur, directie en het management van de organisatie handvatten en overzicht biedt, en inzicht in het belang van de verschillende risicomanagementaspecten (inclusief de samenhang).

## 2.5 Onderzoeksvragen en structuur

Voor het ontwerpen van een risicomanagementraamwerk voor een meezijdig platformbedrijf zal het beantwoorden van de hoofdvraag een oplossing moeten bieden voor de probleemstelling van Bovemij. Onderstaand **Fout! Verwijzingsbron niet gevonden.** bevat de hoofdvraag, deelvragen en de hoofdstukken van deze thesis waarbinnen de antwoorden op de deelvragen zijn geformuleerd.

**Figuur 2-1 Structuur thesis, hoofdvraag en deelvragen**



De probleemstelling en hoofdvraag bevatten kernbegrippen die worden verkend en onderzocht behulp van literatuuronderzoek voor begripsbepaling. Binnen hoofdstuk vier worden de uitkomsten uit het literatuuronderzoek geresumeerd beschreven en zullen deelvragen 1a en 1b worden beantwoord. Ook levert het literatuuronderzoek de theoretische kaders voor het onderzoek bij Bovemij en de equivalente

bedrijven, een theoretisch samengesteld risicomanagementraamwerk en de vanuit wetenschappelijke literatuur aangedragen risico's behorende bij een meezijdig platformbedrijf.

De kernbegrippen en het theoretische kader uit het literatuuronderzoek zijn binnen hoofdstuk vijf toegepast voor de diagnose bij Bovemij en aangevuld met de informatie vanuit equivalente bedrijven. Zodoende worden deelvragen 2a en 2b beantwoord. Voor de diagnose bij Bovemij worden gesprekken met leden van de Raad van Bestuur, directie, discussies en brainstormsessies met 1<sup>ste</sup> lijn risicomangers, externe adviseurs, strategische beleidsplannen en rapportages vanuit toezichhouders gebruikt. Hiermee wordt de context voor het risicomanagementraamwerk geïdentificeerd en wat het dient te bereiken. Voor de diagnose van equivalente bedrijven belicht dit hoofdstuk overeenkomsten qua risicoprofiel tussen de bedrijven en Bovemij. Daarbij zet het onderzoek de door deze bedrijven toegepaste methodieken, modellen, "best practices" en dergelijke raamwerken voor risicomanagement uiteen indien dit is beschreven in hun jaarverslagen.

Als gevolg van hoofdstuk vijf bevat hoofdstuk zes het ontwerp risicomanagementraamwerk voor Bovemij. Het ontwerp beantwoordt deelvraag 3a en bij ieder component van het raamwerk zal deelvraag 3b zijn beantwoord om duidelijk te krijgen onder welke voorwaarden het raamwerk kan slagen. Ongeacht dat het raamwerk door de onderzoeker wordt ontwikkeld, worden tussentijdse deelproducten gevalideerd bij de verschillende stakeholders van Bovemij. Zodoende wordt het ontwerp tussentijds gevalideerd.

De thesis sluit af met hoofdstuk 7, waarin conclusies zijn getrokken en bediscussieerd in de beantwoording van de hoofdvraag. Vanwege het ontwerp vraagstuk bevat dit hoofdstuk ook aanbevelingen richting Bovemij. Als afsluiting bevatten de bijlagen aanvullende informatie behorende bij de informatie in de eerdere hoofdstukken.

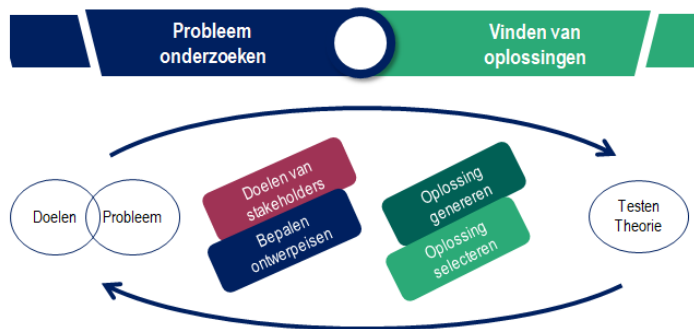
### **3 Methodologie**

Om een risicomanagementraamwerk voor Bovemij te ontwerpen dat in "real life" gebruikt kan worden en op basis van wetenschappelijk onderzoek is, is voor een onderzoeksmethode gekozen die de wetenschap en praktijk combineert. Dit hoofdstuk beschrijft de wijze waarop een risicomanagementraamwerk als oplossing is ontwikkeld vanuit het probleem en doel.

### 3.1 Type onderzoek

Voor dit onderzoek is gekozen voor het uitvoeren van een combinatie (abductief) onderzoek, waarbij wetenschappelijke theoretisch onderzoek wordt verricht in combinatie met praktijkgericht onderzoek. De literatuur maakt hierin onderscheid tussen theoretisch onderzoek (theorie ontwikkelen of toetsen) en praktijkgericht onderzoek (waaronder diagnosticeren van een complex probleem en ontwerpen van een oplossing) (Smit, 2018; Verschuren & Doorewaard, 2016). Voor zowel het theoretische als praktijkgerichte deel van het onderzoek is gekozen voor een verklarend en verkennend onderzoeksopzet.

**Figuur 3-1** De cyclus van ontwerpgericht onderzoek<sup>2</sup>



Het probleem binnen dit onderzoek betreft een zogenaamd complex managementvraagstuk. Smit, (2018) geeft hiervoor aan dat een zogenaemde ontwerpstrategie “Design thinking” toegepast kan worden. De ontwerpstrategie heeft een kort-cyclische karakter, weergegeven in **Fout! Verwijzingsbron niet gevonden.**, dat idealiter zorgt dat met het ontwikkelen van de oplossing rekening is gehouden met de randvoorwaarden van stakeholders en voorwaarden gericht op het laten slagen van het ontwerp. Dit is volgens Brown, T (2009), geciteerd uit Smit, (2018), een discipline die gebruik maakt van de sensitiviteit en methoden van de ontwerper om de behoeften van de mensen af te stemmen op wat enerzijds technologisch haalbaar is en anderzijds wat een levensvatbare strategie kan omzetten in waardecreatie en kansen.

### 3.2 Onderzoeksmodel (Onderzoeksonwerp)

Het onderzoek bestaat uit zes fases. In de eerste fase voorafgaand aan het onderzoek wordt inzicht verkregen in het probleem en definiëren ervan voor Bovemij als stakeholder van het onderzoek. Binnen deze fase is geleerd wat globaal het probleem is van Bovemij en waarom het risicomanagementraamwerk als oplossing nodig is.

<sup>2</sup> Overgenomen uit Complexe problemen oplossen: design thinking of ontwerpgericht onderzoek, Smit (2018), p20.

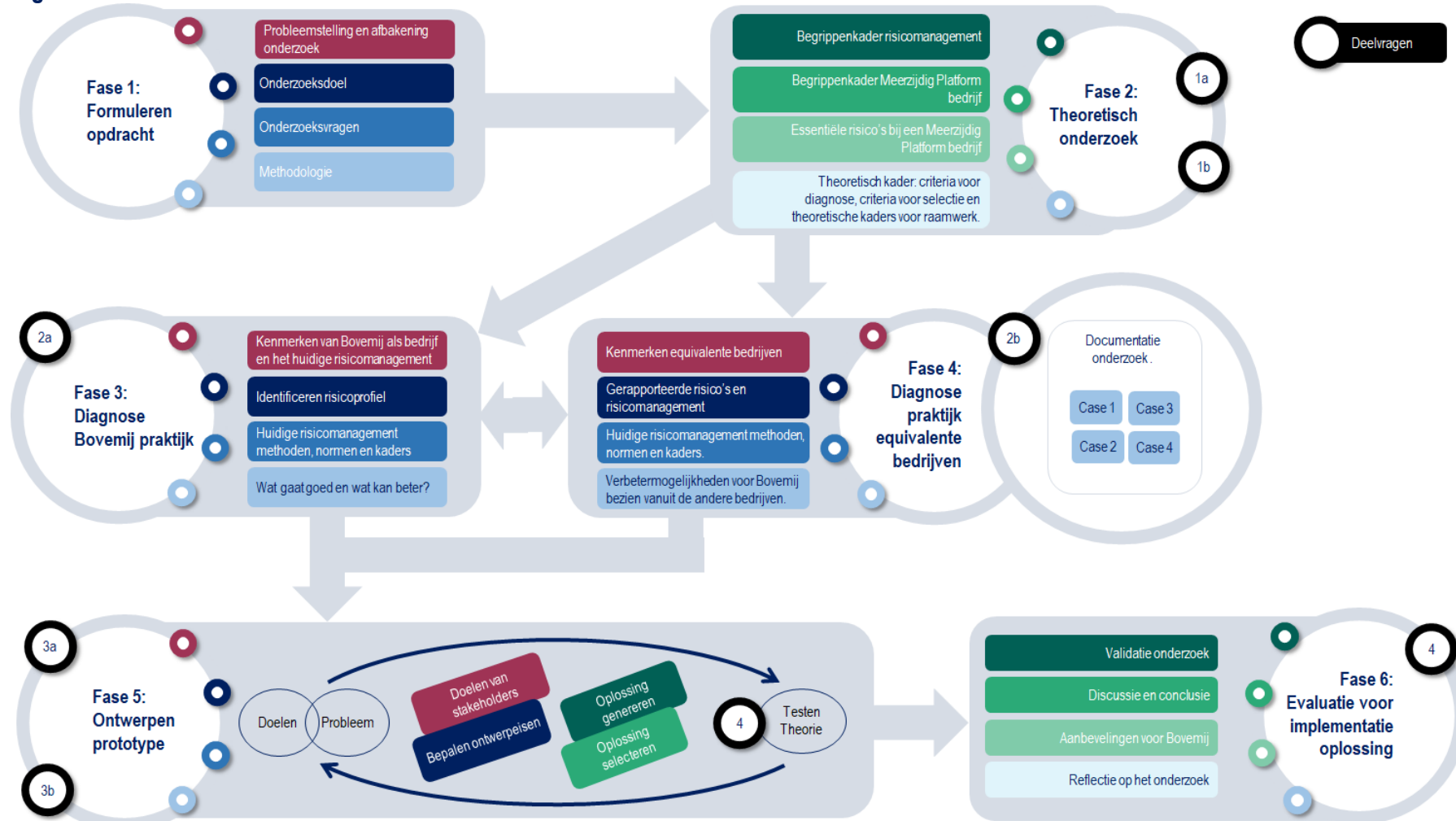
De tweede fase van het onderzoek bevat de bestudering van begrippen binnen het wetenschappelijke domein en het opdoen van (nieuwe) inzichten. Dit leidt tot een aantal verschillende theoretische begrippen en tot een theoretisch onderzoekskader voor fase drie en fase vier. In deze fase wordt op basis van literatuur ook het theoretisch ontwerp opgesteld. Waarbij deelontwerpen bij de stakeholders van het onderzoek worden voorgelegd. Het doel hiervan is te zorgen dat alvast feedback op de oplossingsrichting (prototype) kan worden verkregen van stakeholders en het prototype door ontwikkeld kan worden.

De begrippen en het theoretische kader worden vervolgens in het praktijkdomein gebruikt voor het uitvoeren van de diagnose bij Bovemij voor fase drie. Ditzelfde wordt aangevuld met de criteria voor caseselectie voor het uitvoeren van de diagnose bij equivalente bedrijven. Naast de standaard kaders voor onderzoek, laat de diagnose zich leiden door datgene wat belangrijk is om over de onderzoekseenheden te weten te komen (Verschuren & Doorewaard, 2016) en wat per toeval wordt gezien. De analyse van de overeenkomsten tussen Bovemij en de cases in combinatie met de theorie, de theoretisch gevalideerde kaders dienen te leiden tot het inhoudelijke ontwerp van het risicomanagementraamwerk.

Binnen fase vijf is de cyclus van ontwerpgericht onderzoek toegepast. Binnen deze cyclus wordt op basis van gesprekken en discussie met stakeholders de eisen aan de oplossing nader gedefinieerd en worden er nieuwe en of alternatieve oplossingsrichtingen ontwikkeld. Ook in deze fase worden de oplossingsrichtingen tussentijds gevalideerd (getest) bij de verschillende stakeholders, totdat er een ontwerp is ontwikkeld dat voldoet aan het gespecificeerde doel van het ontwerp (Brown, 2009 geciteerd in Smit, (2018)).

Op de volgende pagina is het onderzoekmodel visueel weergegeven (**Fout! Verwijzingsbron niet gevonden.**) inclusief de onderzoeksvragen die per fase worden beantwoord.

**Figuur 3-2 Onderzoeksmodel**



### 3.3 Methodische verantwoording

#### Gebruikte literatuur

Omwille van drie redenen is een literatuuronderzoek uitgevoerd. De eerste reden voor literatuuronderzoek is het plaatsen van het onderzoek in een wetenschappelijk perspectief. De tweede reden is het vermijden van duplicatie en replicatie van onderzoek. De derde reden is pragmatischer. Gebruik maken van al eerder verricht onderzoek.

Het literatuuronderzoek bestreek meer dan 80 bronnen, bestaande uit boeken en wetenschappelijke publicaties teruggaand tot en enkele bron uit het jaar 2003 en het merendeel uit de jaren vanaf 2016. Geraadpleegde bronnen zijn onder meer: Google-scholar, FindUT, SpringerLink en ScienceDirect. Er is gezocht met de volgende sleuteltermen (in Nederlands en Engels): “meerzijdig platformbedrijf/ aanbieder” “platformeconomie”, “platform(en)”, “digitale economy”, “type platformen” en “digital platforms”. Deze termen zijn gecombineerd gezocht in combinatie met “risicomanagement”, “risico/ risicofactoren”, “risicomanagementraamwerk” en “risicomanagementproces”. Deze laatste termen zijn ook op individuele basis onderzocht voor het begrippenkader risicomanagement. Onderstaande tabel bevat de meest gebruikte literatuur (geen eindige lijst<sup>3</sup>) voor het kwalitatief onderzoek.

**Tabel 3-1 Meest gebruikte bronnen voor (kern)begrippen**

Functionerend risicomanagement raamwerk	Digitaal Meerzijdige Platform Aanbieder
NEN-ISO 31000+C11 (NEN, 2009)	Multi-sided Platforms: Current State And Future Research (Yablonsky, 2019)
Handboek Risicomanagement ERM-plus: een praktische toepassing van COSO ERM (Claassen, 2009)	Virtual Reality enriched Business Model Canvas Building Blocks for enhancing Customer Retention (Brunner & Wolfartsberger, 2020)
Enterprise Risk Management Integrating with Strategy and Performance Executive Summary (COSO, 2017)	The architecture of platforms a unified view (Baldwin & Woodard, 2009)
Cobit 5 for risk (ISACA, 2013)	Multi-sided platforms (Abdelkafi et al., 2019)
Fundamentals of Risk Management 5 <sup>th</sup> edition (Hopkin, 2018)	Multi-sided platform diffusion in competitive B2B networks: inhibiting factors and their impact on network effects. (Wallbach et al., 2019)

Meerzijdige platformaanbieders hebben de laatste jaren veel aandacht gekregen in het wetenschappelijk onderzoek. Zoals door McIntyre et al. in 2018 beschreven is de invloed van meerzijdige

<sup>3</sup> De totale lijst van gebruikte literatuur is opgenomen in de literatuurlijst.



platformaanbieders in de afgelopen jaren steeds relevanter geworden in een breed scala van industrieën. Ondanks de theoretische vooruitgang in de wetenschap, blijkt uit de onderzoeken van McIntyre et al. (2018) en Eisape (2019) dat er nog verschillende kernvragen blijven bestaan over de bedrijfsmodellen van de meezijdige platformaanbieders. In deze scriptie is het onderzoeken en ontwikkelen van een bewezen bedrijfsmodel voor een meezijdig platformaanbieder geen onderdeel van de onderzoeksdoelstelling en scope. In verschillende literatuur wordt echter benadrukt dat een business model aanpak voor het onderzoeken, begrijpen en beschrijven van een bepaalde organisatie een nuttig analytisch kader biedt. Zodoende zijn de boeken *Business Model Generation* (A Osterwalder & Pigneur, 2019) en *Bedrijfsarchitectuur op basis van Novius Architectuur Methode* (Bayens & Tönissen, 2015) gebruikt voor twee doeleinden. Het eerste doel om het systematisch en gestructureerd onderzoek uit te kunnen voeren. Ten derde zijn de boeken gebruikt voor het opstellen van de kaders (**Fout! Verwijzingsbron niet gevonden.**) waar risicomanagement onderdeel van hoort te zijn. Voor de begripsvorming zijn verschillende bestaande literaire bronnen gebruikt en vergeleken. Van overeenkomende kenmerken binnen verschillende omschrijvingen is samenvattend een begrip uitgewerkt. Hierbij zijn zoveel mogelijk raakvlakken gezocht met de context van Bovemij.

Ten tijde van deze thesis was er nog geen specifieke literatuur over een risicomanagementraamwerk voor het typologie meezijdig platformbedrijf. Verschillende risico's bevonden zich verschillende in verschillende artikelen en werd op de detail ingezoomd, waaronder "supply chain riskmanagement strategies", "The platform businessmodel and business ecosystem: quality management and revenue structures", en "Electronic Markets on platform competition". Dit laatste artikel bevat geen enkele keer het woord risico en beschrijft dit als "issues" en "barriers". Dit bemoeilijkte de poging om risicomanagement en of een risicomanagementraamwerk systematisch te meten en analyseren. Om toch te komen tot een oplossing voor Bovemij, werd voor deze thesis eerst een literatuuronderzoek verricht in fase twee.

### **Diagnose Bovemij en equivalente bedrijven**

De casestudie is het meest geschikt bevonden omdat er geen gevonden theoretisch casussen zijn voor een deductieve studie (Eisenhardt 1989, geciteerd in Veisdal, 2020; Yin, 2009) in de combinatie van de constructen risicomanagement en meezijdig platformbedrijf. De case studie is ingezet voor het beantwoorden van de onderzoeksvragen die betrekking hebben op 'hoe vragen' (Eisenhardt 1989, geciteerd in Veisdal, 2020, Alt & Zimmermann, 2019). Bij een case studie is het bedrijf in de omgeving onderzocht en door onderzoek naar meerdere cases zijn de resultaten als robuuster beoordeeld dan bij een enkele case studie (Halman et al., 2003). Yin (2009) stelt wel dat de case studies van begin af aan

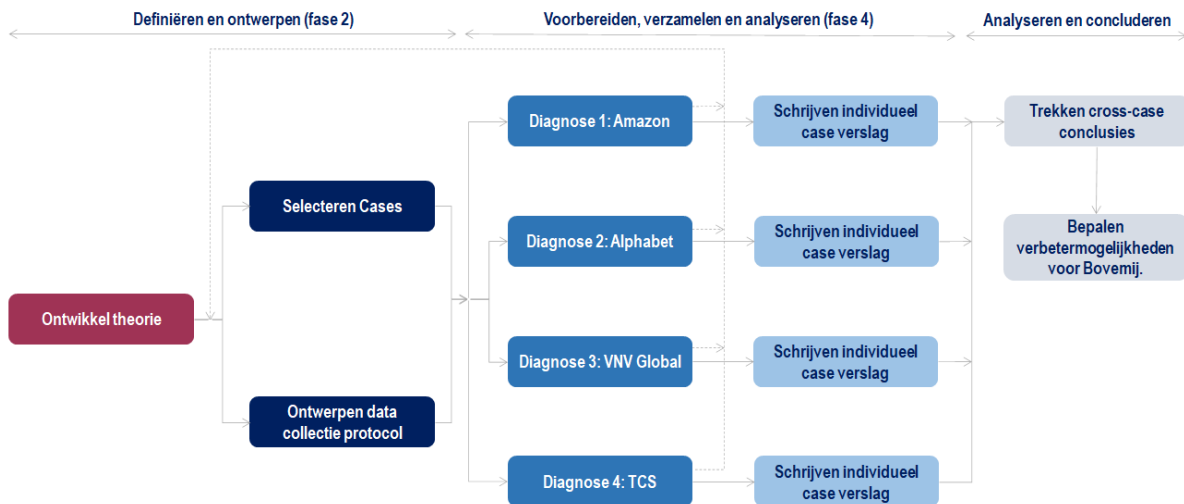


een theoretisch kader nodig hebben omdat het anders de onderzoeksvragen, de analyse en de interpretatie van de bevindingen zou beïnvloeden.

De primaire bron voor het verzamelen van gegevens over Bovemij is de organisatie, waarbij bedrijfs- en beleidsinformatie van Bovemij is bestudeerd. Hierbij is gebruik gemaakt van beleidsdocumenten, presentatiemateriaal van de Raad van Bestuur (RvB) over de nieuwe strategie, rapporten van toezichthouders, verschillende rapportages van externe adviseur KPMG, gesprekken en discussies binnen bestaande risico comités en in periodieke individuele gesprekken met directieleden en RvB.

Het onderzoek naar equivalente bedrijven is in meerdere fasen uitgevoerd (zie **Fout! Verwijzingsbron niet gevonden.**). Zoals Verschuren & Doorewaard, (2016) aanbeveelt zijn de bedrijven in de eerste stap van het onderzoek eerst als afzonderlijke cases bestudeerd. Waarbij een vast patroon is gevolgd. In de tweede stap vormden de individueel bestudeerde cases input voor de vergelijkende analyse waarmee getracht wordt om verklaringen te zoeken voor verschillen en overeenkomsten tussen de diverse cases. De cases zijn geselecteerd voor het kwalitatieve onderzoek vanwege hun relevantie voor het onderzoeksonderwerp en het hebben van een bepaald verband met Bovemij.

Figuur 3-3 Case study methode en proces<sup>4</sup>



<sup>4</sup> De opzet voor het figuur overgenomen uit Boeksectie: How to do better case studies, (Yin, 2009). Voor alle vier de cases is het verslag en een beknopte weergave van de uitkomsten opgenomen in de bijlage.

Om voor het ontwerp van het risicomanagementraamwerk een afspiegeling te hebben met Bovemij, werd platformbedrijf Vostok New Ventures LTD geselecteerd met innovatieve dochterondernemingen binnen de transportsector (waaronder de mobiliteitssector): BlaBlaCar, Voi Technology, GT Gettaxi Limited ("Gett"), SWVL, OneTwoTrip en Monopoliya. Vervolgens is NewLink Technology Inc – gekozen als IT solution provider die zich primair richt op bedrijven met traditionele software voor financiële instellingen en deze willen vervangen voor moderne platformsoftware. Dit bedrijf is vergelijkbaar bedrijf met Tata Consultancy Services (TCS). TCS kon voor dit onderzoek niet worden gebruikt omdat dit de belangrijke strategische alliantie van Bovemij is, waardoor ook geen objectieve dataverzameling kon plaatsvinden. Amazon is gekozen omdat zij een meezijdig platform bedrijf zijn dat zowel via fysieke als online winkel producten verkopen. Dit is vergelijkbaar met het verkopen van de Bovemij producten: auto's en fietsen. Eveneens vergelijkbare kernwaarden met Bovemij. *Customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. In each of the segments, they primary serve customer sets, consisting of consumers, sellers, developers, enterprises and content creators.* Alphabet is vergelijkbaar met Bovemij omwille van de bedrijfsinvesteringen die Bovemij in het verleden heeft gedaan. Alphabet is net als Bovemij een verzameling van verschillende type bedrijven, waarvan Google de grootste is en bij Bovemij is de verzekeraar het grootste.

### Ontwerp risicomanagementraamwerk

Voor het ontwerpen van het risicomanagementraamwerk is in de basis het theoretische raamwerk uit fase 1 gehanteerd en dat is aangevuld met de uitkomsten uit de diagnose in fase 2. Tussentijds en daarna ter validatie zijn met verschillende stakeholders discussies gevoerd over de opzet en de inhoud van de mogelijk oplossing. De volgende stakeholders (geanonimiseerd) hebben bijgedragen het ontwerp:

**Tabel 3-2 Informatie vanuit stakeholders**

Stakeholder	Organisatie	Belang(en) en relevante input voor het onderzoek
Raad van Bestuur (RvB)	Bovemij	Besluitvorming over de te hanteren "best practices" waaronder COBIT, ISO 31000 en ISO 27001. De RvB is eindverantwoordelijk voor de integere en beheerste bedrijfsvoering en daarmee ook verantwoordelijk voor het beschikken over een functionerend risicomanagementraamwerk.
Directieleden	Bovemij	De directieleden hebben voornamelijk input geleverd voor de beschrijving over de huidige inrichting of eigenlijk ontbreken van risicomanagement in de praktijk. De directieleden hebben periodiek performance gesprekken met de RvB over de effectiviteit van risicomanagement binnen hun verantwoordelijkheidsgebied.
1 <sup>ste</sup> lijn en 2 <sup>e</sup> lijn risicomanagers, compliance officer en interne auditfunctie	Bovemij	De zogenoemde 1 <sup>ste</sup> en 2 <sup>e</sup> lijnfunctionarissen (interne risico- en compliance deskundigen) hebben in methodieken, werkwijzen en processen overeenkomsten. Vanuit de organisatie is aangegeven dat een eenduidige werkwijze vanuit deze functionarissen gewenst is.

		Daarom is hen verzocht input te geven bij de ontwikkeling van het risicomanagementraamwerk.
Externe (kleine zelfstandigen) adviseurs van Bovemij	Privé	De zelfstandigen die input hebben gegeven zijn expert met betrekking tot: COBIT-raamwerk, programmamanagement, business procesmanagement, target operating model, informatiebeveiliging, IT-risicomanagement en Administratieve Organisatie en Interne Controle. Zij hebben geen specifiek belang bij het risicomanagementraamwerk.
Externe adviseur	KPMG, EY en PWC	KPMG heeft een risicomanagementvolwassenheidsscan uitgevoerd voor Bovemij. PWC ondersteunt de 2 <sup>e</sup> lijn risicomanagement met rapportages over de kwaliteit van risicomanagement binnen twee primaire (kritische) projecten van Bovemij. EY is de externe accountant en stelt jaarlijks management letter opgesteld waaruit blijkt dat er tekortkomingen zijn binnen de beheerste bedrijfsvoering. Vooral EY heeft er in het kader van de jaarrekening controle belang bij dat Bovemij over een integere en beheerste bedrijfsvoering beschikt.
Toezichthouder	DNB, RDW, AP, BD en AFM <sup>5</sup>	In eerste instantie moet Bovemij voldoen aan wet- en regelgeving, samengevat wordt dit 'beheerste en integere bedrijfsvoering' genoemd. Ten tweede heeft Bovemij sinds 2018 toezichthouderrapportages ontvangen waaruit blijkt dat Bovemij onvoldoende in staat is geweest aan te tonen dat zij aan wet- en regelgeving voldeed.

### 3.4 Validiteit en betrouwbaarheid van het onderzoek

In dit onderzoek is triangulatie van bronnen gebruikt om de nauwkeurigheid van het onderzoek te vergroten. Nikpay et al., (2017) geeft in een vergelijkbaar onderzoek naar de 'implementatie van een effectieve architectuur' aan dat verschillende invalshoeken voor het onderzoek een breder beeld opleveren. Ook beoogt dit de validiteit en betrouwbaarheid van de resultaten te verhogen. Voor het verzamelen van data is daarom gebruik gemaakt van expert rapportages, toezichthouderrapportages, jaarverslagen met een assurance verklaring van externe accountants, door de RvB vastgestelde strategie en beleidsdocumentatie, en tot slot formeel en vastgestelde notulen van officiële comités binnen Bovemij.

In de probleemstelling is duidelijk dat het onderzoek voornamelijk een casus op zich betreft; Bovemij. Het onderzoek bij Bovemij is een combinatie van documentonderzoek, zeepkisten<sup>6</sup> en het verstrekken van een standaard vragenlijst voor het verkrijgen van het risicoprofiel van Bovemij vanuit de RvB (de resultaten zijn samengevat opgenomen in de bijlage van deze thesis). De vier casussen die aanvullend zijn geselecteerd zorgen ervoor dat er vanuit een breder domein een uitspraak kan worden gedaan over het risicoprofiel van een meezijdig platformbedrijf. De diagnose die is verricht binnen de verschillende

<sup>5</sup> De Nederlandsche Bank, Autoriteit Financiële Markten, Rijksdienst voor het Wegverkeer, Belastingdienst en Autoriteit Persoonsgegevens.

<sup>6</sup> Dit zijn periodieke (meestal ieder kwartaal) videomomenten waarin bestuursleden (één per keer) specifieke onderdelen van de nieuwe strategie presenteren aan alle medewerkers. Vergelijkbaar met medewerker bijeenkomsten en dan digitaal.

cases is niet te generaliseren en strekt niet verder uit dan de bestudeerde cases op zich. Echter is een standaard vragenlijst voor het onderzoek gehanteerd dat ook hergebruikt worden voor onderzoek naar andere platformbedrijven. Voor het bestuderen van sociale systemen en of cultuuraspecten binnen een bedrijf als zodanig zou een grotere steekproef nodig zijn volgens (Swanborn, 1994).

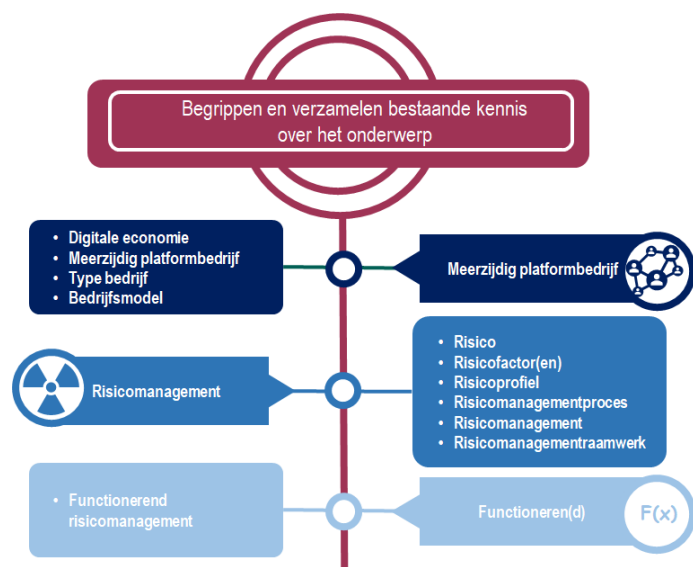
Discussies binnen formele comités (overleggrema) zijn vastgelegd in notulen. Door de vertrouwelijkheid van deze informatie is het niet mogelijk om dit aan deze thesis toe te voegen. De notulen van de verschillende overleggrema worden bewaard bij de bestuurssecretaris en de bestuurssecretarissen. Dit geldt eveneens voor de vertrouwelijke toezichouderrapportages over de integere en beheerste bedrijfsvoering van Bovemij.

Tijdens de brainstormsessies en discussies met interne deskundigen en de kleine zelfstandigen is een beknopt verslag bijgehouden en naderhand aan alle participanten ter bevestiging verstuurd. Dit gaf hen de gelegenheid om te reageren. Deze informatie wordt bewaard binnen de OneDrive (cloud) omgeving van Bovemij. De resultaten zijn samengevat opgenomen in Bijlage E van deze thesis.

#### 4 Literatuuronderzoek

De probleemstelling en hoofdvraag bevatten kernbegrippen die met het literatuuronderzoek zijn gedefinieerd. In dit deel van de thesis zijn verschillende kernbegrippen (Figuur 4-1) en waaruit de begrippenlijst Bijlage L is ontstaan. Het literatuuronderzoek biedt ook bestaande wetenschappelijke kennis (aanvullende informatie is opgenomen in Bijlage A) over het onderwerp, inclusief de risico's die aan een meezijdig platformbedrijf zijn verbonden en dit hoofdstuk schetst de eerste contouren voor het ontwerp van het risicomanagementraamwerk.

**Figuur 4-1** Kernbegrippen en bestaande literatuur



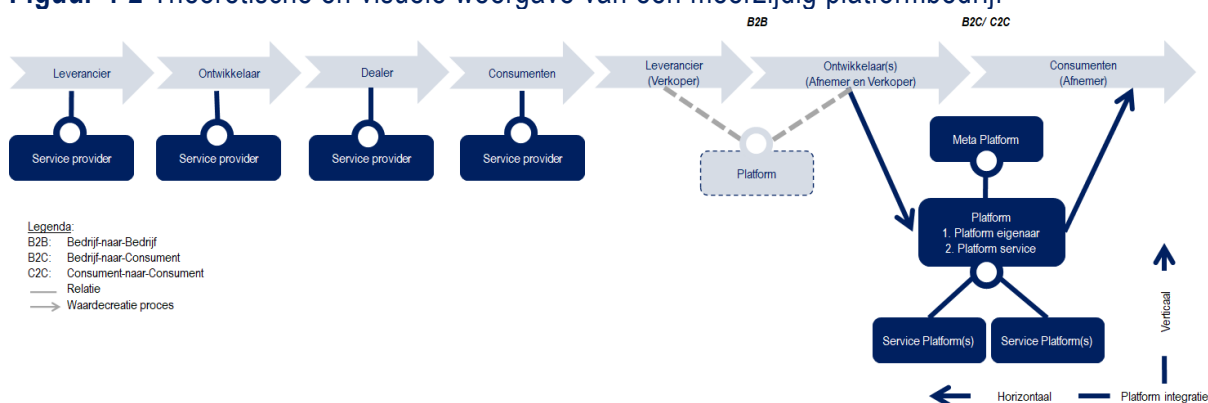
#### 4.1 Digitale economie en Meezijdig platformbedrijf

Een digitale economie is een op digitale technologie gebaseerde marktplaats die de handel of activiteit in producten (goederen) en diensten digitaal faciliteert (Evans, Gawer, 2016, in Yablonsky, 2019). In bredere zin is dit "een economie die gebaseerd is op digitale informatietechnologieën (Heerschap et al., 2019).

Een meezijdig platformbedrijf is een organisatie die waarde creëert door (in)directe interacties mogelijk te maken om een soort van marktplaats voor verkoop (Yablonsky, 2019)) te faciliteren tussen twee (of meer) aangesloten platformgebruikers (actoren) of serviceproviders (samenwerkingspartners) via een digitaal (internet en andere netwerken) ecosysteem. Denkende hierbij aan het verrichten van betalingen, communicatie, financiële uitwisselingen, advertentie-ondersteunende media, besturingssystemen.

Ook zijn er specifieke combinaties mogelijk waarbij een leverancier (verkoper) aan een zakelijke afnemer verkoopt (B2B) en waarbij zakelijke afnemers de producten/ diensten weer verkopen via een platform aan de consumenten (eveneens afnemer) (B2C). Deze zogenoemde meezijdige platform aanbieders bieden services via meerdere (markt)actoren aan door de zijde van een platform aan elkaar te verbinden, d.w.z. meer dan één aanbieder en meer dan één consument. Hierbij vervangen de platformen niet noodzakelijk de gehele supply-chain (linkerkant van **Fout! Verwijzingsbron niet gevonden.**), maar positioneren zich binnen verschillende niveaus van de supply-chain (rechterkant van **Fout! Verwijzingsbron niet gevonden.**).

**Figuur 4-2** Theoretische en visuele weergave van een meezijdig platformbedrijf

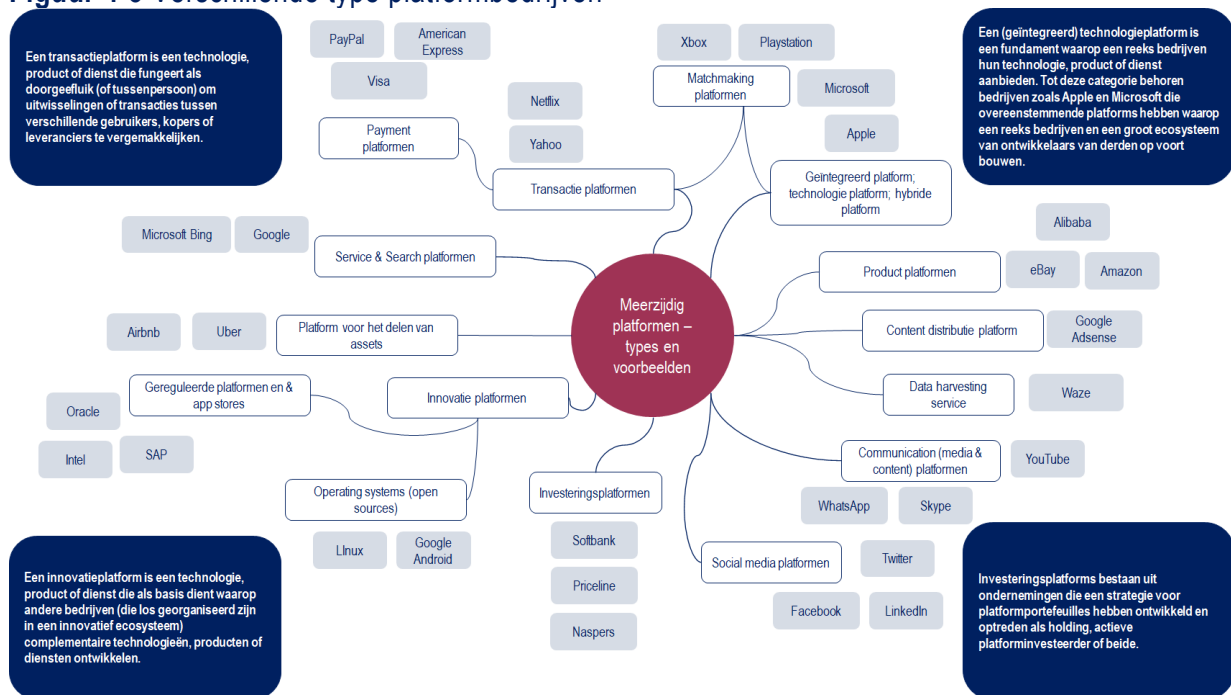


In dit onderzoek worden platformen gezien als het technologische fundament waarop software is gebouwd, als onderdeel van een technologische infrastructuur van een platformbedrijf. Het platform is ontworpen om deelnemers een zoals klanten, partners, medewerkers en andere intelligente machines in staat te stellen een bepaalde activiteit uit te laten voeren.

## 4.2 Type bedrijf en bedrijfsmodel

De afgelopen jaren hebben platformbedrijven bewezen zeer succesvolle bedrijfsmodellen te hebben, zoals Apple, Google, Amazon, Uber, Airbnb, Salesforce, LinkedIn, Alibaba, FlipKart en Jumia (The Center for Global Enterprise, 2021). Dit zijn verschillende type bedrijven met verschillende doelstellingen, doelgroep, bedrijfsactiviteiten enzovoorts. **Fout! Verwijzingsbron niet gevonden.** geeft de verschillende type bedrijven weer met toelichting in de donker blauwe vlakken. Categorisering van typen platformbedrijven kan zowel exclusief, specifiek als algemeen van aard zijn. Ook kan het zijn gebaseerd op verschillende criteria, waaronder interactiemodaliteit, product- of activacombinaties, winstgerichtheid, onderliggende beweegredenen en strategieën (Heerschap et al., 2019). Het meezijdig platformbedrijf groeit in waarde naarmate het meer gebruikers aantrekt, dit is het fenomeen dat bekendstaat als netwerkeffect (A Osterwalder & Pigneur, 2019).

**Figuur 4-3** Verschillende type platformbedrijven<sup>7</sup>



De strategie van een meezijdig platformbedrijf ziet over het algemeen toe op de besturing van strategische managementprocessen en creëert op verschillende manieren waarde door middel van interacties tussen twee of meer verschillende gelieerde gebruikers. De strategieën van verschillende praktijkvoorbeelden lijken iets gemeen te hebben: (i) Het online platform faciliteert meezijdige uitwisseling

<sup>7</sup> Afbeelding samengesteld uit de volgende bronnen: (Evans et al., 2019; Heerschap et al., 2019; Mishra & Tripathi, 2020; Yablonsky, 2019).

tussen aanbieders en gebruikers, (ii) handelt in goederen en diensten, met inbegrip van arbeid en financiën, wisselt informatie en kennis uit, (iii) verschillende organisaties leveren het aanbod van goederen, diensten en informatie en (iv) dit is voor winst of zonder winstoogmerk (Heerschap et al., 2019). Een bedrijfsmodel<sup>8</sup>, inclusief het bedrijfsmodel van een eenvoudig meezijdig platformbedrijf, beschrijft een visie en missie (business drivers), bedrijfsprincipes, doelen en hoe en waarmee een organisatie waarde creëert, levert en behoudt voor haar klanten (gevisualiseerd in bijlage B).

Het bedrijfsmodel van een eenvoudig platformbedrijf is een model dat waarde genereert door het bedienen van twee of meer onafhankelijke groepen, normaal gesproken verkopers en kopers (Mishra & Tripathi, 2020; Parker et al., 2016). Hoewel er vele soorten platforms bestaan, hebben ze volgens Van Alstyne et al., (2016) binnen het digitale ecosysteem eenzelfde basisstructuur, bestaande uit vier soorten spelers: (i) De eigenaren van platformbedrijven die zeggenschap hebben over hun intellectuele eigendom en governance, (ii) aanbieders die als interface tussen de platforms en gebruikers fungeren, (iii) producenten die creëren aanbod, en (iv) consumenten gebruiken het aanbod (Van Alstyne et al., 2016). Het meezijdig platformbedrijf stelt als het ware een instrument ter beschikking door verschillende technologieën te combineren en brengt daarmee nieuwe zakelijke mogelijkheden op een inventieve en transformationele wijze (De Reuver et al., 2018; Mishra & Tripathi, 2020; Mishra & Triptahi, 2019). Echter is de bedrijfsvoering van een Meezijdig platformbedrijf en de samenhang met de technologie gecompliceerd (Yablonsky, 2019, p. 527). Een digitaal Meezijdig platformbedrijf is een business-driven-framework dat een community van partners, providers en klanten in staat stelt om digitale processen en “capabilities” te delen en deze te verbeteren of uit te breiden voor wederzijdse voordelen (geciteerd in Yablonsky (2019) Burton, Basiliere, (2016). Een digitaal platformbedrijf is daarom veel meer dan alleen een bedrijfsmodel of alleen maar de technologie.

### 4.3 Risicofactor(en) en Risicoprofiel

In zogenaamde “best practices” zoals ISO en COSO worden risico’s vaak aangeduid als gebeurtenissen met oorzaken en gevolgen. Literatuur over platformbedrijven en gelijkwaardige literatuur over technologiebedrijven refereren daarentegen vaak naar zogenoemde risicofactoren. Tegelijkertijd kunnen onderzoekers op het gebied van risicomanagement niet voorbijgaan aan het feit dat er verschillende ideeën en opvattingen bestaan over risico’s en de definities ervan (Bijlage B bevat aanvullende

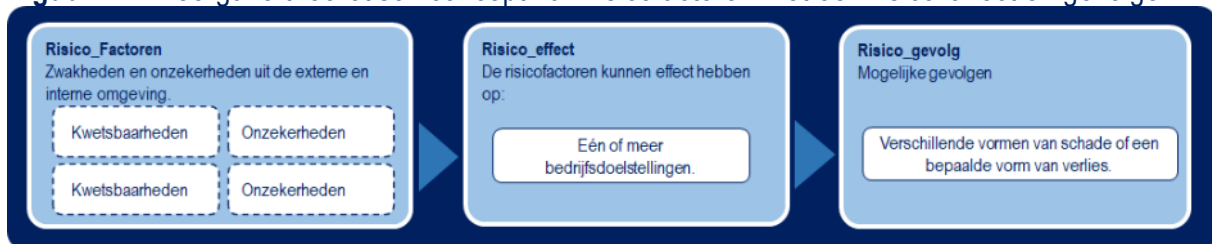
---

<sup>8</sup> Een meer uitgebreidere toelichting van wat een bedrijfsmodel omvat is in Bijlage A opgenomen.



informatie). Vele hiervan hebben betrekking op specifieke disciplineprincipes zoals (register)accountants en hebben vooral betrekking op de implicaties en verklaringen van risico's (Aven, 2012). Vrij gelijkaardig in de literatuur is de verklaring dat een risico een gebeurtenis is onder bepaalde omstandigheden, die al dan niet nauwkeurig zijn te voorspellen, worden onderkent en een wezenlijk nadelig effect kan hebben op de (bedrijfs)activiteiten, groei, reputatie, vooruitzichten, financiële toestand, bedrijfsresultaten en dergelijke (Aven, 2012; NEN, 2019; Zhang et al., 2020). Daarentegen is een risicobron of risicofactor een situatie die alleen of in combinatie met andere situaties tot een risico kan leiden (ISACA, 2013; NEN, 2019). Waardoor een risico daarmee het effect (resultaat) is vanuit een onzekere gebeurtenis op een of meer bedrijfselementen die doelen kunnen bereiken en/ of (tegelijkertijd) verschillende uitkomsten hebben. Een recenter artikel van Zhang et al. (2020) gaat vooral in op de kwetsbaarheden van technologie.

**Figuur 4-4** Weergave theoretisch concept van risicofactoren met een risico-effect en gevolgen



Binnen het Cobit-raamwerk voor risicomanagement wordt gesproken over een risico universum, dat de risico's bevat die inherent zijn verbonden aan een organisatie. De kenmerken van deze risico's, in dit onderzoek risicofactoren genoemd, vormen samen het zogenoemde risicoprofiel op van het bedrijf. Een risicoprofiel is een overzicht van risico's inclusief de kans dat ze zich kunnen voordoen en een schatting van de impact als ze zich voordoen. Het risicoprofiel van een organisatie of onderdeel van een organisatie is het resultaat van de bedrijfsdoelstellingen en de gekozen strategie om deze doelen te bereiken (Hopkin, 2018). Risicomanagement is daarmee ook een primaire discipline van elk bedrijf en omgekeerd die tot de kern van elke onderneming behoort en omgekeerd beïnvloeden de bedrijfsactiviteiten het risicoprofiel (Hopkin, 2018; Stoneburner et al., 2002). Daarom hoeft de inrichting en de functie van risicomanagement dan ook niet hetzelfde te zijn voor alle Meezijdig platformbedrijven of bedrijfsentiteiten in de hele onderneming (Hopkin, 2018). Risicomanagementpraktijken die geschikt worden geacht voor de ene bedrijfsentiteit, zijn mogelijk niet geschikt voor een andere.

#### 4.4 Typische risicofactoren

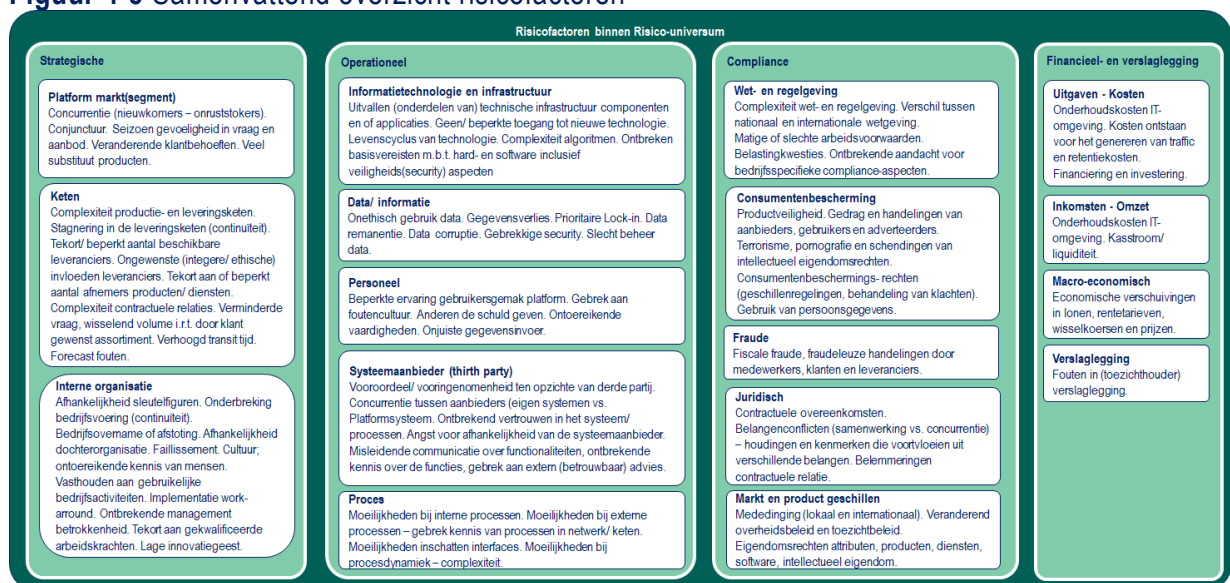
Wanneer het management van een bedrijf er zeker van wil zijn dat het risicomanagement een volwaardige bijdrage levert aan de organisatie, is het belangrijk om de doelstellingen met betrekking tot



risicomanagement en het type bedrijf in overweging te nemen (Hopkin, 2018). Dit hoofdstuk gaat daarom in op typisch voorkomende risicofactoren voor een meezijdig platformbedrijf en bijlage B gaat op een aantal risico's verder in.

Platformbedrijven bestaan al jaren (Van Alstyne et al., 2016) en de bijbehorende strategieën zijn begeerd door CEO's over de hele wereld. In navolging van de enorme succesverhalen die het platformbedrijven als Airbnb en Google hebben opgeleverd. Uit het onderzoek van IBM (2018) onder leidinggevendenden bleek dat 46 procent van hen het potentieel van een platformstrategie wilde realiseren (geciteerd uit Bradford, 2019). Meezijdige platformbedrijven fungeren als intermediair waardoor verschillende groepen afnemers (ook wel platformzijden genoemd) met elkaar kunnen communiceren (Holzweber, 2017). Partnerschappen in de toeleveringsketen, kwaliteitsborging, managementleiderschap, internationale en concurrerende zakelijk omgeving zijn enkele van de belangrijkste organisatorische risicofactoren die de bedrijfsprestaties kunnen beïnvloeden (Oduoza, 2020). In het tijdperk van lean werken (Oduoza, 2020) is de bedrijfsvoering van een organisatie vaak tijd-, kosten- en kwaliteitsgevoelig en waardoor er weinig ruimte is voor vertragingen binnen de gehele keten (Oduoza, 2020). Zo zijn er verschillende risicofactoren binnen en buiten de organisatie die vaak zijn gegroepeerd in het zogenoemde risico-universum, zoals is weergegeven in Figuur 4-5.

**Figuur 4-5** Samenvattend overzicht risicofactoren



## 4.5 Risicomanagement en Risicomanagementproces

Risicomanagement is het geheel aan systematisch toepassen van protocollen, principes, processen, gecoördineerde activiteiten en methodieken (benaderingen) op alle niveaus van een organisatie om zo goed mogelijk op een gecontroleerde manier tot goede resultaten te komen (Claassen, 2009; Hopkin,

2018; Murray-Webster & Williams, 2010; NEN, 2009). Het wijst er in verschillende opzichten op dat risicomanagement gaat over het bereiken van het best mogelijke resultaat voor het bedrijf en het beperken van de volatiliteit of variabiliteit van het resultaat (Hopkin, 2018).

Het risicomanagementproces is een integraal onderdeel van risicomanagement. Het risicomanagementproces heeft verschillende definities, beschrijvingen, ander aantal stappen, verschillende namen voor de stappen, en de toepassing is hangt af van het type bedrijf. Zoals beschreven in het artikel van Stoneburner et al. (2002), is het risicomanagementproces van een technologiebedrijf onderdeel van een groter geheel van risicomanagement. Hoewel er een aantal verschillende processtappen kunnen zijn, komt het erop neer dat de activiteiten in het risicomanagementproces leiden tot het managen van en (enige vorm van) controle hebben in de omgang met risico's. Verschillende artikelen beschrijven dat de methodieken (bijvoorbeeld kwantitatief, kwalitatief of strategische versus operationeel) die worden gebruikt in het risicomanagementproces kunnen verschillen. Overeenkomsten tussen de risicomanagementprocessen gegeven vanuit "best practices" COBIT 5, COSO ERM, ISO 31000 en het artikel van Stoneburner et al. (2002) zijn in Figuur 11-3 **Fout! Verwijzingsbron niet gevonden.** (in bijlage B) samengevat en gevisualiseerd.

#### **4.6 Risicomanagementraamwerk en het functioneren ervan**

Een risicomanagementraamwerk geeft structuur, richting, overzicht van onderling samenhangende bedrijfs- en risicomanagementcomponenten, zodat de organisatie wordt geholpen om risicomanagement en compliance te integreren binnen de (bedrijfs)activiteiten om daarmee de specifieke doelstellingen te bereiken. De term 'raamwerk' en 'framework' worden vaak gebruikt in wetenschappelijke publicaties, maar ook in COSO, ISO 31000 en Cobit5. Het lijkt er ook op dat auteurs van wetenschappelijke publicaties de term niet op een consistente manier gebruiken. Hoewel de hiervoor genoemde definitie in deze thesis wordt gehanteerd, variëren de beschrijvingen in de literatuur en lijkt het concept van een raamwerk (of kader) in de eerste plaats een manier te zijn om te communiceren, te verenigen en te structureren en met behulp van wat in een bepaald domein bekend is iets gemeenschappelijks te creëren (Stamer et al., 2016). Dit zijn nog steeds algemene omschrijvingen, maar aangezien vastgestelde kaders in alle opzichten sterk van elkaar kunnen verschillen, is het vinden van een zeer specifieke beschrijving niet zinvol geacht volgens Stamer et al. (2016).

De context van een raamwerk varieert ook. Het raamwerk, ook wel genoemd als een conceptueel model, is volgens Palvia et al. (2003) bijzonder nuttig voor een bepaalde discipline of onderwerp wanneer

inspanningen voor theorie te ontwikkelen ontbreken (Palvia et al., 2003). Zoals Tabel 4-1 weergeeft kan ook de indeling van onderdelen in het raamwerk verschillen en toch kan de inhoud overeenkomen.

**Tabel 4-1** Generieke onderdelen van een Risicomanagementraamwerk

Raamwerken <sup>9</sup>	COBIT 5 for Risk	ISO 31000	COSO
▶	Principes, Beleid en raamwerk	Leiderschap & Commitment.	Governance & Cultuur
	Processen	Integratie in organisatiestructuren en -context.	Strategie & Formulering doelstelling
	Organisatiestructuren	Ontwerp: -Inzicht in organisatie en context. -Uitspreken commitment -Toewijzen rollen, bevoegdheden, verantwoordelijkheden en verantwoordingsplicht. -Toewijzen van middelen -Inrichten communicatie en consultatie	Prestatiemanagement
	Cultuur, Ethiek en gedrag	Implementeren	Review & herziening
	Informatie	Evaluatie Verbetering: -Aanpassen -Continu verbeteren	Informatie, communicatie en rapportage
	Service, Infrastructuur en Applicaties		
	Mensen, kennis en kunde.		

Het doel van een risicomanagementraamwerk is om een organisatie te helpen risicomanagement te integreren in kernactiviteiten en -functies van het bedrijf (NEN, 2019). Het doet dit door te helpen bij het organiseren en structureren van een aanpak die zowel meetbaar als reproduceerbaar is. Het raamwerk is daartoe een raamwerk dat de implementatie van risicomanagement ondersteunt. De dynamiek, resultaten en verwachte prestaties van risicomanagement variëren van organisatie tot organisatie (Hopkin, 2018).

De eerste en misschien wel de belangrijkste stap voor het functioneren is te zorgen dat het risicomanagementinitiatief wordt erkend en gesponsord door een lid van de raad van bestuur of senior executive van de organisatie (Hopkin, 2018). Het functioneren of effectiviteit van het risicomanagementraamwerk zal afhangen van de integratie ervan in de governance van de organisatie,

<sup>9</sup> Geen specifieke volgorde m.u.v. het raamwerk van COSO.

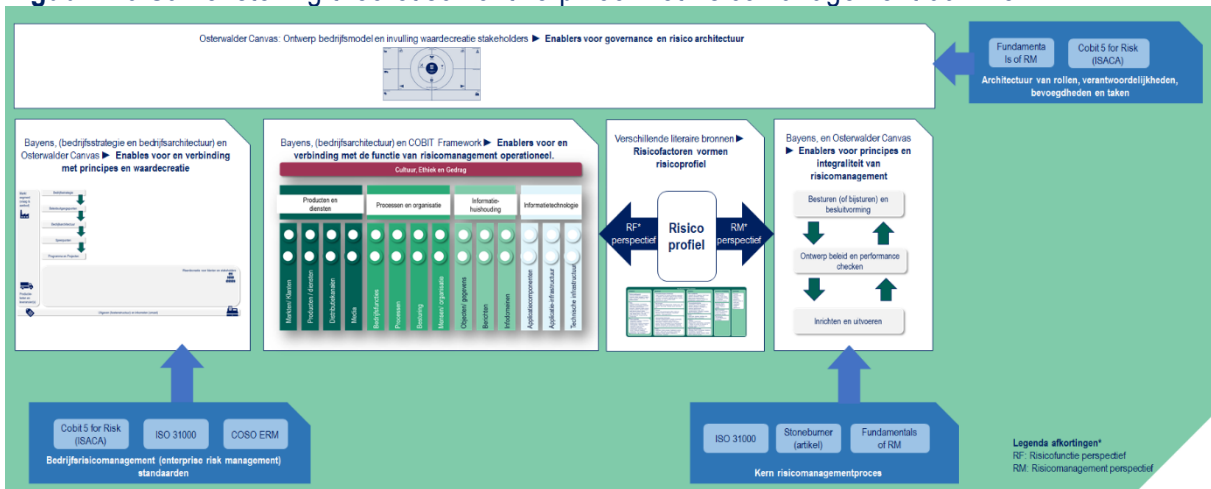
inclusief besluitvorming (NEN, 2019). Ook kunnen veel factoren van invloed zijn op hoe goed een risicomanagementtraamwerk werkt, waaronder:

- invloed van het hoger management binnen afdelingen;
- externe invloeden, met inbegrip van corporate governance;
- de aard van de onderneming, haar producten en cultuur;
- bedrijfshouding, inclusief eerdere RM-ervaringen; of
- de oorsprong of het ontstaan van een afdeling risicomanagement (Hopkin, 2018).

#### 4.7 Samenstelling theoretisch ontwerp

Vanuit de literatuur is een theoretisch ontwerp voor een risicomanagementtraamwerk ontworpen. Figuur 4-6 toont de samenstelling van het theoretische ontwerp en hoe het zich dit verhoudt tot de theorie van het type meezijdig platformbedrijf. Samen levert dit de richtlijnen en kaders op voor de verdere uitwerking van het risicomanagementtraamwerk met informatie uit de praktijk.

**Figuur 4-6** Samenstelling theoretisch ontwerp voor het risicomanagementtraamwerk



Figuur 4-6 toont dat:

- De algemene focus van het risicomanagementtraamwerk ligt op het toepassen van risicomanagementkaders vanuit een bedrijfs perspectief (platformbedrijf) en een risicomanagementfunctieperspectief. Dat wil zeggen, hoe bestuurders hun bestuursprocessen, governance en risicomanagement kunnen gebruiken om risico's binnen het risicoprofiel van de organisatie op een effectieve en efficiënte manier te managen.

- Het raamwerk begeleiding en overzicht biedt op bedrijfs- en operationeel niveau om risico's te identificeren, analyseren en beheersen van risico's door het risicomanagementproces toe te passen. Waarbij het risicomanagementproces is afgestemd op de organisatiestructuur en -functies, kernprocessen, systemen, informatie, producten, diensten en informatietechnologie.
- Het raamwerk aansluit op marktstandaarden voor risicomanagement en voor de inhoud is aangevuld met wetenschappelijke publicaties (zoals normen en praktijkrichtlijnen waaronder risicomanagement bij informatietechnologiesystemen van Stoneburner en Cobit).

Het theoretisch ontwerp geeft op dit punt nog geen inzicht en raakvlakken tussen het risicoprofiel en de kaders die kunnen worden gebruikt door Bovemij.

## 5 Beschrijving, Analyse en Diagnose Bovemij en praktijkvoorbeelden

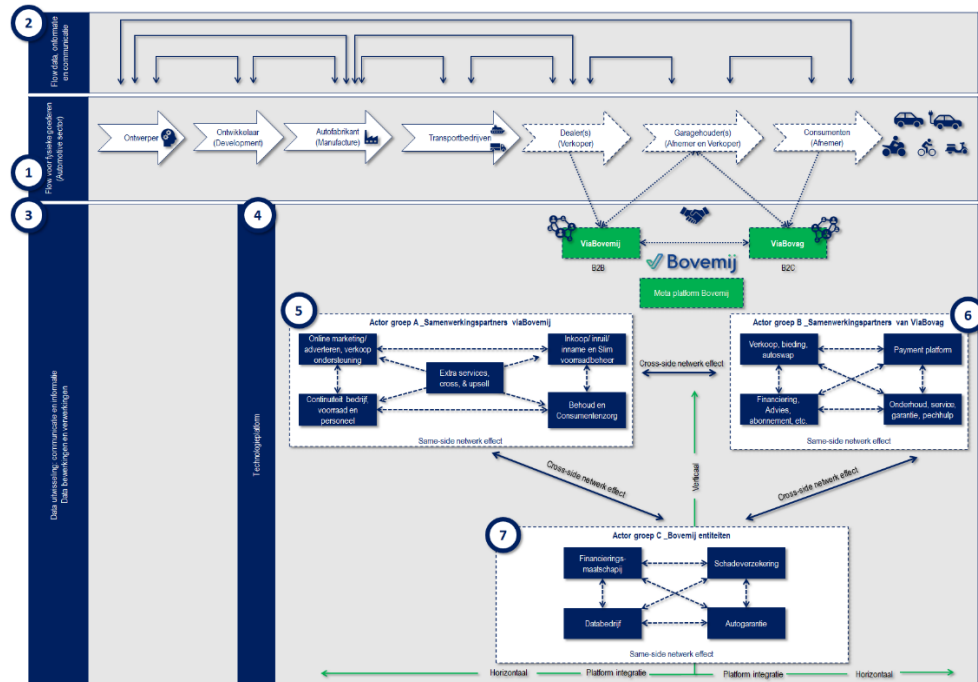
Binnen het literatuuronderzoek is de toepassing van raamwerken (paragraaf 4.6) onderzocht. Zoals COSO, ISO en Cobit stellen dient het raamwerk te passen bij de context van de organisatie. Voor het ontwerpen van het raamwerk is daarom in dit hoofdstuk de externe en interne context van de organisatie beschreven als uitkomst van de diagnose van Bovemij. Dit resultaat is voor het raamwerk aangevuld met informatie uit de praktijk vanuit vergelijkbare bedrijven. Dit hoofdstuk beschrijft de diagnose en werkt toe naar hetgeen het raamwerk dient te bereiken.

### 5.1 Externe context – Mobiliteitsbranche

Sinds het ontstaan van Bovemij heeft de organisatie zich gericht op het zijn van een financiële dienstverlener in de mobiliteitsbranche. Begin 2020 telt de Nederlandse mobiliteitsbranche bijna 8,7 miljoen personenauto's, waarvan ruim 7,6 miljoen personenauto's in particulier bezit en 1 miljoen op naam van een bedrijven (CBS, 2020) ofwel doelgroepen van Bovemij. Bovemij biedt aan deze branche een breed scala aan verzekeringsproducten, financieringen (kredieten), rechtshulp en dataproducten. Tot op de dag van vandaag zit de kracht van Bovemij in het leveren van alle vormen en soorten oplossingen voor kleine/ grote ondernemers en hun werknemers in de mobiliteitsbranche. Kenmerkend voor Bovemij is haar wilskracht en doorzettingsvermogen om haar zakelijke klanten op een creatieve wijze blijvend een helpende hand aan te reiken en hen te verbinden met particuliere klanten (consumenten). Zodoende heeft de Raad van Bestuur een zogenoemd mobiliteitsplatformplan ontwikkeld. Dit plan dient ertoe te leiden dat Bovemij de volledige distributieketen (nummer 1 in afbeelding 5-1) binnen de mobiliteit sector kan faciliteren. Door de platformen viaBovag en viaBovemij aan elkaar te verbinden zou idealiter een optimale end-to-end klantervaring moeten ontstaan.

Bovemij heeft sinds 2020 een strategie<sup>10</sup> ontwikkeld, de zogenaamde ‘matchmaking’, die via het platform de behoeftes van verschillende doelgroepen digitaal aan elkaar koppelt. Dit betekent dat verschillende actoren via het platform met elkaar zijn verbonden. Het platform bedient hiermee 'zakelijke en individuele klanten', 'samenwerkende partners' en 'leveranciers'. Met deze strategie wil Bovemij ruim 1 miljoen mobiliteitsgebruikers te verbinden met meer dan 10.000 mobiliteitsbedrijven in Nederland. Zodoende bestaan waardeproposities bestaan van Bovemij onder meer uit het digitaliseren van processen waar menselijk gedrag geen waarde toevoegt en daarmee het bouwen van een flexibele, schaalbare en veilige ICT-infrastructuur op basis van Cloud-technologie. Als platform creëert Bovemij hiermee waarde door klanten en hun (toekomstige) behoeften te kennen en te gebruiken in nieuwe producten en diensten. Dit platform is een open platform waarop andere belanghebbenden kunnen aansluiten en biedt daarmee diensten en producten aan die een aanvulling vormen op de bestaande producten en diensten van Bovemij.

**Figuur 5-1** Bovemij<sup>11</sup> als Meezijdig platformbedrijf, met de verschillende actorengroepen, binnen de mobiliteitsbranche



Bovemij verbindt straks verschillende organisaties en verschillende groepen actoren (zie nummers 5, 6 en 7 in figuur 5-1). Dit zijn organisaties die bijdragen aan de verkoop van producten en dienstverlening in

<sup>10</sup> De beschrijving voor deze alinea is overgenomen uit het strategische plan dat binnen Bovemij bekend staat onder het project Hermes (Vertrouwelijk).

<sup>11</sup> Afbeelding is een samenvatting uit (Bovemij N.V., 2021). Grote afbeelding is beschikbaar in Bijlage A.

de mobiliteitsbranche. Daarnaast blijven de dochterondernemingen (nummer 7) van Bovemij desgewenst producten en diensten rechtstreeks via hun kanalen blijven aanbieden. Het Bovemij platform gaat functionaliteiten met verschillende modules (werkplaatsvoorraadbeheer, marketingondersteuning, etc.) aanbieden via meerdere samenwerkende partners (nummers 5 en 6). Hieruit blijkt dat het digitale ecosysteem rondom Bovemij ontstaat en dat er netwerkeffecten gaan ontstaan.

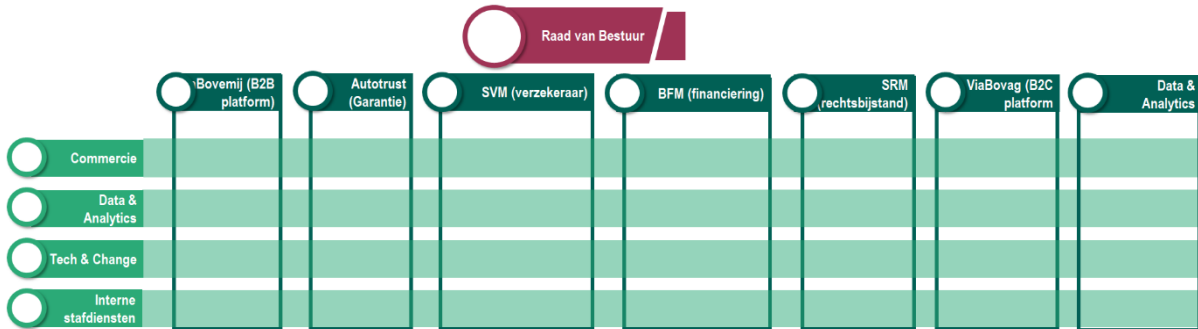
Belangrijke sturende factoren en trends die van invloed zijn op de doelstellingen van Bovemij zijn volgens het Bovemij marktvisie document (samengevat):

- Technologie, 'in' het voertuig en 'eromheen'.
- Keten, van showroom verkoop naar een lineaire waardeketen binnen een netwerkmodel, dealers uit de keten door directe marktbenadering vanuit fabrikanten.
- Business Model Canvas, door vraag en aanbod veranderingen in behoefte van klant verschuift het koopgedrag naar online, hierdoor van transactie naar relatie door abonnement.
- Mobiliteitsvorm, van bezit naar gebruik, abonnementsvormen fixed naar pay per use en meer B2B2C.
- Ecologische Footprint, CO2 en energie/ aandrijving, 'well to wheel', verduurzaming, hervorming van autobelastingen.
- Wagenpark, structurele groei verkoop auto's door meer mensen (huishoudens) en zakelijk gebruik, occasionhandel sterke groei in B2C, veroudering wagenpark.

## 5.2 Interne context - Meezijdig platform bedrijf – organisatie

De rechtspersoon Bovemij N.V. is een groep van verschillende juridische bedrijfsentiteiten. In 2020 is het organisatiemodel aangepast naar een matrixorganisatie dat gebruikmaakt van horizontalen en verticalen (zoals weergegeven in figuur 5-2). De verticale bedrijfsentiteiten leveren de producten, diensten en services naar de klanten. De zogenaamde horizontalen ondersteunen de verticalen in de bedrijfsvoering, wat idealiter leidt tot een efficiënte bedrijfsvoering.



**Figuur 5-2** Organisatiemodel Bovemij Groep<sup>12</sup>


Zoals blijkt uit het organigram in bijlage A, heeft Bovemij als groep te maken met verschillende ondernemingen (BV's) en daarmee verschillende grondtypen ondernemingen. Bovemij heeft verschillende type bedrijven, waaronder: Verzekeringsmaatschappijen, garantiebedrijven, financieringsbedrijven (financiële instellingen), databedrijven en autoverkoopplatform. De stafafdelingen zijn ondergebracht in één business unit: Technologie (ICT) en Change, HRM, Inkoop, Financiën en Control, Financiële Administratie en in de toekomst ook een Juridische zaken (nu nog bij Dirk Zwager ingekochte dienstverlening). Met deze opzet is het duidelijk dat het risicomanagementraamwerk van toepassing is op alle bedrijfsonderdelen en verschillende typen bedrijfsonderdelen binnen de groep moet adresseren. Het is van belang dat het risicomanagementraamwerk minimaal voldoet aan de wettelijke eisen, aangezien de entiteit SVM onder toezicht staat van DNB, BFM onder toezicht van de AFM en D&A onder toezicht van de RDW.

Bovemij is één van de bedrijven in de wereld met een sterk verouderde informatietechnologie (IT) en een enorm erfenis van systemen en processen die voortkomen uit bestuursbesluiten van eerdere bestuurders.

De nieuwe raad van bestuur ontwikkelde in 2020 de digitalisering/platformstrategie voor de komende vijf jaar. Deze strategie moet er onder andere voor zorgen dat de zogenoemde "basis op orde" komt, onder meer de vervanging van verouderde informatietechnologieën en het inrichten van procesmanagement. Daarnaast bouwt Bovemij, middels een radicale transformatie, aan een toekomstbestendig (technisch) meezijdig platform bedrijf dat B2B en B2C met elkaar gaat verbinden.

<sup>12</sup> Overgenomen uit het Strategisch bedrijfsplan, hoofdstuk inrichting topstructuur, Copyright door Bovemij N.V. (2021)



Voor de transformatie zijn zes programma's opgezet om het transformatieplan<sup>13</sup> tot uitvoering te brengen: 1. Bouwen aan een digitale organisatie, 2. Opschalen ViaBovag, 3. Inrichten viaBovemij, 4 Inrichten dataplatform, 5. Digitalisering van bedrijfsonderdelen, 6. Ontwikkelen technologieplatform. Het doel van het transformatieplan is een efficiënte, gecontroleerde en succesvolle transformatie naar een mobiliteitsplatform. De ontwikkeling van het technologieplatform is uitbesteed aan de provider Tata Consultancy Services (TCS). Om van een financiële dienstverlener naar een veelzijdig platformbedrijf te gaan, heeft Bovemij een transformatieplan opgesteld en eind 2020 vastgesteld.

Het business- en verdienmodel van Bovemij als meezijdig platformbedrijf ontbreekt nog. Dit leidde in 2021 onder andere tot het opstellen van een Target Operating Model en het identificeren van enablers voor Bovemij naar aanleiding van de bevindingen vanuit KPMG. In 2020 heeft KPMG (Strategic Consultant) namelijk de volwassenheid van Bovemij als platformbedrijf onderzocht en vergeleken met vergelijkbare organisaties. Het KPMG model bevatte een zestal dimensies (figuur 5-2) waar Bovemij tegen is geëvalueerd. Deze dimensies richtte zich op de procesinrichting, het personeelsbeleid, services en sourcing, governance en controls, performance management, technologie en data. Het is ook belangrijk op te merken dat Bovemij Tech & Change en Data & Analytics – Agile Safe toepast binnen haar business units, en dat Change de going concern is. Het is ook anders dan de verzekeringsmaatschappij SVM die Lean principes gaan toepassen.

**Figuur 5-3 Elementen in Target Operating Model voor Bovemij**



### 5.3 Huidig risicomanagement bij Bovemij

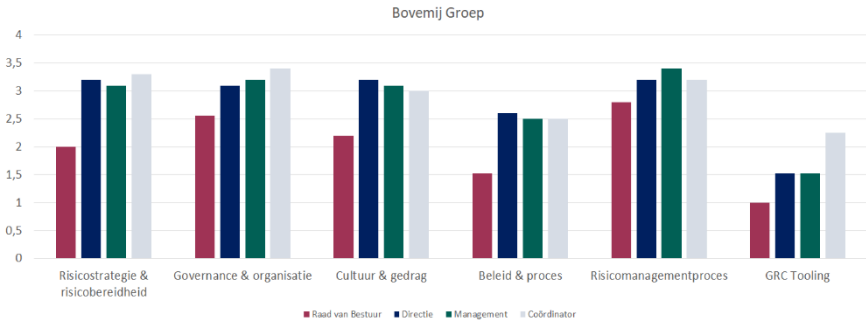
Bovemij heeft volgens de onderzoeksresultaten een 'informele en ad-hoc' volwassenheidsniveau in de toepassing van risicomanagement. Echter representeert dit onderzoek de perceptie van medewerkers en niet persé de feiten, als in aantoonbaar. Anno 2019 ontbrak een structurele en aantoonbare integere en beheerste bedrijfsvoering. Bovemij was eveneens tot voor kort een verzekeringsmaatschappij onder groepstoezicht bij DNB en geen meezijdig platformbedrijf. Dit in combinatie met significante incidenten (vóór 2019) door niet-naleving van wet- en regelgeving die aan toezichhouders werd gemeld, moest

<sup>13</sup> Beschrijving is verkort overgenomen uit het transformatieplan d.d. 26-11-2020 (Bovemij N.V., 2020).

Bovemij onder zeer hoge druk een risicomanagementfunctie en een compliancefunctie opzetten. Sindsdien hebben met name verschillende projecten de huidige risicomanagementinrichting aantoonbaar gemaakt. De bij Bovemij zogenoemde ‘tegels zijn opgetild’ om te kunnen verbeteren.

In 2021 is met **Figuur 5-4 Onderzoeksresultaten op groepsniveau**

ondersteuning van KPMG (advisory) onderzoek gedaan naar de volwassenheid van risicomanagement bij Bovemij. Van de 98 uitgenodigde



respondenten hebben 51 personen de vragenlijst geopend, 43 personen hebben de eerste vraag van het eerste onderwerp beantwoord en 33 van hen hebben de vragenlijst in z'n volledigheid afgerond. Op basis van de resultaten van 43 (gestarte) deelnemers scoorden de bedrijfsonderdelen van Bovemij gemiddeld een 2,9 op een schaal van 5,0. Dit getal representeert het niveau dat nog net onder 'informele en ad-hoc' toepassing valt, maar wat het niveau nadert van 'gestructureerd en gestandaardiseerd'. De resultaten<sup>14</sup> van dit onderzoek zijn de eerste nulmeting. KPMG geeft expliciet aan dat de gegeven scores zijn gebaseerd op de percepties van medewerkers, managers en directeuren (zogenoemde 1<sup>ste</sup> lijn functionarissen) en dus per definitie niet de feitelijke mate van volwassenheid weergeven die ook kan worden aangetoond. Dit onderzoeksresultaat is noch de perceptie van de risicomanagementfunctionarissen (zogenoemde 2<sup>e</sup> lijn functionarissen) en KPMG.

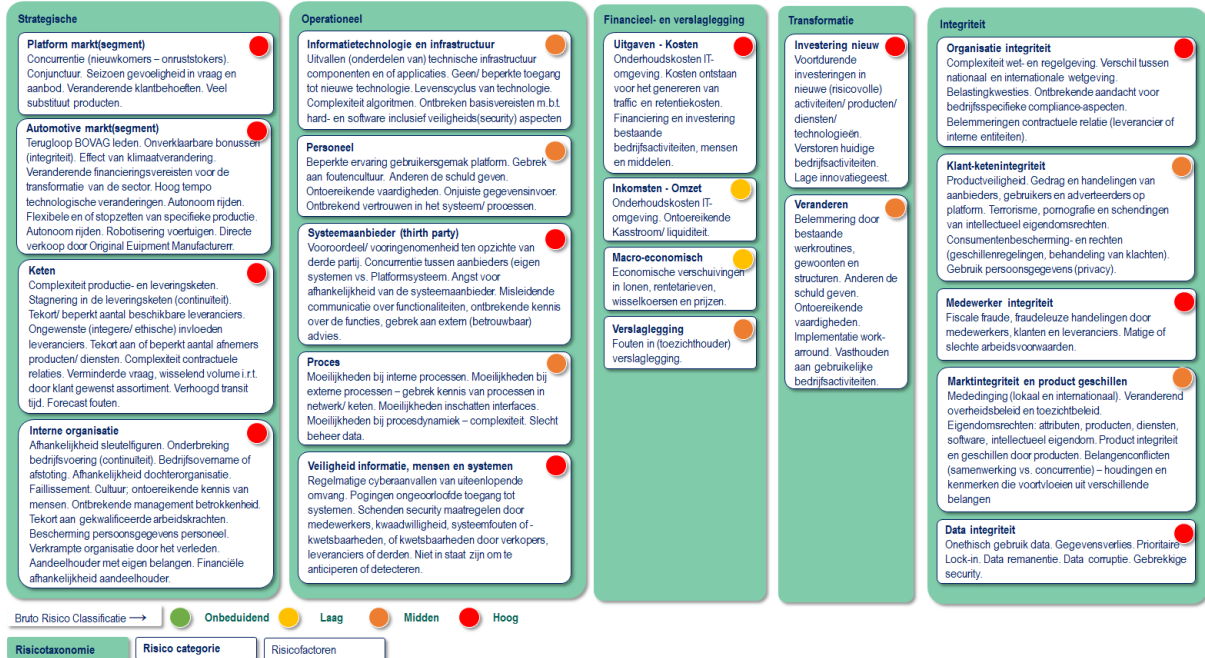
### Huidig risicotaxonomie en Risicoprofiel Bovemij

De risicotaxonomie, als in de risicotypologieën waaraan de bedrijfsvoering van Bovemij is blootgesteld, komt voort uit de COSO ERM componenten: strategisch, operationeel, verslaglegging en compliance (integriteit). Vanwege de huidige levensfase waarin Bovemij zich als bedrijf bevindt, zijn Financieel en Transformatie als hoofdcategorieën toegevoegd. Ook is in samenspraak met zogenaamde sleutelfunctionarissen het risicoprofiel ontwikkeld en bevat de risicofactoren die het risicoprofiel van

<sup>14</sup> De belangrijkste resultaten uit het onderzoek zijn opgenomen in Bijlage D.

Bovemij zowel positief (kans) als negatief (risico) kunnen beïnvloeden. Dit tezamen is weergegeven in Figuur 5-4.

**Figuur 5-5 Huidige risicoprofiel van Bovemij**



## 5.4 Equivalente bedrijven

Jaarverslagen van grote (uiteraard) succesvolle bedrijven stellen dat het functioneren van risicomanagement vaak afhankelijk is van een effectieve implementatie door mensen. De implementatie van het risicomanagementtraamwerk is onderhevig aan menselijke beslissingen, fouten of vergissingen op alle niveaus binnen een organisatie en kan een aanzienlijk negatief effect hebben op de activiteiten en prestaties van het bedrijf. Het grootste verschil in de toepassing van risicomanagement tussen de vier geanalyseerde bedrijven zit hem in de wettelijke verplichtingen waaraan zowel continentaal als nationaal moet worden voldaan.

Verder wordt in de jaarverslagen niet expliciet vermeld dat er gebruik wordt gemaakt van een specifiek kader (of een onderdeel daarvan) zoals COSO, anders dan de wettelijke verplichtingen die voortvloeien uit een beursgang, zoals richtlijnen voor openbaar bestuur (Corporate Governance Guidelines). Dit zijn meestal afzonderlijke documenten die de rollen, verantwoordelijkheden, taken en bevoegdheden van de verschillende audit- en risicocomités, bestuurders, commissarissen en dergelijke beschrijven. De wet schrijft ook voor hoe verschillende risicomanagementkaders moeten worden toegepast. Zo schrijft de “Standing Committee of the National People’s Congress in China” regels voor informatiebeveiliging en

privacy voor. Maar net als de wetgeving Basel (bankieren) en Solvency II (verzekeringsmaatschappij) in Europa, heeft China de “Guidelines on Information Technology Risk Management of Commercial Banks” die beschrijft hoe banken in de sector risicomanagement moeten toepassen.

Tijdens het onderzoek zijn verschillende soorten risico categorieën en risicofactoren geïdentificeerd. Tabel 5-1 bevat een samenvatting van wat er door verschillende bedrijven is gerapporteerd (bijlage G). Wat opvalt, is het verschil in het aantal gerapporteerde risicofactoren. Alle vier de bedrijven zijn beursgenoteerd, wat betekent dat ze onder strikte regels moeten rapporteren. VNV Global noemt risicofactoren echter minimaal en rapporteert alleen oppervlakkig over hun risico categorieën en niet over risicofactoren.

**Tabel 5-1 Geïdentificeerde risico categorieën en aantal verschillende risicofactoren per categorie**

Aantal van Risico_factor	Kolomlabels				Eindtotaal
Rijlabels	Amazon.com, Inc. (leeg)	Alphabet Inc	VNV Global	NewLink Technology	Eindtotaal
Data_informatie_risico	1	2		3	6
Financieelrisico	6	12	9	14	41
Informatietechnologierisico	4	9			13
Integriteitsrisico	1	2			3
Ketenrisico_supply_chain	6	2		1	9
Procesrisico_operationeel	4		1		5
Product_Dienst_Service_risico	6	6		4	16
Strategisch_omgevingsrisico	12	14	5	18	49
Strategisch_organisatierisico	18	10	4	16	48
(leeg)					
<b>Eindtotaal</b>	<b>58</b>	<b>57</b>	<b>19</b>	<b>56</b>	<b>190</b>

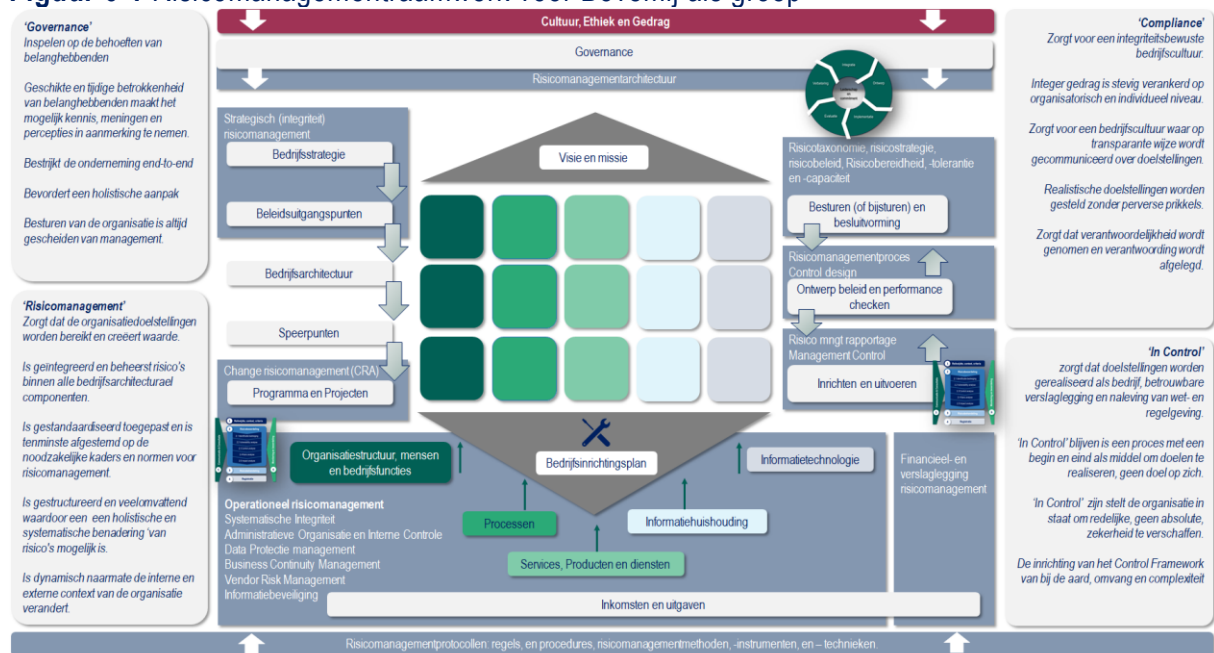
Het aantal financiële risico's bij Alphabet en NewLink is beduidend hoger dan bij de andere twee. De risicofactoren hiervoor hebben met name een verband met de handelsprijs voor bedrijfsaandelen. Opmerkelijke risicofactoren die in alle vier de bedrijven opvallen, zijn strategisch milieurisico en organisatierisico. Vermeldenswaard zijn hier de risicofactoren die samenhangen met wet- en regelgeving en de afhankelijkheid van sleutelfiguren. Wetgevende en regelgevende factoren zijn voornamelijk het resultaat van de internationale bedrijfsvoering. De afhankelijkheid van sleutelfiguren is opmerkelijk, aangezien alle vier de bedrijven rapporteren over specifieke directieleden en bestuursfunctionarissen waarvan zij beweren afhankelijk te zijn. Daarnaast onderscheidt NewLink zich van de andere drie bedrijven doordat het ook rapporteert over hoe zij zorgen dat producten en diensten voldoen aan (lokale) wet- en regelgeving en welke risicomanagementstandaarden en of methoden worden gehanteerd bij de ontwikkeling ervan.

De conclusie van het onderzoek naar andere bedrijven is dat het vooral hielp bij het identificeren van de risicotaxonomie, risicotypen en risicofactoren. Voor dit onderzoek en vanwege de wijze van onderzoek bieden de resultaten geen aanvullende input voor het ontwikkelen van het risicomanagementraamwerk.

## 6 Ontwerp risicomanagementraamwerk Bovemij

Dit hoofdstuk bevat de uitwerking van het ontwerp risicomanagementraamwerk als resultaat van het literatuuronderzoek en resultaten uit de diagnosefase. Het risicomanagementraamwerk, getoond in figuur 6-1, bestaat uit verschillende componenten die in het geheel dan wel gedeeltelijk op verschillende plekken van de organisatie van toepassing zijn. In dit hoofdstuk is per component ingegaan op hoe, waarom en wat Bovemij ermee gaat doen.

**Figuur 6-1** Risicomanagementraamwerk voor Bovemij als groep



### 6.1 Governance en risicomanagementarchitectuur

Het functioneren van het risicomanagementraamwerk is afhankelijk van de integratie van governance binnen de organisatie (figuur 6-2). Governance zorgt voor een evenwichtige integratie van behoeften, voorwaarden en in onderling overleg met stakeholders ondernemingsdoelstellingen worden bepaald. Het geeft richting aan de organisatie, stelt prioriteiten, biedt kaders, zorgt ervoor dat beslissingen op de juiste plaats in de organisatie worden genomen, stuurt de organisatie aan, stuurt op prestaties omwille van de bedrijfsdoelstellingen. Idealiter geldt de governance binnen Bovemij op een eenduidige manier voor het hele bedrijf. Risicomanagement is daarbij een integraal onderdeel van de governance. Waarbij governance binnen Bovemij explicieter wordt gemaakt door het vaststellen van rollen in de organisatie,

verantwoordelijkheden waarover een verantwoordingsplicht is en de wijze waarop toezicht wordt uitgeoefend met betrekking tot risicomanagement.

**Figuur 6-2** Bovenste component governance en risicomanagementarchitectuur



De risicomanagementarchitectuur is de samenstelling van verantwoordelijkheden, bevoegdheden, taken en rollen die zijn toegewezen aan functionarissen en comités. Hierbij is eigenaarschap en eigen verantwoordelijkheid nemen essentieel voor het laten slagen van risicomanagement. Elke verwarring inzake verantwoordelijkheden, communicatie en rapportagestructuur moet worden opgelost. De volgende aspecten voor het managen van risico's vereisen duidelijke verantwoordelijkheden:

- Vaststellen en toepassen van vereiste kaders voor risicobeheersing en voldoen aan wet- en regelgeving
- Toezicht houden op de risicoprestaties

Bovemij richt hiervoor de Three Lines of Defence in en verschillende Risico Comitès en communicatielijnen.

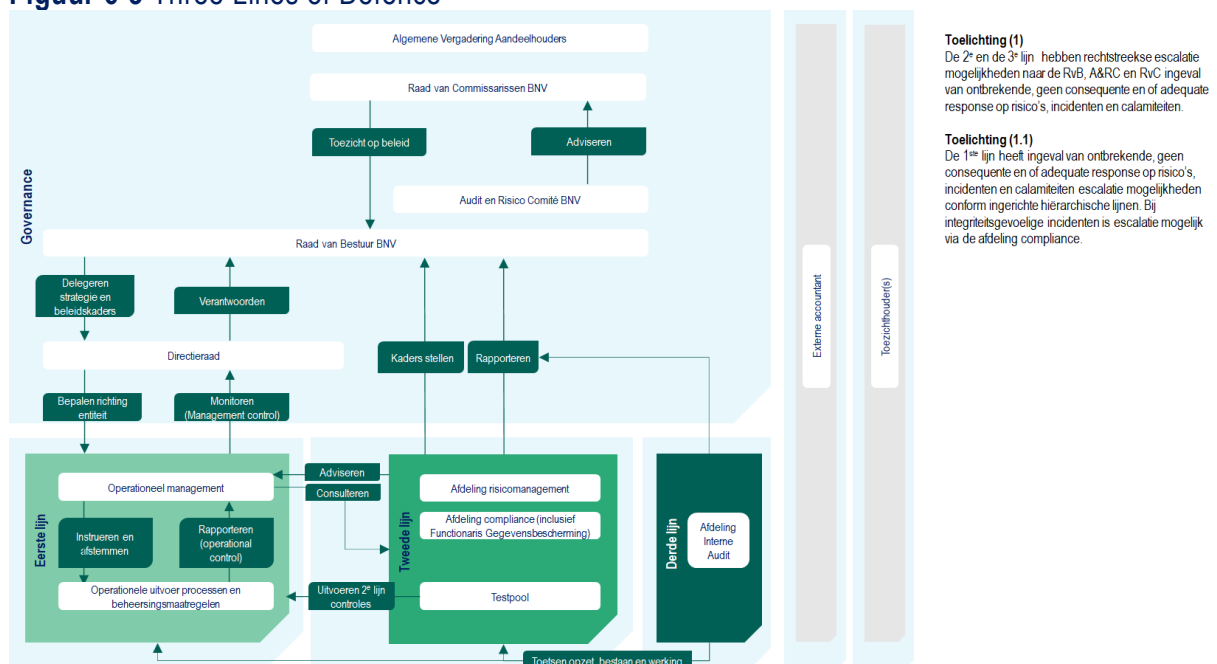
### 6.1.1 Three Lines of Defence

De Three Lines of Defence (3LoD) betreft de door Bovemij gekozen inrichting van de organisatie voor risicomanagement; hoe functionarissen betrokken zijn, wat ze doen en hoe ze met elkaar omgaan in hun eigen verantwoordelijkheidsgebieden. Het model bevat ook de escalatiepaden om conflicten op te lossen die verband houden met de toepassing van het risicomanagementraamwerk en het onderliggende beleid. De gecombineerde benadering van governance en risicomanagementarchitectuur binnen de 3LoD (zoals in figuur 6-3 verticaal is weergegeven) is gebaseerd op de algemene opvatting dat de Raad van Bestuur eindverantwoordelijk is voor alle governance- en risicomanagement aangelegenheden in de hele organisatie. Het bestuur van Bovemij bestaat uit een raad van bestuur en een directiecomité, waarbij de chief executive officer de eindverantwoordelijkheid heeft voor het bestuur binnen de raad van bestuur. Het bestuur van Bovemij zal in zijn rol alle drie de verdedigingslijnen in overweging nemen om ervoor te zorgen dat risico's voldoende aandacht krijgen en op de juiste wijze worden aangepakt. De raad van bestuur van Bovemij delegeert verantwoordelijkheden voor het toezicht op de toepassing van risicomanagement in de verschillende lijnen. Andersom dienen de zogenoemde 1<sup>ste</sup> lijn functionarissen verantwoording af te leggen richting de Raad van Bestuur.



In de 3LoD zijn de verdedigingslijnen ook horizontaal (onderste drie groen gekleurde blokken) verdeeld met betrekking tot rollen, verantwoordelijkheden, bevoegdheden, taken en communicatielijnen voor de beheersing van risico's, vraagstukken en gebeurtenissen met betrekking tot risicomanagement en compliance. Het doel is om de verantwoordingsplicht te vereenvoudigen om verantwoordelijkheid te nemen voor effectieve en efficiënte risicomanagementprestaties, ofwel het risicomanagementraamwerk op onderdelen laten functioneren. Cruciaal is dat 3LoD het eigenaarschap van het risico van de risico-eigenaar versterkt en dat de 2<sup>e</sup> en 3<sup>e</sup> lijn onafhankelijk en objectief zijn gepositioneerd. Daarom is de filosofie van 3LoD in Bovemij gebaseerd op het idee dat 1) operationeel management primair verantwoordelijk is voor de aantoonbare effectieve uitvoering van beleid en beheersingsmaatregelen; 2) specifieke tweedelijns functies het operationeel management bijstaat bij het ontwikkelen van methoden voor het uitvoeren van hun verantwoordelijkheden en onafhankelijk de effectiviteit van beheersingsmaatregelen toetst; en 3) de interne-auditfunctie toetst opzet, bestaan en werking van de governance, het risicomanagementsysteem of dat dit effectief is ingericht.

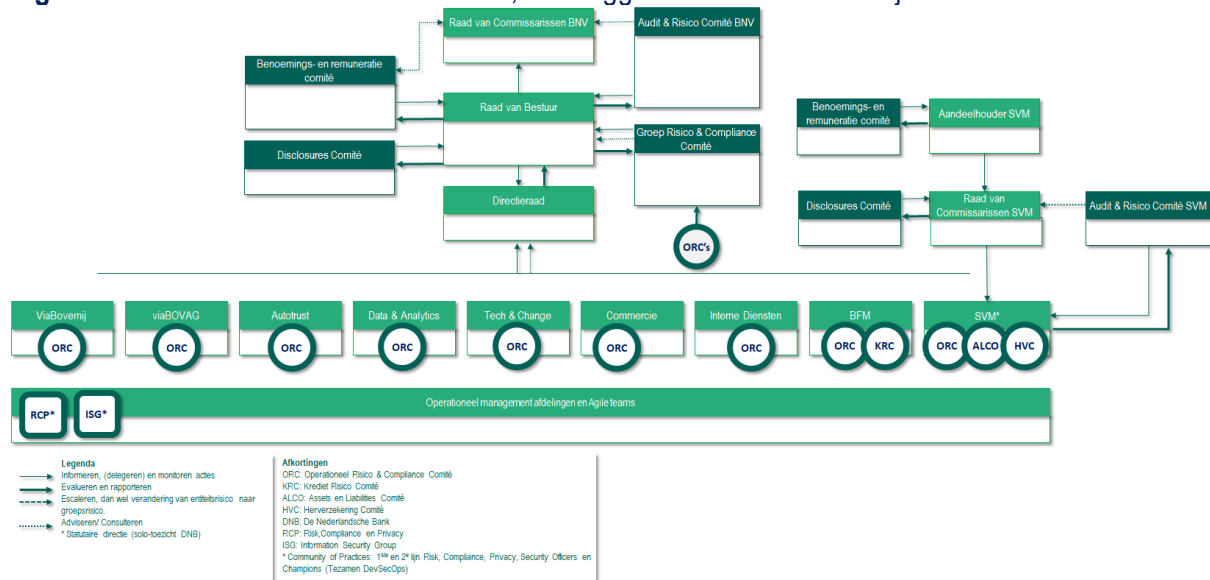
**Figur 6-3 Three Lines of Defence**



### 6.1.2 Risico Comités en communicatielijnen

Bovemij stelt risicocomités in met een duidelijk doel, taakomschrijving en samenstelling functionarissen in elk comité, standaarden<sup>15</sup> die zich tezamen richten op een integrale en beheerste bedrijfsvoering en hebben een signaleringfunctie. Ter ondersteuning van een doeltreffende toepassing van risicomanagement hanteert Bovemij voor communicatie en consultatie het de Nederlandse Corporate Governance, COSO ERM model in combinatie met de ISO31000 principes. Een dergelijke structuur van comités is weergegeven in onderstaand schema (figuur 6-4), waar de gelaagdheid van boven naar beneden laat zien welke lijn binnen de organisatie de eerste en tweede lijn moet volgen voor escalatie vanwege risico of verantwoordelijkheden moet worden besproken.

**Figuur 6-4** Overzicht van Risico comités, overleggen en communicatielijnen



Ook de toewijzing van verantwoordelijkheden, bevoegdheden en verplichtingen aan comités als onderdeel van het risicobeheersingsraamwerk is een belangrijke overweging. Samenstelling, rollen, verantwoordelijkheden, communicatie- en rapportagestructuren moeten worden beschreven binnen de taakomschrijving van elke commissie en gemeenschap. Tezamen draagt dit risicobeheersingsmodel voor Bovemij op een efficiënte wijze bij aan continue transparantie en vertrouwen geven aan toezichthouders en van de klanten.

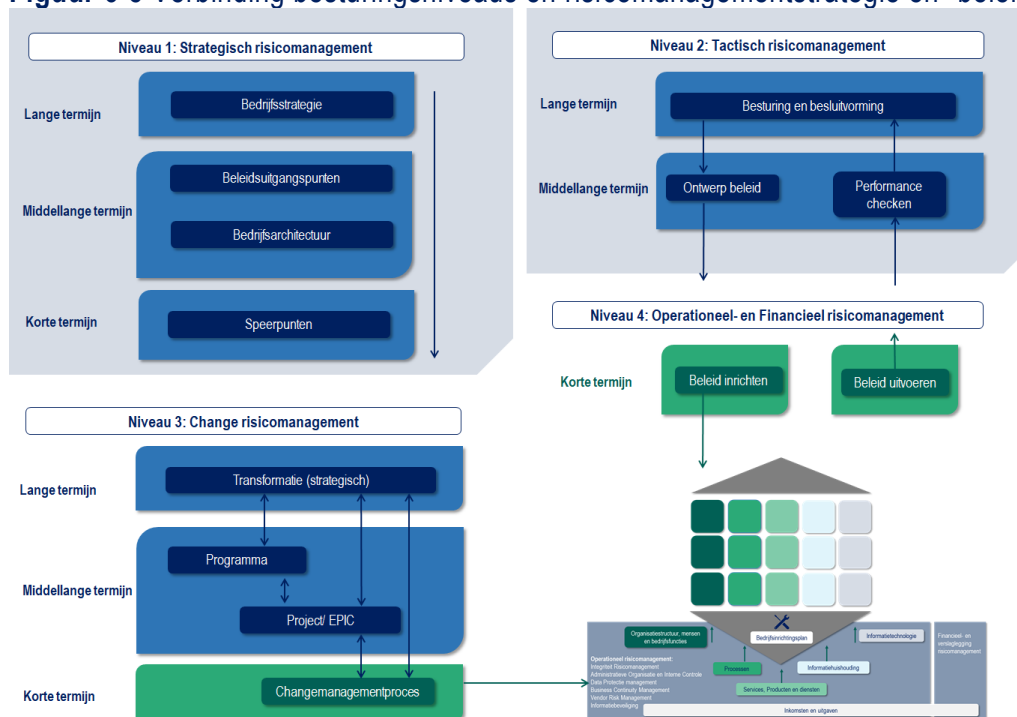
<sup>15</sup> Standaarden zijn als zodanig in paragraaf 6.4 van deze thesis beschreven.



## 6.2 Risicomanagement Strategie en -beleidskaders

Strategie en beleidskaders zorgen samen met een integrale toepassing van risicomanagement op de verschillende besturingsniveaus en dat de organisatie een effectieve en efficiënte risicomanagementfunctie kan bouwen (ontwerpen), onderhouden en controleren. Een belangrijk onderdeel van functionerend risicomanagement is de vereiste dat risicomanagement onderdeel is van strategische, verandermanagement-, tactische en operationele besluitvormingsprocessen, zoals weergegeven in figuur 6-5.

**Figuur 6-5** Verbinding besturingsniveaus en risicomanagementstrategie en -beleid



De directieraad (niveau 2) van Bovemij plant, ontwerpt, leidt en controleert beleidsactiviteiten in overeenstemming met de door (niveau 1) de Raad van Bestuur vastgestelde strategische richting en doelstellingen van het bedrijf. Governance zorgt binnen alle niveaus dat risicomanagement onderdeel is van bestuursregelingen, beleidskaders worden geïmplementeerd en dat risico-informatie en afwegingen worden meegenomen in de besluitvorming.

Om de strategie voor risicomanagement te bepalen, zal het bestuur van Bovemij belangrijke beslissingen moeten nemen met betrekking tot de risicobereidheid op het hoogste organisatieniveau. Risicobereidheid is namelijk gebaseerd op de bereidheid investeringen te doen in risico's, aanvaarding van beheersingsmaatregelen (risico's versus rendement) en de welwillendheid (tolerantie) van de organisatie om risico's te accepteren. Het is van belang dat de risicobereidheid valt binnen het feitelijke vermogen

(capaciteit in beschikbaar geld, middelen en mensen) van de hele organisatie. Het is ook belangrijk om te overwegen hoe (risicohouding) de totale inherente risicoblootstelling van de organisatie wordt gebruikt in de besluitvormingsprocessen op strategisch en tactisch niveau. Met andere woorden: risicobereidheid, risicoblootstelling, risicocapaciteit en risicohouding moeten worden beschouwd als onderdeel van beslissingen en of gevolg ervan, in plaats van de drijvende kracht achter die beslissingen. Hierbij is de samenhang met governance en risicomanagementarchitectuur van belang, waarbij gelet wordt op ethiek, houding en gedrag.

Zoals de resultaten uit de diagnose laten zien, schrijven organisatie vaak de strategische doelstellingen, bedrijfsdoelstellingen en het bedrijfsinrichtingsplan (bedrijfsmodel) als afzonderlijke documenten op. Terwijl de theoretische kaders voor de inrichting van een bedrijf juist wijst op de domeinen in samenhang te bezien (zoals in het Risicomanagementraamwerk Figuur 6-1). Wanneer het management van Bovemij aansluitend wil zorgen dat risicomanagement een volwaardige bijdrage levert aan de organisatiedoelstellingen, is het van belang ook de risicomanagementdoelstellingen in samenhang te bezien en frequent de relatie ertussen te onderzoeken. De risico's die aan de bedrijfsdoelstellingen zijn verbonden, houden namelijk verband met de robuustheid en efficiëntie van het bedrijfsmodel. Bijvoorbeeld, bij een risicoanalyse voor de jaarlijkse begroting zou ook gekeken moeten worden naar de risicofactoren die de inkomsten kunnen ondermijnen, zoals factoren die de levering van diensten en producten kunnen verstoren, waardoor een verminderde inkomstenstroom ontstaat.

### 6.3 Risicomanagementproces

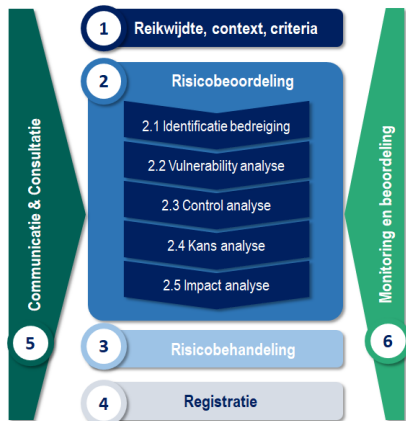
Het risicomanagementproces (figuur 6-6) voor Bovemij bestaat uit zes stappen voor een integrale en beheerste bedrijfsvoering. Het risicomanagementproces is onderdeel van de managementprocessen van Bovemij en van toepassing voor de vier besturingsniveaus zoals opgenomen in figuur 6-5. De basis van het proces bestaat uit de ISO31000 componenten en vanwege het typologie meezijdig platformbedrijf is stap 2.2. voor Bovemij toegevoegd<sup>16</sup>.

#### **Figuur 6-6** Ontwerp Risicomanagementproces Bovemij

---

<sup>16</sup> Overgenomen vanuit de theorie die Stoneburner et al. (2002) voor technologiebedrijven heeft uitgeschreven.

**Niveau 1:** Strategisch risicomanagement ofwel enterprise risicomanagement is verbonden met de



strategische doelstellingen van Bovemij. Op dit organisatieniveau is strategisch risicomanagement op Bovemij als groep en worden strategische doelstellingen afgesproken die voor alle entiteiten van toepassing zijn. Dit leidt tot het algehele risico universum en het risicoprofiel van Bovemij als meezijdig platformbedrijf. Binnen COSO ERM is dit het integraal risico overzicht genoemd.

**Niveau 2** Wanneer Bovemij tactisch risicomanagement toepast, betekent dit het implementeren van het risicomanagementproces

op niveau bedrijfsentiteit. Door het risicomanagementproces op tactisch niveau te implementeren en het lijnmanagement beleid opstelt, ondersteunt risicomanagement actief de realisatie van bedrijfsentiteit-/ afdelingsdoelstellingen. Daarnaast zullen beleidsdocumenten de risico's weergeven die door het specifieke beleid worden beheerd, inclusief risicotaxonomie, risicostrategie, risicobereidheid, tolerantie en capaciteit.

**Niveau 3:** Van change risicomanagement is sprake wanneer verandermanagement wordt toegepast. Bovemij zal het risicomanagementproces toepassen op de in figuur 6-5 weergegeven veranderniveaus: transformatie, programma en projecten/ EPIC<sup>17</sup>. Bij Bovemij zorgt het niveau transformatie dat een ingrijpende verandering van de organisatie plaatsvindt. Qua risicomanagement kan hierbij sprake zijn van interne en externe risicofactoren met een effect op de transformatiedoelstelling(en). Een programma zorgt binnen een specifiek aandachtsgebied dat de verandering gestructureerd wordt uitgevoerd. Bijvoorbeeld het inrichten van het technologieplatform en een programma voor het inrichten van de Agile organisatie. Hierbinnen zijn projecten/ EPIC's opgezet voor de deelproducten van de programma's. Programma- en projectdoelstellingen kunnen worden beïnvloedt door risicofactoren die zich manifesteren binnen één of meerdere programma's en of (in mindere mate) projecten binnen het programma. Het changemanagementproces valt onder de gestandaardiseerde operationele processen waarbinnen herhaaldelijk (iteratieve) wijzigingen worden aangebracht aan bedrijfsobjecten<sup>18</sup> (Assets). Hierdoor valt het changemanagementproces ook onder niveau 4.

<sup>17</sup> Volgens de theorie van Agile Safe. De toepassing hiervan is net gestart binnen Bovemij en wordt nog geïmplementeerd.

<sup>18</sup> Bedrijfsobjecten/ assets zijn: Organisatiestructuur, mensen, bedrijfsfuncties, processen, services, producten, diensten, informatiehuishouding en informatietechnologie.

**Niveau 4** Operationeel risicomanagement is voor Bovemij het beheersen van risico's die voor een verstoring van de (normale) dagelijkse (bedrijfs)activiteiten zorgen. In veel opzichten is het operationeel risico nauw verwant met componenten binnen de bedrijfsarchitectuur/-infrastructuur. Hoewel het om dezelfde soorten risico's gaat, onderscheiden operationele risico's in een financiële instelling zich door het feit dat deze risico's worden gekwantificeerd als potentiële financiële verliezen. Terwijl operationele risico's van een platformbedrijf bekend staan als kwalitatieve risico's. Daarom moeten financiële instellingen beschikken over voldoende kapitaalreserves zoals wettelijk vereist om bestand te zijn tegen (potentiële) financiële verliezen en voldoen aan de (contractuele) verplichtingen waarmee de instelling wordt geconfronteerd. Als wordt gesproken over financiële risico's dan worden veelal risicofactoren bedoeld die effect hebben op de wijze waarop geld wordt/is gemanaged en winstgevendheid bereikt.

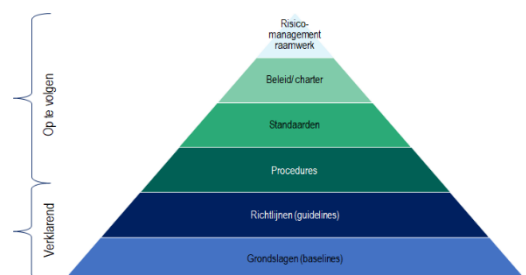
#### 6.4 Risicomanagementprotocollen

↑ Risicomanagementprotocollen: regels, en procedures, risicomanagementmethoden, -instrumenten, en -technieken ↑

De risicomanagementprotocollen beschrijven de reeks en reikwijdte van de activiteiten die worden uitgevoerd als onderdeel van risicomanagement. Protocollen omvatten (samengevat) de (beleids)regels, procedures, de activiteiten die uitgevoerd moeten worden, de wijze waarop en welke methoden, instrumenten en technieken toegepast moeten worden binnen de bedrijfsarchitectuur componenten en bedrijfsobjecten/ assets. Ook worden protocollen voor risicomanagement gedefinieerd als essentieel eerstelijns beleid, tweedelijnsbeleid,- en richtlijnen voor de organisatie dat beleidsregels en procedures bevat. Evenals risicomanagement-, instrumenten, -technieken en monitoringsmethoden die moeten worden gebruikt.

**Figuur 6-7** Gelaagdheid van bedrijfsbeleid

Het bedrijfsbeleid (beleidsregels) bestaat uit een gelaagdheid (figuur 6-7) bestaande uit verklarende en op te volgen interne regels. In elk beleidsdocument (groeps- of entiteitbeleid) zal moeten zijn aangegeven wat Bovemij of de entiteit wil bereiken op het gebied van risicomanagement binnen de specifieke beleidscontext (figuur 6-8). Hiermee zorgt Bovemij dat risicomanagement een integraal onderdeel is van het beleid wat wordt gevoerd.



Om risicomanagement volledig te kunnen verankeren binnen de bedrijfsarchitectuur componenten als:

**Figuur 6-8** Integratie risicomanagement binnen beleidsmanagementcyclus



organisatiestructuur, mensen, bedrijfsfuncties, processen, services, producten, diensten, informatiehuishouding en informatietechnologie van een organisatie, is een duidelijke verklaring van rechten en plichten inzake risicomanagement vereist. Dit behoort Bovemij te beschrijven in een zogenoemd charter. Bovendien moet Bovemij, als onderdeel van de analyse (binnen het risicomanagementproces) van elk significant risico, de verantwoordelijkheid voor het risico duidelijk worden toegewezen aan een eigenaar, zodat wordt voldaan aan de aspecten:

- Besluiten over de risicostrategie en ontwikkelen van standaarden voor de beheersing;
- toepassing van de overeengekomen standaarden en procedures; en
- toezien op de naleving van de overeengekomen standaarden.

Vanwege specifieke wet- en regelgeving waaraan bepaalde bedrijfsentiteiten van Bovemij moeten voldoen, moeten procedures en richtlijnen voor het beoordelen van risico's – behorende niveau 1 tot en met 4 - schriftelijk zijn vastgelegd. De organisatie dient eveneens procedures vast te stellen over de frequentie en inhoud van risicomanagementrapportages en wie verantwoordelijk is voor het verzamelen van deze informatie. Richtlijnen voor risicomanagement verwijzen gewoonlijk naar de normen die moeten worden aangehouden, in enkele gevallen zal voor bepaalde bedrijfsentiteiten meer details zijn opgenomen over de te nemen (verschillende type) maatregelen. Dit geldt vooral voor richtsnoeren die beschrijven welke procedures moeten zijn toegepast. Deze procedures zullen richtinggevend zijn voor directeuren, managers en personeel binnen de organisatie.

Een belangrijke overweging voor een risico-escalatieprocedure is de noodzaak van een consistente reactie op risico's, waaronder wanneer zich een nieuw risico voordoet of bestaande risico's ingrijpend veranderen. In die omstandigheden zal Bovemij een escalatieprocedure moeten toepassen, zodat de gewijzigde

**Figuur 6-9** Principes binnen het risicomanagementraamwerk

omstandigheden door het hogere management worden bekeken. Het ontwerpen en invoeren van deugdelijke escalatieprocedures voor risico's behoort plaats te vinden met passende training om deze functionerend te krijgen.

### 6.5 Principes

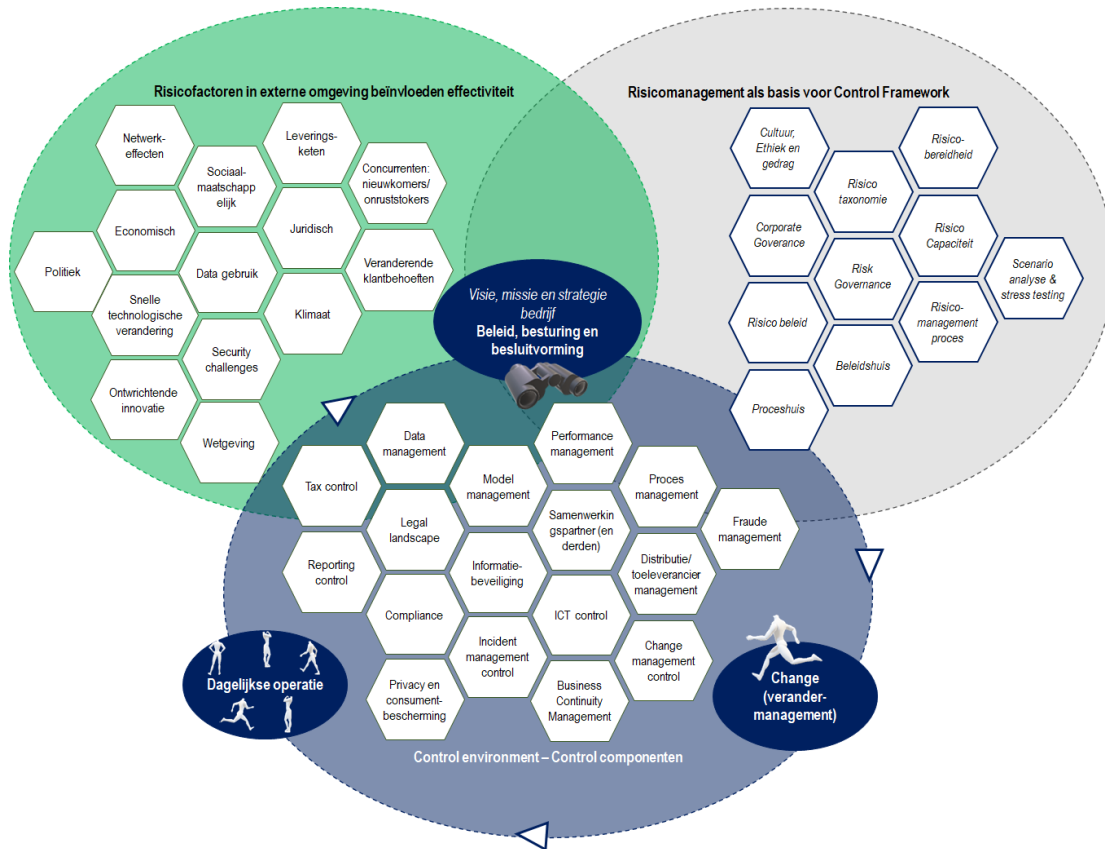
Het voornaamste uitgangspunt (principe) voor risicomanagement is dat het waarde creëert voor de organisatie. Geen enkele organisatie heeft een eindige lijst van beleid, maatregelen en dergelijke voor het beheersen van risico's. Het is daarom van belang dat in afwezigheid of bij het uitblijven van beleidskaders, maatregelen altijd worden uitgevoerd binnen de beleidsprincipes. Binnen het risicomanagementtraamwerk zijn vier soorten principes voorgesteld: Governance, Risicomanagement, Compliance en In Control. De principes zijn uitgeschreven in figuur 6-9.

<p><b>'Governance'</b>  <i>Inspelen op de behoeften van belanghebbenden</i></p> <p><i>Geschiede en tijdige betrokkenheid van belanghebbenden maakt het mogelijk kennis, meningen en percepties in aanmerking te nemen.</i></p> <p><i>Bestrijkt de onderneming end-to-end</i></p> <p><i>Bevordert een holistische aanpak</i></p> <p><i>Besturen van de organisatie is altijd gescheiden van management.</i></p>	<p><b>'Compliance'</b>  <i>Zorgt voor een integriteitsbewuste bedrijfscultuur.</i></p> <p><i>Integer gedrag is stevig verankerd op organisatorisch en individueel niveau.</i></p> <p><i>Zorgt voor een bedrijfscultuur waar op transparante wijze wordt gecommuniceerd over doelstellingen.</i></p> <p><i>Realistische doelstellingen worden gesteld zonder perverse prikkels.</i></p> <p><i>Zorgt dat verantwoordelijkheid wordt genomen en verantwoording wordt afgelegd.</i></p>
<p><b>'Risicomanagement'</b>  <i>Zorgt dat de organisatie doelstellingen worden bereikt en creëert waarde.</i></p> <p><i>Is geïntegreerd en beheerst risico's binnen alle bedrijfsarchitecturale componenten.</i></p> <p><i>Is gestandaardiseerd toegepast en is tenminste afgestemd op de noodzakelijke kaders en normen voor risicomanagement.</i></p> <p><i>Is gestructureerd en veelomvattend waardoor een holistische en systematische benadering van risico's mogelijk is.</i></p> <p><i>Is dynamisch naarmate de interne en externe context van de organisatie verandert.</i></p>	<p><b>'In Control'</b>  <i>zorgt dat doelstellingen worden gerealiseerd als bedrijf, betrouwbare verslaggeving en naleving van wet- en regelgeving.</i></p> <p><i>'In Control' blijven is een proces met een begin en eind als middel om doelen te realiseren, geen doel op zich.</i></p> <p><i>'In Control' zijn stelt de organisatie in staat om redelijke, geen absolute, zekerheid te verschaffen.</i></p> <p><i>De inrichting van het Control Framework van bij de aard, omvang en complexiteit</i></p>

### 6.6 Functionerend RM – Bovemij Control Framework

Het Bovemij Control Framework (BCF), zoals weergegeven in figuur 6-10, is het risicobeheersingssysteem van de organisatie en maakt vanwege de manier waarop het werkt onderdeel uit van het risicomanagementtraamwerk. Het BCF houdt zich bezig met het functioneren van beleid, de methoden, procedures en controles die binnen Bovemij nodig zijn om ervoor te zorgen dat Bovemij haar (beheersings)doelstellingen bereikt en voldoet aan de wet- en regelgeving waar de verschillende entiteiten mee te maken hebben. Het doel van het BCF is om bestuurders en directieleden in staat te stellen de organisatie met vertrouwen vooruit te sturen, door goede en slechte tijden. Een ander doel van het BCF is het beschermen van de middelen van Bovemij en het waarborgen van de toereikendheid, adequaatheid van administraties en verantwoordingssystemen te waarborgen. Met andere woorden, kan het BCF worden gezien als de maatregelen die worden ondernomen door RvB, directie en operationeel management om de toereikendheid (effectiviteit) van risicomanagementactiviteiten te plannen, organiseren en sturen teneinde redelijke zekerheid te bieden dat de doelstellingen zullen worden bereikt. Het BCF is hiermee het "middel" (Enabler) die zorgt voor structuur, duidelijkheid over verantwoordelijkheden en eigenaarschap, zodat Bovemij sturing kan geven en transparant kan zijn over haar daadwerkelijke risicobeheersing (In control).

**Figuur 6-10** Bovemij Control Framework





## 6.7 Validatie van het ontwerp en bruikbaarheid

Over het algemeen is een onderzoeksresultaat geldig wanneer is bewezen op welke wijze het tot stand is gekomen. De wijze waarop het tot stand is gekomen moet redenen geven om aan te nemen dat het onderzoeksresultaat juist of toereikend is (van Aken & Berends, 2018). Voor de toepassing geven van Aken & Berends (2018) drie verschillende type validatie: Construct-, interne-, en externe validatie. Construct validatie viel voor dit onderzoek af doordat het voorziet in een validatie op het meten van de effecten bij de operationalisering van een ontwerp. De interne validatie viel af doordat het conclusies betreft over de relatie tussen verschijnselen die bestaan binnen de grenzen van het bestudeerde systeem. Externe validiteit verwijst naar de generaliseerbaarheid of overdraagbaarheid van onderzoeksresultaten en conclusies naar situaties, mensen, organisaties en landen buiten de grenzen van het beschouwde systeem. Externe validiteit is van belang bij theoriegericht onderzoek en focust op een specifiek probleem in een specifieke organisatie. De structuur van het risicomanagementwerk zou door andere meezijdig platformbedrijven wellicht gebruikt kunnen worden. Echter, zal met name de specifieke inhoud vooral toepasbaar zijn in de reële omgeving van Bovemij. Ondanks dat de cases zijn gekozen op basis van theoretische gronden had validiteit verder verhoogd kunnen worden indien meer andere equivalente cases waren onderzocht.

Op verschillende momenten zijn de kaders voor het ontwerp en de inhoud van het ontwerp besproken met stakeholders van Bovemij. Op drie momenten is het ontwerp expliciet doorgesproken en op andere momenten is het ontwerp in zogenoemde periodiek overleggen met directieleden en bestuursleden besproken. De mapping-technieken die tijdens het onderzoek zijn gehanteerd als validatietechniek waren erop gericht om de cognitieve representaties die mensen in hun hoofd hebben over het onderwerp risicomanagement, te eliciteren (naar buiten brengen) en in kaart te brengen (Homan, 2006). Zo worden onzichtbare *cognitieve maps* van het individu omgezet naar zichtbare *cause maps* (Homan, 2006). Deze mapping-techniek is gehanteerd voor Bovemij doordat *maps* in staat zijn om *the real thing* (datgene dat iemand denkt) adequaat visueel te kunnen representeren (Homan, 2006). Zodoende bestaat ook het risicomanagementtraamwerk voornamelijk uit afbeeldingen en een zeer beperkte hoeveelheid tekst wat weer aansluit op *sense makings* van het management. De elicitering is een sociaal proces dat vermoedelijk is beïnvloed door persoonlijke behoefte van de bevroagde personen. Een punt van kritiek op deze techniek is dat in de meeste gevallen het uiteindelijk toch de onderzoeker is die de *cause maps* feitelijk vormgeeft. Hierdoor bestaat het risico dat de onderzoeker de betekenis van woorden invult in de uitingen van de bevroagde mensen. Om dit risico enigszins te mitigeren is daarom gekozen om zowel mensen van de community (risicomanagement, compliance en privacy) te bevroagen en de gebruikers.



Op 6 december 2021 zijn de initiële kaders voor het ontwerp besproken. Bij de stakeholders in eerste instantie feedback verkregen op het conceptuele model in verband met de bruikbaarheid ervan en vervolgens is hen verzocht eventuele knelpunten voor implementatie aan te dragen. Samen met de stakeholders is vervolgens een soort van ontdekkingstocht gehouden waarin de kaders zijn doorgesproken en (on)bewuste business requirements voor de inhoud expliciet zijn gemaakt. Omdat niet iedereen de gelegenheid had om aanwezig te zijn is aanvullend, in zogenoemde Bilateralen, de behoeften opgehaald. Wat tijdens de gesprekken opviel is het gebruik van de woorden “Control Framework” en een “benodigde governance”. Een andere zoektocht op inhoud – voornamelijk tijdens gesprekken - was de toepasbaarheid op zowel Bovemij als Groep als op de onderliggende bedrijfsentiteiten.

Het concept raamwerk is ingebracht binnen het Risk, Compliance en Privacy overleg (d.d. 14-12-2021) en doorgesproken. De verschillende componenten van de het raamwerk zijn n.a.v. de opmerkingen in dit gezamenlijke overleg nog eens met de individuen doorgesproken om de details van de feedback goed te begrijpen en te kunnen doorvragen. Zodoende is bijvoorbeeld het risicoprofiel aangescherpt met de integriteit thema’s die voor compliance doeleinden worden gehanteerd. En is op basis van de terugkoppeling van de 1<sup>ste</sup> lijn Risk & Compliance Officer alleen de risicotaxonomie in het raamwerk opgenomen zonder de risicoclassificatie wat tezamen het risicoprofiel zou vormen. Naderhand is schriftelijk nog feedback en input ontvangen vanuit de verschillende stakeholders (waaronder de CFRO) voor onderdelen van het raamwerk om het nog concreter te kunnen invullen voor Bovemij specifiek.

Het concept raamwerk is gepresenteerd aan de directieleden binnen het opdrachtgeversoverleg d.d. 20-12-2021. Binnen dit overleg waren de (potentiële) eindgebruikers van het risicomanagementraamwerk aanwezig. Uit dit overleg hebben twee directieleden (van BFM en viaBovemij) verzocht om het risicomanagementraamwerk in verder detail toe te lichten. Hieruit is verder geen feedback of inhoudelijke verbeterpunten ontvangen, wat op zich wel aansluit met de lage volwassenheid van de organisatie en deze is nog vrij laag.

Verder is men positief over de contouren van het risicomanagementraamwerk en zijn er nog zorgen over de operationalisering van het raamwerk en niet eens zozeer de bruikbaarheid van het raamwerk. Binnen het GRC Comité is gesproken over de uitdagingen die er zijn over de capaciteit in aantal mensen voor de uitvoer en benodigde capaciteit uitgedrukt in benodigde kennis en kunde. Een ander discussiepunt is de integratie van raamwerkcomponenten binnen Business Procesmanagement en het huidige ICT-legacy

systeem. Op dit moment heeft Bovemij de basis nog niet op orde, in het verleden nauwelijks procesmatig gewerkt en zijn legacy systemen ontstaan. Ook zal het inrichten binnen de ICT met name uitvoerend werk zijn, waarvoor een van de bestuursleden transparant aangeeft dat op de capaciteit (in aantal FTE, kennis en kunde) ontbreekt. Ook is gesproken over het lage risico-bewustzijn van directieleden en management, die zich nog onvoldoende beseffen dat risicomanagement onderdeel is van de organisatieperformance en daarmee onderdeel van hun verantwoordelijkheden. In het verleden is immers nauwelijks tot geen aandacht geweest voor risicomanagement, waardoor de verwachting is dat een top-down-benadering nodig is qua communicatie en benadrukken de leden het belang van de rol van directieleden en management.

*De notulen (verslagen) zijn geen onderdeel van deze thesis omdat dit vertrouwelijke bedrijfsinformatie bevat, inclusief bestuursbesluiten. Hetgeen in dit paragraaf beschreven is een samenvatting van de voor deze thesis relevante opmerkingen.*

## **7 Conclusie, aanbeveling en discussie**

Deze thesis eindigt met hoofdstuk 7, waarin conclusies worden getrokken en bediscussieerd in de beantwoording van de hoofdvraag: *Hoe ziet een functionerend risicomanagementraamwerk eruit voor Bovemij als meezijdig platformbedrijf?* Door het doen van literatuuronderzoek en de diagnose is informatie verzameld om deze hoofdvraag te beantwoorden.

### **7.1 Conclusie**

Bij het beantwoorden van de onderzoeksvragen 1a en 1b van het literatuuronderzoek lijkt er veel aandacht te zijn voor verschillende op zichzelf staande risicomanagementgebieden en verschillende type bedrijfsmodellen voor een meezijdig platformbedrijf, of voor de specifieke (type) risico's van een meezijdig platformbedrijf. Dit kan worden gesuggereerd alsof er nog nooit is nagedacht over een specifiek risicomanagementraamwerk voor een meezijdig platformbedrijf. Alle literatuur tezamen vormen de basis kaders voor een risicomanagementraamwerk.

Wat betreft de risicofactoren (deelvraag 2b) die volgens de theorie vaak voorkomen bij platformbedrijven, kunnen ze worden onderverdeeld in COSO ERM-categorieën: strategisch, financieel, operationeel en compliance. Typische risicofactoren die vaak optreden zijn software- en informatierisico's, zoals cybersecurityrisico's. Ook zijn er risicofactoren die samenhangen met de rol van de onderneming in de

keten, bijvoorbeeld ten aanzien van leveranciers (continuïteit), concurrenten en juridische consequenties. En natuurlijk zijn er intrinsieke interne risico's, dat de mensen betreft (fouten maken).

De basis van het risicomanagementraamwerk is afkomstig van COSO ERM, ISO 31000 en de Fundamentals of Risk Management. Het valt nog te bezien of dit een "kansrijk" raamwerk is (deelvraag 3a). Maar de hele organisatie, dat wil zeggen alle bedrijfsentiteiten van de groep, kan ervan profiteren, ondanks dat de typen entiteiten verschillen. Met de concrete invulling van het risicomanagementraamwerk werd tegemoetgekomen aan de specifieke behoeften van Bovemij vanuit de basisgedachte waarbij verschillende bedrijfsentiteiten diensten, producten en/of diensten leveren aan het bedrijf van het meezijdig platformbedrijf (via Bovemij en via Bovag). Hierdoor kunnen verschillende entiteiten een basisbeleid voor risicomanagement ontwikkelen en organiseren dat past bij het specifieke bedrijfstype, de omvang, de complexiteit en risico's van de organisatie. Of dit ook zal leiden tot een functionerend raamwerk is afhankelijk of dat risicomanagement kan bijdragen aan de realisatie van doelstellingen en functionarissen zoals RvB, directie en management de toegevoegde waarde ervan willen dan wel kunnen ervaren. Minstens zo belangrijk is de mate waarin de risicomanagementgedachte wordt uitgedragen binnen de organisatie en als het ware wordt geadopteerd door de verschillende functionarissen en stakeholders binnen de organisatie. In zowel de literatuur als de diagnose van het onderzoek begint de behoefte aan het hebben van functionerend risicomanagement in samenhang met het bedrijf binnen de digitale economie steeds op te doemen. Achter deze trend lijkt een fundamentele behoefte aanwezig te zijn op grip te krijgen en houden (in control) op gebeurtenissen die zowel binnen als buiten de organisatie kunnen plaatsvinden. In tegenstelling tot een bedrijf als Bovemij dat nationaal opereert, lopen de onderzochte bedrijven allemaal verschillende risico's op nationaal, internationaal en op alle niveaus van de organisatie. Wat daarbij opvalt is de noodzaak om risicomanagement in te zetten in relatie tot innovatiedoelstellingen en de noodzaak om voor toezichthouders transparant te zijn over de effectiviteit van governance, compliance en risicomanagement.

(Deelvraag 3b) Per definitie behoort het voorgestelde risicomanagementraamwerk als een leidraad, kaders, overzicht van onderling samenhangende items (activiteiten) om een aanpak voor het bereiken van een specifiek doel te faciliteren. In deze context voor Bovemij hoort het risicomanagementraamwerk ook de implementatie van risicomanagement en de transformatie te ondersteunen. Het doet dit door te helpen bij het organiseren en structureren van een praktische aanpak die zowel meetbaar als herhaalbaar is. Het ontwerp risicomanagementraamwerk voor Bovemij heeft nu met name het doel om de basis voor risicomanagement op orde te krijgen en het beheerst functioneren van de verschillende bedrijfs-/

architecturale componenten te borgen. Een risicomanagementraamwerk is daarom nog voornamelijk een organisatorisch specifieke set van kaders, functionele activiteiten en de bijbehorende definities die het risicomanagementsysteem voor de organisatie definiëren en zal in de komende jaren nog evolueren. De juiste ondersteuning van de Bovemij organisatie bij de implementatie kan ervoor zorgen dat de mensen in organisatie het gevoel gaan krijgen weer grip op hun verantwoordelijkheden te krijgen.

(Deelvraag 4) Een risicomanagementraamwerk, met inbegrip van de verschillende componenten, kan worden gezien als zogenoemd structureel of standaard werk, waarbij de basisvereisten om het hoofd te bieden aan de meeste weersomstandigheden die hetzelfde zijn. De basis voor een risicomanagementraamwerk kan voor elke organisatie hetzelfde zijn, ongeacht de omvang en/of complexiteit van de organisatie. Zo kan er een genuanceerd verschil zijn de gebruikte terminologie of een verschil in het aantal stappen in het risicomanagementproces. Het primaire resultaat dat een risicomanagementwerk moet opleveren is het begrijpen van de risico's die aan de organisatie zijn verbonden, het maken van keuzes met betrekking tot risicostrategieën of -beheersingsmaatregelen en het volledig integreren van risicomanagement in de organisatie. Anderzijds omvat de implementatie van het risicomanagementraamwerk de specifieke kenmerken van de onderneming waarvoor het raamwerk zal worden gebruikt.

## 7.2 Aanbevelingen

Vanwege het probleem van het ontwerpen en verkrijgen van een functioneel raamwerk, bevat dit hoofdstuk aanbevelingen voor de implementatie van het raamwerk op korte en middellange termijn.

1a) **Van risicomanagement training en communicatie naar een risicocultuur.** De organisatie heeft een gemeenschappelijke risicotaal nodig om haar raamwerk voor risicomanagement te kunnen ondersteunen en onderhouden en om mee te kunnen evolueren met de transformatie die Bovemij doormaakt. Dit vereist training en communicatie over de meest basale en fundamentele onderwerpen om risicomanagement en governance toe te passen (risicomanagementarchitectuur). Iedereen in de organisatie heeft ook een rol in het vergroten van de kans op succes en dus functioneren van het raamwerk. Net als Bovemij hebben de meeste organisaties meerdere lagen (bijvoorbeeld leidinggevend, lijnmanagers en werknemers) en 'silo's', zoals entiteiten. Er is een gemeenschappelijke taal nodig om klassen en silo's te doorbreken. Omgekeerd, zonder een gemeenschappelijke taal, zal het risicomanagementteam te veel tijd besteden aan het behandelen van communicatieproblemen tegen een ten kosten van hun primaire verantwoordelijkheden.

**1b) Transformeren naar een platformbedrijf inclusief een cultuur waar risicomanagement onderdeel van is.** Zoals in meerdere marktstandaarden voor risicomanagement naar voren komt is het belangrijk risicomanagement te verankeren binnen de cultuur. Deze aanbeveling is gebaseerd op de theorieën van Kotter, (2019) over leiderschap bij verandering. Wanneer binnen de transformatie bij Bovemij nieuwe risicomanagementpraktijken met behulp van het risicomanagementraamwerk niet te verenigen zijn met de relevante, dan wel beoogde cultuur zal deze altijd aan regressie onderhevig zijn. Volgens Kotter, (2019) heeft cultuur namelijk betrekking op gedragsnormen en gedeelde waarden in een groep mensen die moeilijk zijn te veranderen. Het succes van het risicomanagementraamwerk zal daarom mogelijk afhangen van de afstemming op de beoogde cultuur voor Bovemij als platformbedrijf en hoe goed de medewerkers in staat zijn om zich hieraan aan te passen. Dit betekent volgens Kotter, (2019) dat de cultuur van de organisatie, inclusief risicomanagement, pas verandert nadat met succes de handelingen van mensen veranderd zijn, nadat het nieuwe gedrag voor de groep een bepaalde periode lang voordeel heeft opgeleverd en pas als mensen het verband zien tussen de nieuwe handelingen en de verbetering van de prestaties. Dit betekent concreet dat het gevoel voor risicomanagement binnen de cultuur niet in de eerste fasen van een transformatie van essentieel belang is. Het is aan te bevelen om in de eerste fasen van de transformatie te proberen om de gewoonten te veranderen en teamwerk te bevorderen met behulp van een leidende coalitie. Dit vereist volgens Kotter, (2019) echter wel veel praten: zonder mondelinge instructie en ondersteuning zijn mensen vaak niet bereid om de geldigheid van nieuwe praktijken toe te geven (wat weer aansluit met aanbeveling 1a).

**2a) Radicaal implementeren risicomanagementraamwerk.** Het onderzoek richtte zich op het ontwikkelen van een risicomanagementraamwerk voor een meezijdig platformbedrijf om Bovemij te ondersteunen. Hierbij richt het zich op de integratie en afstemming op Bovemij specifieke kenmerken, waarbij het nu nog voor een groot deel een methodologie van kaders is voor het systematisch kunnen inrichten. Hierdoor is de specifieke inhoud nog in minder mate aanwezig. Daarom is het advies om de kaders radicaal te implementeren en de inhoud incrementeel te laten ontstaan tijdens de transformatie waar Bovemij in de komende 3 tot 4 jaar nog in zit. Dit betekent dat de organisatie het beste ervoor kan zorgen dat de kaders voor het managen van risico's duidelijk worden begrepen en zo snel mogelijk in de praktijk worden gebracht. Dat de van toepassing zijnde besluitvormingsprocessen waar nodig worden aangepast en te identificeren waar, wanneer, door wie ("key players") en hoe verschillende risicomanagement gerelateerde besluiten binnen de organisatie genomen mogen worden.

**2b) Inhoud risicomanagementraamwerk binnen lange termijn incrementeel laten veranderen.** De context van een organisatie kan gedurende de tijd veranderen. Daar waar het risicomanagement het ene moment effectief kan zijn, kan door de tijd heen het functioneren van een risicomanagementraamwerk verminderen. Om het functioneren van een risicomanagementraamwerk vast te stellen is het advies om het functioneren van het risicomanagementraamwerk periodiek te evalueren aan de hand van:

- Het periodiek meten van de prestaties aan de hand van de doelstellingen, implementatieplannen, Key Performance Indicatoren en het verwachte gedrag.
- Periodiek vaststellen of het raamwerk geschikt blijft om het bereiken van de organisatiedoelstellingen en transformatie te ondersteunen.
- Periodiek vaststellen van interne en externe veranderingen.
- Periodiek vaststellen van de geschiktheid, toereikendheid, doeltreffendheid en doelmatigheid van het risicomanagementraamwerk.

**3) Volgende versie raamwerk baseren op intelligente (artificiële intelligentie) en geautomatiseerde bedrijfsproces.** Het ontwerp risicomanagementraamwerk voor Bovemij heeft nu nog met name het doel om de basis voor risicomanagement op orde te krijgen en het functioneren van de verschillende bedrijfsprocessen en middelen te borgen. Doordat bedrijfsmodellen van een platformbedrijf zijn gebaseerd op intelligente processen en geautomatiseerde processen, zijn wendbaarder, kunnen hierdoor sneller reageren en efficiënter werken voor de (digitale) klantervaringen. Hierdoor zullen de kaders en zal de inhoud van het huidig voorgestelde risicomanagementraamwerk voor Bovemij zich in de nabije toekomst nog veel meer moeten richten op:

- de ondersteuning en ontwikkeling van klantervaringen en waardecreatie (inclusief vraag en aanbod);
- het gebruik van nieuwe, beschikbare en integere technologieën om kosten te besparen (inclusief voorkomen van legacy systemen waar hoge investeringskosten aan zijn verbonden en de security te borgen) en kwaliteit (incrementeel) te blijven verbeteren;
- op het gebruiken van “artificial intelligence”, big data en geavanceerde analysemogelijkheden in het voorspellen van risico’s, meten van de risicomanagementvolwassenheid van bedrijfscomponenten, meten van (key performance en -risico) prestaties (indicatoren), het functioneren van digitale/ geautomatiseerde processen en effectieve meting van financiële risico’s omwille van het bedrijfskapitaal.

De precieze invulling hiervan zal nog wel vervolgonderzoek en analyse behoeven.

## 8 Reflectie

### “Get my head around it”

Het begin met het opstellen van het onderzoeksvoorstel ging vrij snel van start. Daarna ervaaarde ik wat opstartproblemen met het opstellen van de hoofdvraag en deelvragen. Wat wilde ik nou eigenlijk weten en wat is nodig om te weten zodat een antwoord gegeven kan worden op de hoofdvraag. Ditzelfde gebeurde ook weer met het literatuuronderzoek. Snel van start willen gaan en vervolgens vastlopen omdat ik nog onvoldoende de kaders waarin ik wilde en moest werken duidelijk had in mijn hoofd.

### “Check, check, dubbel check”

Gedurende het onderzoek veelvuldig en regelmatig de bestaande theorieën, consistentie toepassing, rode draad theorie versus praktijk, typo's en zinsconstructies gecondoleerd. Merkte dat door snelheid te willen maken ik stappen oversloeg in het onderzoek – snelle halen thuis. Hierdoor sloten theoretische resultaten, praktijkresultaten, analyse en conclusies niet (meer) op elkaar aan. Om een voorbeeld te noemen heb ik de theorie uit de literatuur binnen de foutieve hoofdstukken, theoretische kaders, geplaatst waardoor achteraf de theorie onlogisch was ten opzichte van de te onderzoeken aandachtsgebieden tijdens het caseonderzoek. Verder moest ik case 1 volledig opnieuw moeten uitvoeren omdat ik elementen gewoon niet had gezien om snel de informatie inventarisatie af te kunnen ronden.

### Kunst van afmaken wat je bent gestart

Te veel tegelijk doen zorgde tijdens het onderzoek dat ik open eindjes voor mezelf creëerde, niks volledig afronden. Dit maakte het onderzoeksproces inefficiënt en moest ik veel tijd stoppen in het opnieuw weer in de materie duiken. Een aantal van de oorzaken is het moeilijk kunnen concentreren, te veel aan mijn hoofd hebben en moeten balanceren tussen tijd voor privétiyd, werk, studie, vrienden, familie en hobby's.

### Vastlopen

Gaandeweg het literatuur liep ik met regelmaat vast in mijn hoofd, doordat ik in mijn hoofd vooral moest voldoen aan alle regels voor het uitvoeren onderzoek. Dit zorgde er onder meer voor dat ik veelvuldige dagenlang bezig ben geweest om de bronnen achter de bronnen te achterhalen totdat ik bij de eerste bron was. Tijdens Het literatuuronderzoek heeft de angst voor het vergeten van een ervoor gezorgd dat ik mij niet meer kon concentreren, mijn nekspieren volledig verkrampten en een vorm van “writers block” creëerde. Om hieruit te komen heb ik ervoor gekozen om tussentijds te gaan exploreren en bewust even van alles door elkaar uitvoeren. Ook de hond heeft zijn voetzolen versleten door het vele wandelen.



### **Omgaan met tegenslagen - Laat het verleden je toekomst niet beheersen**

Na een aantal maanden uitstelgedrag om contact op te nemen met mijn thesisbegeleider, weer nieuwe moed en vertrouwen gekregen. Wat je ook aan tegenslagen hebt ervaren en je persoonlijke doelen ook zijn, het is een

proces om ergens waar je wil zijn te komen, en om door te gaan. Het proces loopt niet altijd volgens een vaste of rechte lijn en al helemaal niet in dezelfde richting. Tussentijds heb ik mijn mindset veranderd van:

- "Ik heb geprobeerd om voorbij het punt te komen dat ik niet meer aan mezelf hoef te twijfelen, waarom zou het dit keer anders zijn", naar:
- "Oké, het gaat even minder, maar ik leer enorm veel nieuwe dingen, leer van nieuwe ervaringen en ik word daarmee steeds sterker".

## 9 Literatuurlijst

- 't Hart, R. (z.d.). *Nieuwe COSO 2017 - uitwerking principes rondom strategie en doelen bepalen*. Geraadpleegd 14 december 2019, van <https://robertthart.risicomanagement.nl/2018/04/23/nieuwe-coso-2017-uitwerking-principes-rondom-strategie-en-doelen-bepalen/>
- Abdelkafi, N., Raasch, C., Roth, A., & Srinivasan, R. (2019). Multi-sided platforms. *Electronic Markets*, 553–559. <https://doi.org/10.1007/s12525-019-00385-4>
- Alphabet Inc. (2019). *Alphabet Inc.*
- Alt, R., & Zimmermann, H. D. (2014). Editorial 24/3: Electronic Markets and general research. *Electronic Markets*, 24(3), 161–164. <https://doi.org/10.1007/s12525-014-0163-9>
- Alt, R., & Zimmermann, H. D. (2019). Electronic Markets on platform competition. In *Electronic Markets* (Vol. 29, Nummer 2, pp. 143–149). <https://doi.org/10.1007/s12525-019-00353-y>
- Amazon.com Inc. (2021). *audit Committee Charter*. <https://ir.aboutamazon.com/corporate-governance/documents-and-charters/audit-committee/default.aspx>
- Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering and System Safety*, 96(7), 719–726. <https://doi.org/10.1016/j.ress.2010.12.020>
- Aven, T. (2012). Foundational Issues in Risk Assessment and Risk Management. *Risk Analysis*, 32(10), 1647–1656. <https://doi.org/10.1111/j.1539-6924.2012.01798.x>
- Baldwin, C. Y., & Woodard, C. J. (2009). The architecture of platforms a unified view. In A. Gawer (Red.), *Platforms, Markets and Innovation* (pp. 19–36). Imperial College Business School. [https://books.google.nl/books?hl=nl&lr=&id=1BvhQT8SHZkC&oi=fnd&pg=PA19&dq=Baldwin,+C.Y.,+%26Woodard,+C.+J.+\(2009\).+The+architecture+of+platforms:+A+unified+view.+In+A.+Gawer+\(Ed.\),+Platforms,+markets+and+innovation+\(pp.+19-44\).+Edward+Elgar:+Cheltenham,+UK](https://books.google.nl/books?hl=nl&lr=&id=1BvhQT8SHZkC&oi=fnd&pg=PA19&dq=Baldwin,+C.Y.,+%26Woodard,+C.+J.+(2009).+The+architecture+of+platforms:+A+unified+view.+In+A.+Gawer+(Ed.),+Platforms,+markets+and+innovation+(pp.+19-44).+Edward+Elgar:+Cheltenham,+UK)
- Bayens, G., & Tönissen, H. (2015). *Bedrijfsarchitectuur op basis van Novius Architectuur Methode; Werken aan een samenhangende bedrijfsinrichting*. Van Haren Publishing.
- Bosch, F. Van Den. (1997). Wat is strategie: zoeken naar unieke resources voor het scheppen van een unieke value chain configuratie. *Nijenrode management review*, nr 6, 37–43. <https://repub.eur.nl/pub/11041/>.
- Bovemij N.V. (2020). *Transformatieplan versie 0.9 (vertrouwelijk)*.
- Bovemij N.V. (2021). *Strategisch bedrijfsplan 2021-2022*.
- Bradford. (2019). Understanding digital platform strategies: Steps toward maintaining a cohesive and competitive business in our online world. *Strategic Direction - Emerald Publishing Limited*, 35(4), 34–36. <https://doi.org/10.1108/SD-01-2019-0001>
- Brunner, M., & Wolfartsberger, J. (2020). Virtual Reality enriched Business Model Canvas Building Blocks

- for enhancing Customer Retention. *Procedia Manufacturing*, 42(2019), 154–157. <https://doi.org/10.1016/j.promfg.2020.02.062>
- CBS. (2020). *Autopark groeit sterker dan bevolking*. <https://www.cbs.nl/nl-nl/nieuws/2020/10/autopark-groeit-sterker-dan-bevolking>
- CBS. (2021). *Centraal Bureau Statistiek: Meer zicht op online platformen in Nederland*. <https://www.cbs.nl/nl-nl/corporate/2020/37/meer-zicht-op-online-platformen-in-nederland>
- Claassen, U. (2009). *Handboek risicomanagement*. Vakmedianet.
- COSO. (2013). *Internal Control - Integrated Framework - Committee of Sponsoring Organizations of the Treadway Commission*. May, 1–20.
- COSO. (2017). *Enterprise Risk Management Integrating with strategy and performance -The Committee of Sponsoring Organizations of the Treadway Commission*. June, 16. <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>
- Davies, H., & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *global Policy*, 9(1), 34–42. <https://doi.org/10.1111/1758-5899.12568>
- De Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: A research agenda. In *Journal of Information Technology* (Vol. 33, Nummer 2, pp. 124–135). <https://doi.org/10.1057/s41265-016-0033-3>
- den Hoed, T. W. (2013). *Handboek Managementmodellen*. Van Haren Publishing.
- Eisape, D. (2019). The Platform Business Model Canvas a Proposition in a Design Science Approach. *American Journal of Management Science and Engineering*, 4(6), 91. <https://doi.org/10.11648/j.ajmse.20190406.12>
- Evans, D. ., Hagi, A., & Schmalensee, R. (2019). Invisible Engines - How Software Platforms Drive Innovation and Transform Industries. In *Journal of Chemical Information and Modeling* (Vol. 53, Nummer 9). The MIT Press. <https://library.oopen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/26084/1004002.pdf?sequence=1&isAllowed=y>
- FRCL. (2018). *THE UK CORPORATE GOVERNANCE CODE - The Financial Reporting Council Limited*. <https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf>
- Gazé, P., & Vaubourg, A. G. (2011). Electronic platforms and two-sided markets: A side-switching analysis. *Journal of High Technology Management Research*, 22(2), 158–165. <https://doi.org/10.1016/j.hitech.2011.09.007>

- Guo Yuntao, Li Suike, B. S. (2011). *Framework of Comprehensive Risk Management System for the Defense Science and Technology Enterprises*. Science And Technology. <https://ieeexplore-ieee-org.ezproxy2.utwente.nl/stamp/stamp.jsp?tp=&arnumber=5920431>
- Hagiu, A. (2007). Merchant or Two-Sided Platform? *Review of Network Economics*, 6(2), 115–133. <https://doi.org/10.2202/1446-9022.1113>
- Halman, J. I. M., Hofer, A. P., & Van Vuuren, W. (2003). Platform-driven development of product families: Linking theory with practice. *Journal of Product Innovation Management*, 20(2), 149–162. <https://doi.org/10.1111/1540-5885.2002007>
- Han, X., Wu, Y., & Zheng, J. (2020). Digital Transformation, Multi-sided Platforms, and Analytical Framework. In *Disruptive Innovation through Digital Transformation* (pp. 9–23). [https://doi.org/10.1007/978-981-15-3944-2\\_2](https://doi.org/10.1007/978-981-15-3944-2_2)
- Heerschap, N. (CBS), Pouw, N. (UvA), & Atmé, C. (UvA). (2019). *Het meten van online platformen*. <https://www.cbs.nl/nl-nl/achtergrond/2019/06/het-meten-van-online-platformen>
- Holzweber, S. (2017). *Market Definition for Multi-Sided Platforms: A Legal Reappraisal*. World Competition. <https://kluwerlawonline.com/journalarticle/World+Competition/40.4/WOCO2017036>
- Homan, T. (2006). Wolkenridders. In *Over de binnenkant van organisatieverandering [Cloud ....* <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Wolkenridders#1>
- Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management* (Kogan Page (red.); 5th ed.).
- Inc., N. T. (2020). *Annual Report 2019 Newlink*. <https://www1.hkexnews.hk/listedco/listconews/sehk/2020/1221/2020122100005.pdf>
- Instituut voor Interne Auditors. (2007). *De internationale standaarden voor de Beroepsuitoefening van de interne auditfunctie*.
- ISACA. (2013). *Cobit 5 for risk*.
- ISACA. (2018). *Introducing Cobit 2019 Executive Summary November 2018*. COBIT® 2019 Framework. <https://www.isaca.org/resources/cobit>
- Jung, D., Kim, B. C., Park, M., & Straub, D. W. (2019). Innovation and policy support for two-sided market platforms: Can government policy makers and executives optimize both societal value and profits? *Information Systems Research*, 30(3), 1037–1050. <https://doi.org/10.1287/isre.2019.0851>
- Kagermann C, Kinney H, Kuting W, W. K. (2008). Nature and Content of Audits. In *Internal Audit Handbook: Management with the SAP- Audit Roadmap*. <https://doi.org/10.1007/978-3-540-70887-2>
- Kotter, J. P. (2019). *Leiderschap bij verandering* (Berber Bast (red.); 24e ed.). Boom Uitgevers Amsterdam.

- Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution and Logistics Management*, 38(3), 192–223. <https://doi.org/10.1108/09600030810866986>
- McIntyre, D. P., & Srinivasan, A. (2017). Networks, Platforms, and Strategy: Emerging views and next steps. *Strategic Management Journal*, 38, 141–160. <https://doi.org/10.1002/smj>
- McIntyre, D., Srinivasan, A., Afuah, A., Gawer, A., & Kretschmer, T. (2018). Multi-sided platforms as new organizational forms. *Academy of Management Perspectives*. <https://doi.org/10.5465/amp.2018.0018>
- Mishra, S., & Tripathi, A. R. (2020). Platform business model on state-of-the-art business learning use case. *International Journal of Financial Engineering*, 7(2), 2050015. <https://doi.org/10.1142/s2424786320500152>
- Mishra, S., & Triptahi, A. R. (2019). Platforms oriented business and data analytics in digital ecosystem. *International Journal of Financial Engineering*, 06(04), 1950036. <https://doi.org/10.1142/s2424786319500361>
- Murray-Webster, R., & Williams, G. (2010). *Management of Risk: Guidance for Practitioners* (Best Management Practice (red.); 2010 editi). Crown - published on behalf of the Office of Government Commerce.
- NEN. (2009). *ISO 31000:2019 Risicomanagement - Principes en richtlijnen - Nederlandse Normalisatie-instituut*.
- NEN. (2019). *NEN-ISO 31000+C11 (nl) Risicomanagement-Richtlijnen*.
- Netessine, S. (2020). *Hoe risico's in uw bedrijfsmodel te integreren*. 1–14.
- Nikpay, F., Ahmad, R. B., Rouhani, B. D., Mahrin, M. N., & Shamshirband, S. (2017). An effective Enterprise Architecture Implementation Methodology. *Information Systems and e-Business Management*, 15(4), 927–962. <https://doi.org/10.1007/s10257-016-0336-5>
- Oduoza, C. F. (2020). Framework for Sustainable Risk Management in the Manufacturing Sector. *Procedia Manufacturing*, 51(2019), 1290–1297. <https://doi.org/10.1016/j.promfg.2020.10.180>
- Osterwalder, A., & Pigneur, Y. (2019). *Business Model Generation*. Vakmedianet.
- Osterwalder, Alexander, Pigneur, Y., Bernarda, G., & Smith, A. (2019). *Waarde Propositie Ontwerp*. Vakmedianet.
- Palvia, P., Mao, E., Salam, A. F., & Soliman, K. S. (2003). Management Information Systems Research: What's There in a Methodology? *Communications of the Association for Information Systems*, 11(March). <https://doi.org/10.17705/1cais.011116>
- Parker, G. G., Van Alstyne, M. W., & Sangeet, P. C. (2016). Welcome to the Platform Revolution. In

*Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for you.*

[https://books.google.nl/books?hl=nl&lr=&id=Bvd1CQAAQBAJ&oi=fnd&pg=PT5&dq=Parker,+GG,+MW+Van+Alstyne+and+SP+Choudary+\(2016\).+Platform+Revolution:+How+Networked+Markets+Are+Transforming+the+Economy%3F+And+How+to+Make+Them+Work+for+You,+WW+Norton+%26+Company](https://books.google.nl/books?hl=nl&lr=&id=Bvd1CQAAQBAJ&oi=fnd&pg=PT5&dq=Parker,+GG,+MW+Van+Alstyne+and+SP+Choudary+(2016).+Platform+Revolution:+How+Networked+Markets+Are+Transforming+the+Economy%3F+And+How+to+Make+Them+Work+for+You,+WW+Norton+%26+Company)

Rochet, J.-C., & Tirole, J. (2004). *Two-Sided Markets: An Overview* \*. [http://web.mit.edu/14.271/www/rochet\\_tirole.pdf](http://web.mit.edu/14.271/www/rochet_tirole.pdf)

Smit, A. J. (2018). Complexe problemen oplossen: design thinking of ontwerpgericht onderzoek? *Onderwijsinnovatie*, 19(2), 17–24.

Stamer, D., Zimmermann, O., & Sandkuhl, K. (2016). What is a framework? - A systematic literature review in the field of information systems. *Lecture Notes in Business Information Processing*, 261, 145–158. [https://doi.org/10.1007/978-3-319-45321-7\\_11](https://doi.org/10.1007/978-3-319-45321-7_11)

Steuperaert, D. (2019). Cobit 2019: a Significant Update. *Edpacs*, 59(1), 14–18. <https://doi.org/10.1080/07366981.2019.1578474>

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*.

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf>

Strikwerda, H. (2016). De Nederlandse Corporate Governance Code. *Maandblad Voor Accountancy en Bedrijfseconomie*, 87(1/2), 43–57. <https://doi.org/10.5117/mab.87.14490>

Swanborn, P. (1994). Het ontwerpen van case-studies: enkele keuzen. *Mens en Maatschappij*, 69(3), 322–335.

Teece, J. D. (2012). *Next-generation competition: New concepts for understanding how innovation shapes competition and policy in the digital economy*.

<https://heinonline.org/HOL/LandingPage?handle=hein.journals/jecoplcy9&div=9&id=&page=>

The Center for Global Enterprise. (2021). *Understanding the Global Platform Economy - Convening top minds. Driving global innovation*. <https://www.thecge.net/understanding-the-global-platform-economy/>

The Committee of Sponsoring Organizations of the Treadway Commission. (2021). *Welcome to COSO*. <https://www.coso.org/Pages/default.aspx>

van Aken, J., & Berends, H. (2018). *Problem Solving in Organizations - A methodological handbook for business and management students* (third). Cambridge University Press.

Van Alstyne, M. W., Parker, G. G., & Paul Choudary, S. (2016). Pipelines, platforms, and the new rules



- of strategy. *Harvard Business Review*, 2016(April).
- Van Staveren, M. (2015). *Risicogestuurd werken* (3e ed.). Vakmedianet.
- Veisdal, J. (2020). The dynamics of entry for digital platforms in two-sided markets: a multi-case study. *Electronic Markets*. <https://doi.org/10.1007/s12525-020-00409-4>
- Verdonschot, S. G. M., & Kessels, J. (2011). Ontwerpgericht onderzoek als innovatiestrategie. In A. A. J. van Aken (Red.), *Handboek ontwerpgericht wetenschappelijk onderzoek* (pp. 377–398). Boom Lemma. <https://research.utwente.nl/en/publications/ontwerpgericht-onderzoek-als-innovatiestrategie>
- Verschuren, P., & Doorewaard, H. (2016). *Het ontwerpen van een onderzoek*. Boom uitgevers Amsterdam.
- Vostok New Ventures. (2019). *Vostok New Ventures LTD ANNUAL REPORT 2019*.
- Wallbach, S., Coleman, K., Elbert, R., & Benlian, A. (2019). Multi-sided platform diffusion in competitive B2B networks: inhibiting factors and their impact on network effects. *Electronic Markets*, 29(4), 693–710. <https://doi.org/10.1007/s12525-019-00382-7>
- Yablonsky, S. A. (2019). Multi-sided Platforms: Current State And Future Research. *Russian Management Journal*, 17(4), 519–546. <https://doi.org/10.21638/spbu18.2019.407>
- Yin, R. (2009). How to do better case studies. In *The SAGE Handbook of Applied Social Research Methods - Leonard Bickman, Debra J. Rog - Google Boeken* (pp. 254–262). [https://books.google.nl/books?hl=nl&lr=&id=9\\_bUtEp-bGUC&oi=fnd&pg=PA254&dq=Yin,+R.+K.+\(2009\).+Case+study+research:+Design+and+methods.+Thousand+Oaks,+CA:+Sage+Publications.&ots=-wN04JORQM&sig=73zvo-No1P99DhQJpKzigwvn83E#v=onepage&q&f=false](https://books.google.nl/books?hl=nl&lr=&id=9_bUtEp-bGUC&oi=fnd&pg=PA254&dq=Yin,+R.+K.+(2009).+Case+study+research:+Design+and+methods.+Thousand+Oaks,+CA:+Sage+Publications.&ots=-wN04JORQM&sig=73zvo-No1P99DhQJpKzigwvn83E#v=onepage&q&f=false)
- Zezulka, F., Marcon, P., Vesely, I., & Sajdl, O. (2016). Industry 4.0 – An Introduction in the phenomenon. *IFAC-PapersOnLine*, 49(25), 8–12. <https://doi.org/10.1016/j.ifacol.2016.12.002>
- Zhang, X., Xie, H., Yang, H., Shao, H., & Zhu, M. (2020). A General Framework to Understand Vulnerabilities in Information Systems. *IEEE Access*, 8, 121858–121873. <https://doi.org/10.1109/ACCESS.2020.3006361>



## 10 Figuren en tabellenlijst

### Figuren

Figuur 2-1 Structuur thesis, hoofdvraag en deelvragen .....	5
Figuur 3-1 De cyclus van ontwerpgericht onderzoek .....	7
Figuur 3-2 Onderzoeksmodel.....	9
Figuur 3-3 Case study methode en proces .....	12
Figuur 4-1 Kernbegrippen en bestaande literatuur.....	15
Figuur 4-2 Theoretische en visuele weergave van een meezijdig platformbedrijf.....	16
Figuur 4-3 Verschillende type platformbedrijven .....	17
Figuur 4-4 Weergave theoretisch concept van risicofactoren met een risico-effect en gevolgen.....	19
Figuur 4-5 Samenvattend overzicht risicofactoren .....	20
Figuur 4-6 Samenstelling theoretisch ontwerp voor het risicomanagementraamwerk .....	23
Figuur 5-1 Bovemij als Meezijdig platformbedrijf, met de verschillende actorengroepen, binnen de mobiliteitsbranche .....	25
Figuur 5-2 Organisatiemodel Bovemij Groep .....	27
Figuur 5-3 Elementen in Target Operating Model voor Bovemij.....	28
Figuur 5-4 Onderzoekresultaten op groepsniveau .....	29
Figuur 5-5 Huidige risicoprofiel van Bovemij.....	30
Figuur 6-1 Risicomanagementraamwerk voor Bovemij als groep .....	32
Figuur 6-2 Bovenste component governance en risicomanagementarchitectuur.....	33
Figuur 6-3 Three Lines of Defence.....	34
Figuur 6-4 Overzicht van Risico comités, overleggen en communicatielijnen .....	35
Figuur 6-5 Verbinding besturingsniveaus en risicomanagementstrategie en -beleid .....	36
Figuur 6-6 Ontwerp Risicomanagementproces Bovemij .....	37
Figuur 6-7 Gelaagdheid van bedrijfsbeleid.....	39
Figuur 6-8 Integratie risicomanagement binnen beleidsmanagementcyclus.....	40
Figuur 6-9 Principes binnen het risicomanagementraamwerk .....	40
Figuur 6-10 Bovemij Control Framework.....	42
Figuur 11-1 Organigram Bovemij N.V. ....	60
Figuur 11-2 Bovemij als platformbedrijf binnen de mobiliteitsbranche .....	61
Figuur 11-3 Theorie bedrijfsmodel .....	63
Figuur 11-4 Osterwalder canvas model .....	64
Figuur 11-5 Voorbeeld bedrijfsmodellen met technische architectuur.....	65

Figuur 11-6 Schematisch: risicofactoren met een risico effect en mogelijke gevolgen.....	68
Figuur 11-7 Risico scenario COBIT, verlies gegevens, bedreigingen en kwetsbaarheden. ....	69
Figuur 11-8 Voorbeeld van een risicoclassificatie spreidingsdiagram.....	73
Figuur 11-9 Criteria voor functionerend intern controlesysteem.....	74
Figuur 11-10 COSO Internal Control.....	75

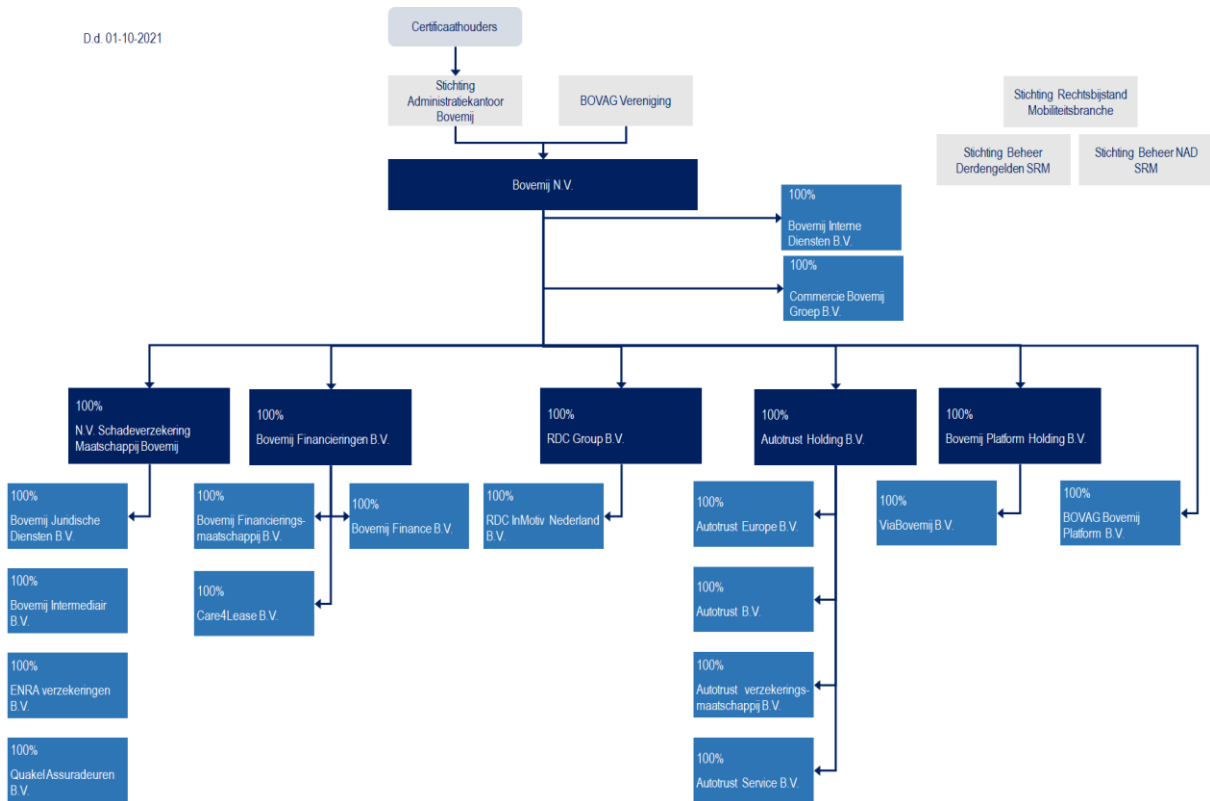
**Tabellen**

Tabel 3-1 Meest gebruikte bronnen voor (kern)begrippen .....	10
Tabel 3-2 Informatie vanuit stakeholders .....	13
Tabel 4-1 Generieke onderdelen van een Risicomanagementraamwerk.....	22
Tabel 5-1 Geïdentificeerde risico categoriën en aantal verschillende risicofactoren per categorie .....	31
Tabel 11-1 Verschillende risicomanagementprocessen en overeenkomende processtappen .....	72

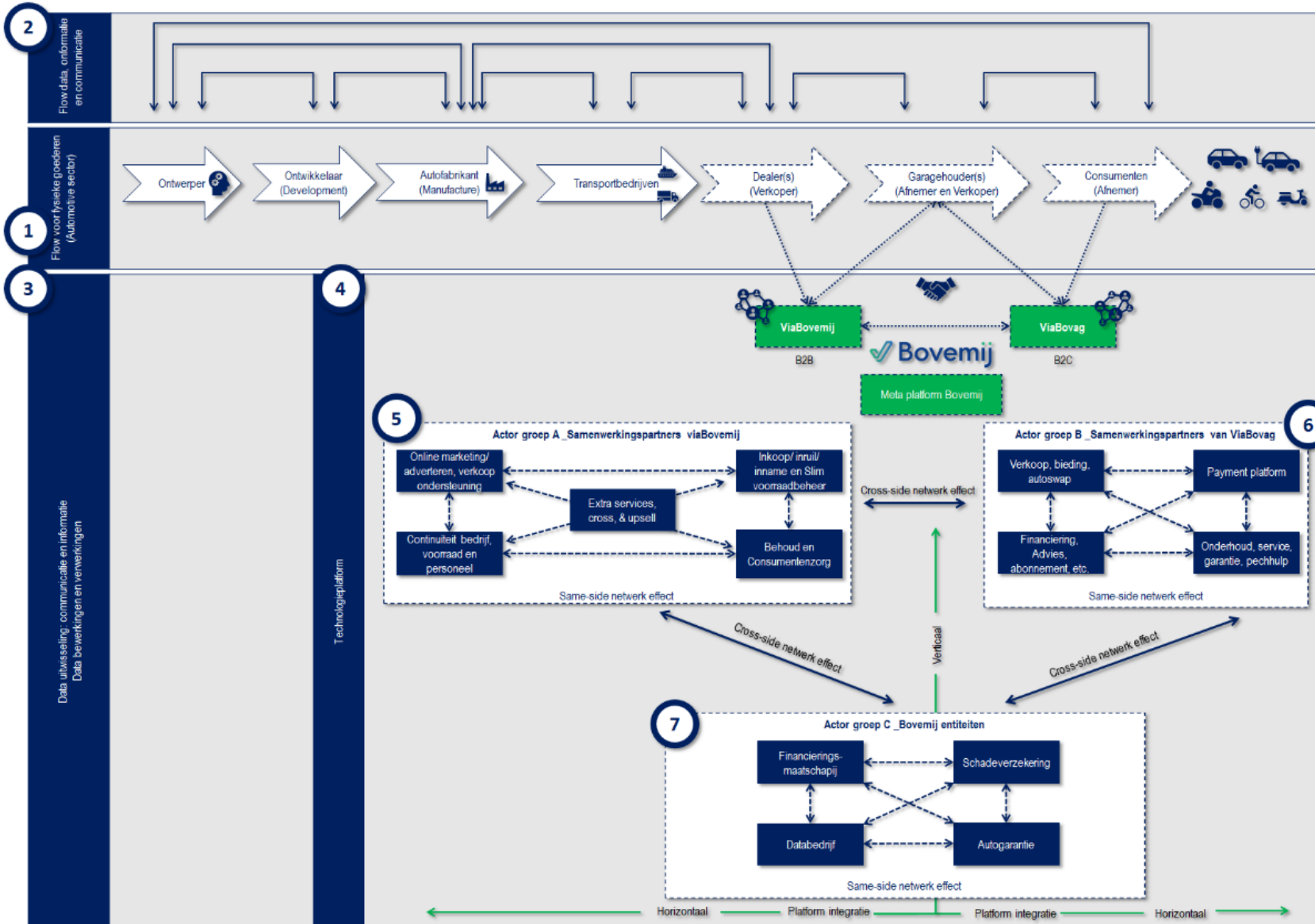
## 11 Bijlagen

### Bijlage A. Informatie Bovemij N.V.

Figuur 11-1 Organigram Bovemij N.V.



Figuur 11-2 Bovemij als platformbedrijf binnen de mobiliteitsbranche



**Bijlage B.      Aanvullende informatie over de begrippen****Digitale (platform) economie en Bedrijfsmodel Meerzijdig Platformbedrijf**

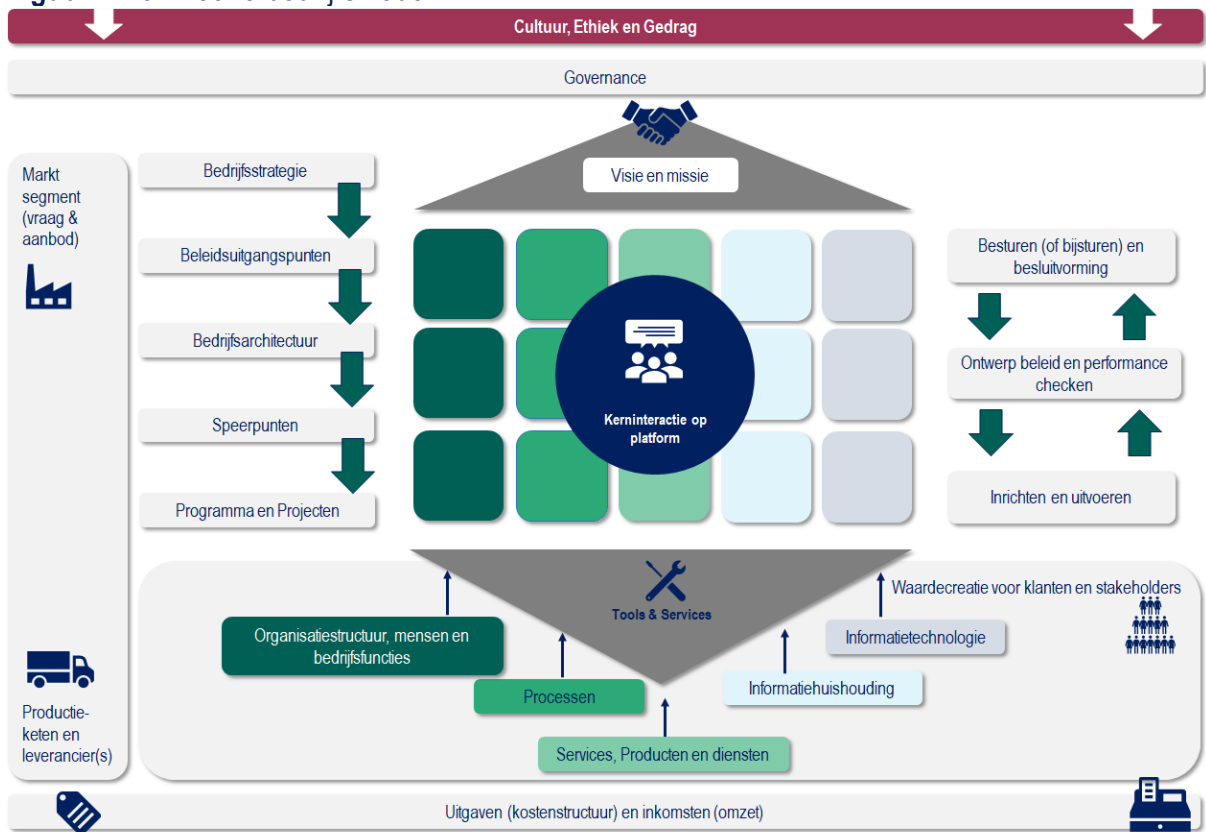
In traditionele waardeketens verworven bedrijven de input van leveranciers en bundelden deze tot producten en diensten, die aan afnemers werden aangeboden via activiteiten als marketing, distributie en klantenservice (Porter (1985), geciteerd in Veisdal, 2020). Op twee- en meerzijdige markten exploiteren platformbedrijven activiteiten als het zijn van een tussenpersoon tussen meerdere groepen deelnemers die willen profiteren van de interactie met andere deelnemers met complementaire behoeften (Veisdal, 2020).

In de tweede golf, identificeerden technologiestrategen, Baldwin & Woodard (2009), platforms als waardevolle controlepunten (en huuraanwinsten) in een industrie. Industriële economen hebben in hetzelfde artikel van Baldwin & Woodard (2009) vervolgens de term 'platform' in de context van een bedrijf gebruikt om producten, diensten, organisatie of instellingen te karakteriseren, die transacties tussen twee of meer groepen bemiddelen. Dit wordt in artikelen van Abdelkafi et al. (2019) en A. Osterwalder & Pigneur (2019) bestempeld als een Meerzijdig platform aanbieder: twee of meer onderling afhankelijke gebruikersgroepen zijn verbonden aan het platform, door het spelen van een bemiddelende of een matchmaking rol. Hier voegen A. Osterwalder & Pigneur aan toe dat dergelijke platformen alleen van waarde zijn voor de ene groep klanten als de andere groepen klanten ook aanwezig zijn (A. Osterwalder & Pigneur, 2019). Het platform creëert waarde door de interacties te faciliteren tussen de verschillende groepen (A. Osterwalder & Pigneur, 2019), figuur 11-6 is hiervan de conceptuele weergave.

De term bedrijfsmodel, ook wel enterprise architectuur genoemd, doet aan het eind van de jaren '90 zijn intrede (den Hoed, 2013). Een bedrijfsmodel beschrijft alle facetten, als in bedrijfscomponenten, die invloed hebben op het creëren van die meerwaarde voor klanten (den Hoed, 2013). Het is een beschrijving van de waarde die een bedrijf biedt aan een of meerdere segmenten van klanten en de architectuur van het bedrijf en zijn netwerk van partners voor het creëren, vermarkten en leveren van deze waarde en relatie kapitaal, om winstgevende en duurzame inkomstenstroom te genereren (Bayens & Tönissen, 2015; A Osterwalder & Pigneur, 2019) geeft de volgende definitie voor een bedrijfsmodel: "een bedrijfsmodel beschrijft de grondgedachte van hoe een organisatie waarde creëert, levert en behoudt" (A Osterwalder & Pigneur, 2019). En het model omschrijft de vereiste capabilities/ skills en partners om deze waarde te creëren, te vermarkten en te leveren. En het omschrijft de onderlinge, waardetoevoegende relaties om te komen tot profijtelijke, duurzame inkomstenstromen. Een

businessmodel is zodoende een afbeelding van hoe een organisatie haar meerwaarde wil creëren en daaraan geld wil verdienen (den Hoed, 2013).

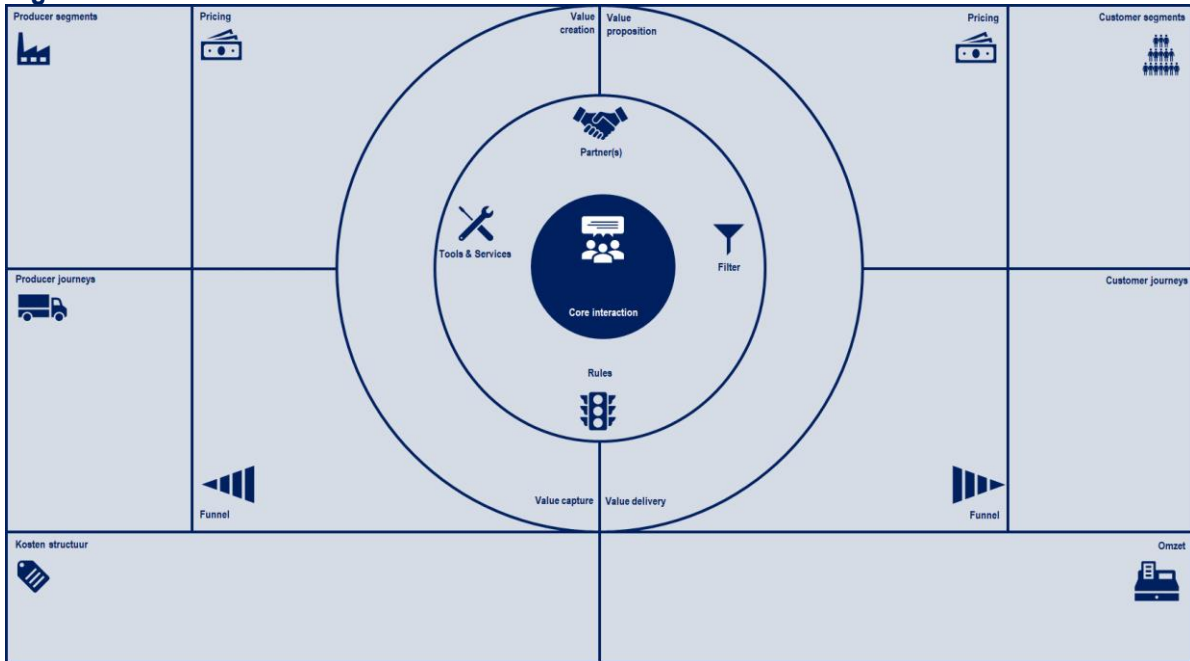
**Figuur 11-3** Theorie bedrijfsmodel<sup>19</sup>



Het bedrijfsmodel van een eenvoudig platformbedrijf is een model dat waarde genereert door het bedienen van twee of meer onafhankelijke groepen, normaal gesproken verkopers en kopers (Mishra & Tripathi, 2020; Parker et al., 2016). Hoewel er vele soorten platforms bestaan, hebben ze volgens Van Alstyn et al., (2016) binnen het digitale ecosysteem eenzelfde basisstructuur, bestaande uit vier soorten spelers: De eigenaren van platformbedrijven die zeggenschap hebben over hun intellectuele eigendom en governance, aanbieders die als interface tussen de platforms en gebruikers fungeren, producenten die creëren aanbod, en consumenten gebruiken dit aanbod (Van Alstyn et al., 2016). Het Meezijdig platformbedrijf stelt als het ware een instrument ter beschikking door verschillende technologieën te combineren en brengt daarmee nieuwe zakelijke mogelijkheden op een inventieve en transformationele wijze (De Reuver et al., 2018; Mishra & Tripathi, 2020; Mishra & Triptahi, 2019).

<sup>19</sup> Afbeeldingen uit de literatuur Bayens & Tönissen (2015), ISACA (2012), A Osterwalder & Pigneur, (2019) overgenomen en samengevoegd tot hetgeen gevisualiseerd in deze scriptie.

**Figuur 11-4** Osterwalder canvas model<sup>20</sup>

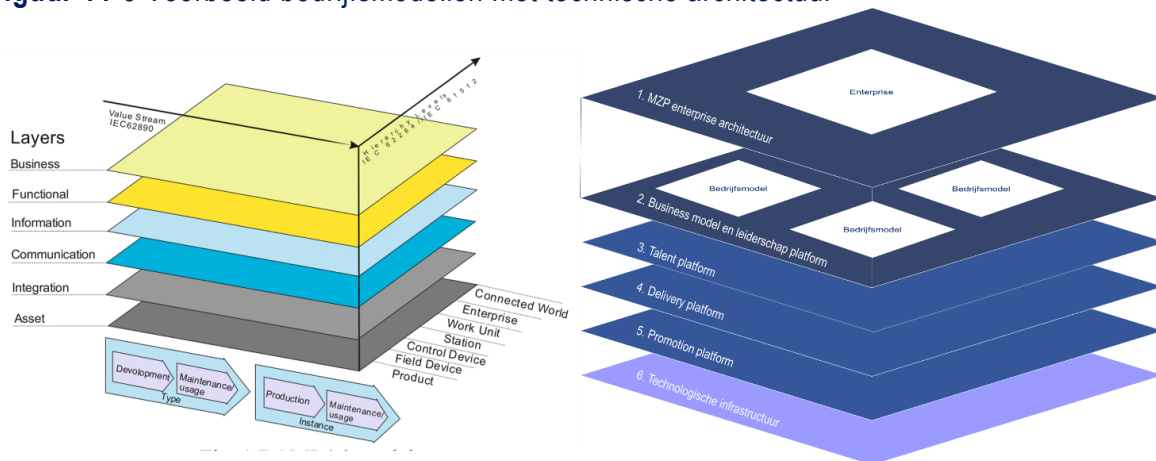


Echter is de bedrijfsvoering van een Meezijdig platformbedrijf en de samenhang met de technologie gecompliceerd (Yablonsky, 2019, p. 527). Een digitaal Meezijdig platformbedrijf is een business driven framework dat een community van partners, providers en klanten in staat stelt om digitale processen en “capabilities” te delen en deze te verbeteren of uit te breiden voor wederzijdse voordelen (geciteerd in Yablonsky (2019) Burton, Basiliere, (2016). Een digitaal platformbedrijf is daarom veel meer dan alleen een bedrijfsmodel of alleen maar de technologie, zie het voorbeeld van Zezulka et al. (links) en Yablonsky (rechts) in **Fout! Verwijzingsbron niet gevonden..**

De voorbeelden van Zezulka et al. (links) en Yablonsky (rechts) in Figuur 11-3 tonen twee verschillende bedrijfsmodellen.

<sup>20</sup> Afbeelding overgenomen uit Mishra & Triptahi, 2019; A Osterwalder & Pigneur, 2019; Yablonsky, (2019)



**Figuur 11-5** Voorbeeld bedrijfsmodellen met technische architectuur


Het raamwerk van Yablonsky maakt verschillende combinaties mogelijk van bedrijfsmodellen, leiderschap, talent, levering en IT-infrastructuurplatforms die digitale bedrijfsecosystemen aandrijven, terwijl het bedrijfsmodel van Zezulka van toepassing is voor één bedrijf. Wat deze modellen echter veel minder op toezien is het inspelen op waardecreatie, klant- en marktsegmenten, samenwerkingspartners, leverancier- en financiële aspecten (prijs, kosten en omzet), zoals Mishra & Triptahi (2019), A Osterwalder & Pigneur (2019) en Yablonsky (2019) dat wel als belangrijk aangeven.

Zoals literatuuronderzoek laat inzien, bestaan meerszijdig platformbedrijven meestal uit bedrijf de componenten: hardware, software, services, diensten, producten (goederen), doelen, regels. Dit tezamen vormt het bedrijfsmodel om de onderneming in leven te houden en meerwaarde te creëren voor de verschillende partijen.

### Technologie als strategie

Zoals in literatuur beschreven kan informatietechnologie samenlevingen, (beleid vanuit) overheden, bedrijven (Jung et al., 2019), producten, klantwensen, logistiek (Hagiu, 2007) en meer (volledig/ deels) transformeren en bij elkaar brengen. Technologische transformatie vereist moeilijke, maar cruciale strategische beslissingen (Jung et al., 2019). Het nemen van (strategische) beslissingen wordt nog uitdagender voor bestuurders van platformbedrijven die nauw verbonden zijn met een spinnenweb van netwerken, ook wel netwerkexternaliteiten of “cross externalities” genoemd (Gazé & Vaubourg, 2011), die onlosmakelijk zijn verbonden aan tweezijdige of meerszijdige markten.

Door de komst van platformbedrijven binnen de verschillende markten treden daarmee ook nieuwe marktspeelers aan. Dit zijn de door Hagiu (2009) zogenoemde, matchmaking bedrijven in de digitale economie. Zo zijn verschillende voorbeelden te noemen die inmiddels duizenden, misschien wel

miljoenen (Hagiu, 2007) verschillende marktspelers verbinden zoals, Amazon's Marketplace en eBay (verkopers en kopers), Booking.com en Hotels.com (Agents en Merchants), Apple (iTunes) en Google's "app stores" (ontwikkelaars en gebruikers) en Airbnb en Camptoo (verhuurders en gasten) (Veisdal, 2020).

### **Platform**

De term 'platform' wordt op verschillende manieren gebruikt en gedefinieerd door industriële managers en onderzoekers in verschillende sectoren (Abdelkafi et al., 2019; Rochet & Tirole, 2004). Het is veelal afhankelijk van de context waarbinnen het begrip 'platform' is gebruikt en gedefinieerd. Volgens Bayens & Tönissen (2015) is een platform de technische basis waarop software wordt gebouwd en onderdeel van de technische infrastructuur. Op het gebied van business en engineering vragen (Baldwin & Woodard, 2009, p. 25) zich af of de "verschillende platformbegrippen synoniem zijn of gewoonweg evocatief gebruik van hetzelfde woord om verschillende dingen te betekenen". Zij bekijken platforms vanuit drie perspectieven: productontwikkeling, technologiestrategie en industriële economie.

Naast dat de term "platform" op verschillende manieren gedefinieerd kan worden, kan het ook een variëteit aan vormen aannemen, afhankelijk van de context van het gebruik (Yablonsky, 2019). Op het gebied van business en engineering vragen Baldwin & Woodard (2009) zich af of de "verschillende platformbegrippen synoniem zijn of gewoon suggestief gebruik van hetzelfde woord om verschillende dingen te betekenen". Zij bekijken drie perspectieven op platforms: productontwikkeling, technologiestrategie en industriële economie. Baldwin & Woodard (2009) hebben uitgezocht dat volgens het Oxford-Engels woordenboek het woord 'platform' al sinds de zestiende eeuw wordt gebruikt om te verwijzen naar *'een verhoogd vlak waarop mensen of dingen kunnen staan, meestal een discrete structuur die bedoeld is voor een bepaalde activiteit of operatie'*. Voorkomende actoren (economische agenten) op een platform zijn klanten, partners, werknemers en slimme machines (Yablonsky, 2019).

### **Elektronische markten en digitale economie**

Zoals in de definitie voor een Meezijdig platformbedrijf zijn Meezijdig platformbedrijf's nauw verwant aan elektronische markten, wat ook bekend staat als digitale meezijdige markten en of wordt aangegeven als digitale economie (CBS, 2021). De meeste van de huidige platforms zijn hoofdzakelijk digitaal, leggen data (gegevens) vast (inclusief persoonsgegevens) verzenden data via het internet en andere netwerken (Evans, Gawer, 2016, geciteerd in Yablonsky, 2019, p. 522). Hiermee is de digitale economie vergelijkbaar met een vorm van digitale marktplaats waar kopers en verkopers aanwezig zijn.

### Kenmerken Meezijdige platformbedrijven aanbieder

Net als dat er verschillende platformbedrijven en definities bestaan voor een platform bedrijf, lopen de typologie-omschrijving, criteria en categorisering voor meezijdige platform aanbieders ook uiteen. Het fenomeen platform, kan duiden op "alle vormen van genetwerkte bedrijven waar meerdere leveranciers en klanten met elkaar in contact komen voor economische doeleinden binnen één of meerdere niveaus in economische waardeketens" (Abdelkafi et al., 2019; Alt & Zimmermann, 2014, p. 162). Volgens Yablonsky (2019) hebben P. Evans en A. Gawer in 2016 aangetoond dat digitale meezijdig platformbedrijven ook wereldwijde fenomenen zijn: ze opereren niet alleen in geavanceerde industriële markten, maar in de hele wereld dankzij de groeiende beschikbaarheid van mobiele digitale technologieën en het internet. Dit is een groot verschil met fysieke platformen voor verkoop en koop, omdat de digitale mogelijkheden de transactie- en andere vormen van bedrijfskosten verlaagt, evenals het vereenvoudigen van interacties tussen verschillende partijen (Evans, Schmalensee, (2018) geciteerd in Yablonsky, (2019)).

Volgens de beschrijving van het Centraal Bureau van de Statistiek (hierna "CBS") bemiddelt een digitaal platform tussen twee groepen die van elkaar afhankelijk zijn (CBS, 2021). Waarbij gaat daarbij om het uitwisselen van goederen, diensten of informatie (CBS, 2021), waarbij het platform gezien kan worden als een tussenpersoon tussen het aanbod en het gebruik van goederen, diensten en/of informatie voor actoren zoals personen (w.o. consumenten), bedrijven, wetenschap en overheid.

M. Cusumano, A. Gawer, D. en Yoffie (2019) verdelen platformbedrijven onder in twee hoofdtypen: Innovatieplatform en transactieplatform. Yablonsky (2019), Heerschap et al., (2019) en Evans en Gawer (2016) (geciteerd in Heerschap et al., 2019), voegen hier nog twee type aan toe: Investeringsplatform en geïntegreerd (technologie) platform.

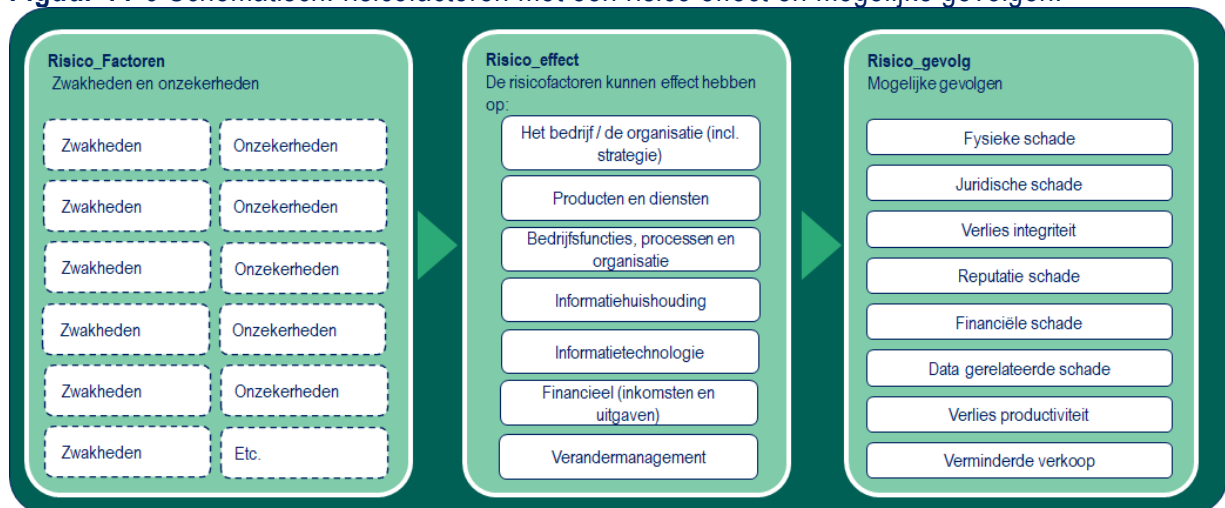
Over de typologieën van platform bedrijven valt veel te discussiëren en filosoferen. Volgens Evans et al., (2019) gaan software- en industrieplatforms namelijk verder dan het hiervoor beschreven over platformbedrijven. Platforms brengen namelijk "*...individuen en organisaties samen zodat ze kunnen innoveren of interageren op manieren die anders niet mogelijk zijn, met het potentieel voor non-lineaire verhogingen van het nut en de waarde van een platform*" (Evans et al., 2019). Ook blijkt uit het overzicht in **Fout! Verwijzingsbron niet gevonden.** dat een eenduidige typologie van een platform niet eenvoudig te maken is. Zo maakt het CBS (2021) ook onderscheid tussen "peer-to-peer" (hierna "P2P"), "business-

to-peer” (hierna “B2P) en strategieën in hybride vormen wat het moeilijk maakt om een duidelijk onderscheid te hebben tussen online platformen.

**Onzekerheid, Risico(factoren) en Risicoprofiel**

Net als voor de andere begrippen zijn er verschillende omschrijvingen te vinden voor risico. Verder is met regelmaat onderscheid te vinden tussen ‘risico’ en ‘onzekerheden’. Wat in alle omschrijvingen over ‘risico’ of ‘risicofactor’ opvalt is dat de ‘onzekerheden’ een bepaald ‘effect’ kunnen hebben op iets. Dit iets kan zijn: de doelstellingen, het bedrijf, de reputatie, de financiële conditie en operating resultaten. Daarom is een risico de resultante van een onzekere (onzekerheid) gebeurtenis (event) d.w.z. dat leidt tot het zich voordoen van risico's (Manuj & Mentzer, 2008). Veelal heeft het een gestructureerde beschrijving van de elementen: risicobron(nen), oorzaken, gebeurtenis, gevolg en onzekerheidsmeting (Aven, 2011), zoals weergegeven in 11-6.

**Figuur 11-6** Schematisch: risicofactoren met een risico effect en mogelijke gevolgen.



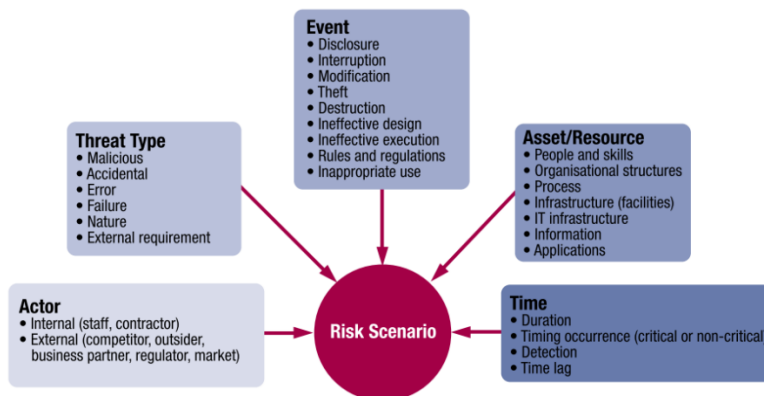
Het effect is een afwijking van hetgeen verwacht of beoogt wordt. Dit kan zowel positief, negatief als beide zijn en kansen of bedreigingen aanpakken, creëren of daarin resulteren (NEN, 2019). Terwijl COSO (2017) aangeeft dat een risico de mogelijkheid is dat gebeurtenissen zich voordoen en de verwezenlijking van doelstellingen beïnvloeden. Risico wordt door Oduoza, (2020) gedefinieerd als een combinatie van de ernst (hoe zwaar het is als de gebeurtenis zich voordoet en de waarschijnlijkheid van een gebeurtenis (hoe vaak de gebeurtenis zich voordoet). Hopkin (2018) beschrijft een risico als een gebeurtenis met het vermogen om de effectiviteit en efficiëntie van de kernprocessen van een organisatie te beïnvloeden (belemmeren, versterken of in twijfel trekken). Hierbij wordt aangegeven dat het effect zowel positief als

negatief kan zijn en dat ieder risico zijn eigen karakteristieken ofwel factoren heeft dat een eigen wijze van analyse behoeft en wijze van hoe te managen.

Wat in alle omschrijvingen opvalt is dat ‘onzekerheden’ een bepaald ‘effect’ kunnen hebben op iets. Dit iets kan zijn: de doelstellingen, het bedrijf, de reputatie, de financiële conditie en operating resultaten. Daarom is een risico de resultante van een onzekere (onzekerheid) gebeurtenis (event) d.w.z. dat leidt tot het zich voordoen van risico's (Manuj & Mentzer, 2008). Veelal heeft het een gestructureerde beschrijving van de elementen: risicobron(nen), oorzaken, gebeurtenis, gevolg en onzekerheidsmeting (Aven, 2011).

COBIT, figuur 11-7, geeft aan dat voor een technologiebedrijf er een wezenlijk verschil is tussen de risicofactoren en de effecten ervan. Bijvoorbeeld: gegevensverlies wordt vaak getriggerd door een bedreigende gebeurtenis (Threat type). De frequentie van de bedreigende gebeurtenis wordt beïnvloed door de risicofactoren ofwel de kwetsbaarheden. De kwetsbaarheid is meestal een toestand dat kan worden verhoogd of verlaagd door bijvoorbeeld verzwakking van controles of een sterke toename van dreigingen. Voor een technologiebedrijf is het belangrijk dat deze soorten gebeurtenissen niet worden vermengd tot één grote risicolijst, maar leiden tot een concrete omschrijving van een risico scenario waar een specifieke maatregel preventief, of detectief dan wel reactief voor wordt ingericht en onderhouden.

**Figuur 11-7** Risico scenario COBIT, verlies gegevens, bedreigingen en kwetsbaarheden<sup>21</sup>.



<sup>21</sup> Afbeelding overgenomen uit COBIT ISACA (2013)

## Risicomanagement en Risicomanagementproces

De laatste jaren is binnen de digitale economie steeds meer aandacht voor risicomanagement (Aven, 2011) en het integreren ervan in het bedrijfsmodel (Netessine, 2020). Er bestaat een sterke opvatting dat risicomanagement het geschikte instrument is om de conflicten die inherent zijn aan enerzijds het verkennen van kansen, en anderzijds het vermijden van verliezen, ongevallen en rampen, in evenwicht te brengen (Aven, 2011).

Risicomanagement is volgens de Management of Risk ('MoR') Guidance een systematische toepassing van principes, benadering, en processen die de taak hebben om risico's te identificeren, beoordelen en vervolgens een gepaste risico reactie te implementeren (Murray-Webster & Williams, 2010). De bedenkers van de COSO ERM theorie voegen hieraan toe dat risicomanagement is gericht op waardecreatie waarbij beleid, processen, mensen, technologie en kennis worden geïntegreerd (Claassen, 2009). Daarentegen beschrijft de ISO 31000 risicomanagement als gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's (NEN, 2009, 2019).

Risicomanagement zou idealiter een aantal kernresultaten opleveren:

1. De organisatie beschikt over een actueel, correct en volledig inzicht in haar risico's;
2. De risico's van de organisatie vallen binnen haar risicocriteria;
3. Volledige verantwoordingsplicht voor risico's;
4. Bij alle besluitvorming wordt gebruik gemaakt van risicomanagement;
5. Doorlopende communicatie met externe en interne belanghebbenden;
6. Volledige integratie in de bestuursstructuur van de organisatie (NEN, 2009, pp. 26–27)

Stoneburner et al., (2002) hebben een artikel geschreven specifiek over risicomanagement voor een technologiebedrijf. In dit artikel geven zij aan dat risicomanagement voornamelijk drie kernprocessen omvat: 1. Risicobeoordeling, 2. Risico mitigatie/ beheersing, 3. Risico evaluatie en beoordeling. De risicobeoordeling is vooral de identificatie en evaluatie risico's en de effecten van risico's, en de aanbevelingen voor risicobeperkende maatregelen. De risico mitigatie/ beheersing het prioriteren, implementeren en handhaven van de risicobeperkende maatregelen die uit het risicobeoordelingsproces naar voren zijn gekomen. Risico evaluatie en beoordeling is het proces van voortdurende evaluatie en de belangrijkste voorwaarden voor de uitvoering van een succesvol risicobeheersingsprogramma.

Het risicomanagementproces kent verschillende definities, omschrijvingen, een verschillend aantal en benamingen voor de stappen, en verschillend toegepast per type bedrijf. Zoals het artikel van Stoneburner et al. (2002), hierin is het risicomanagementproces beschreven als onderdeel van een groter geheel van risicomanagement. Eveneens wordt de term risicobeoordeling gebruikt in plaats van risicomanagementproces. Hierbij is risicobeoordeling het eerste proces in de risicobeheersmethodologie. Voornamelijk technologie bedrijven gebruiken deze wijze van risicobeoordeling om de omvang van de potentiële bedreiging en het risico in verband met de specifieke informatietechnologie gedurende de gehele levensduur van de informatietechnologie te bepalen (Stoneburner et al., 2002). De output van dit proces helpt bij het identificeren van geschikte beheersingsmaatregelen om risico's te verminderen of te elimineren binnen het proces voor risicobeheersing/ mitigatie.




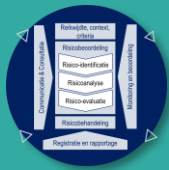
Binnen de integrale toepassing van risicomanagement door COSO ERM wordt gesproken over het gebruik van een standaardproces, doordat dit bijdraagt aan het gedisciplineerd uitvoeren van risicomanagement (Claassen, 2009). Hierbij geeft de COSO organisatie drie doelstellingen aan voor het risicomanagementproces:

- a) Gemeenschappelijk beeld hebben voor alle betrokkenen omtrent het verloop van het proces en de overkoepelende risicodoelen en -doelstellingen;
- b) Een gemeenschappelijk risicomanagementproces vormt het fundament voor het continu verbeteren van de risicomanagementvaardigheden en de mate van volwassenheid van het risicomanagementproces;
- c) Het risicomanagementproces geeft inzicht in specifieke te verrichten risicomanagementtaken. (Claassen, 2009)

Echter, een recentere herziening van dergelijke kaders en normen door Aven, 2011; Van Staveren, (2015) concludeert dat er brede gelijkenis is als het gaat om fundamentele onderliggende ideeën over het risicomanagementproces. Er bestaat overeenstemming over de opeenvolgende stappen binnen het proces, die nodig zijn voor een goed risicobeheer, risicobeoordeling, risico-evaluatie en risicobeheersing (Aven, 2011; Van Staveren, 2015). Onderstaande **Fout! Verwijzingsbron niet gevonden.** geeft de overeenkomsten en verschillen compact weer tussen verschillende toepassingen van het risicomanagementproces. Zoals Van Staveren, (2015) in zijn boek aangeeft zijn de generieke en overeenkomende processtappen opeenvolgend en zowel lineair als cyclisch uit te voeren. Aanvullend is in dit boek aangegeven dat het hierbij belangrijk is om de processtappen te herhalen omdat de hoeveelheid en kwaliteit van beschikbare informatie, evenals percepties, over risico's in de tijd verandert.



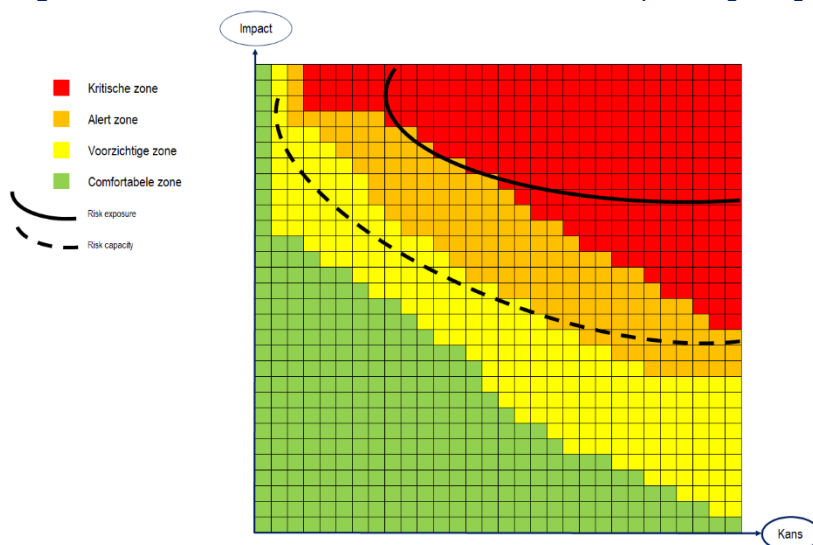
**Tabel 11-1** Verschillende risicomanagementprocessen en overeenkomende processtappen

<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">  <p>(Stoneburner et al., 2002) <b>Risk Management Guide for Information Technology Systems</b></p> </div> <div style="text-align: center;">  <p>(COSO, 2017) <b>COSO ERM</b></p> </div> <div style="text-align: center;">  <p><b>COBIT 5 for Risk (ISACA, 2013)</b></p> </div> <div style="text-align: center;">  <p>(NEN, 2019) <b>ISO 31000</b></p> </div> </div>			
1. Bepalen systeemkarakteristieken	Inventariseren risico's	01. Collect Data	Reikwijdte, context, criteria
2. Identificatie bedreiging	Beoordelen risicoprofiel	02. Analyse risk	Risicobeoordeling: 1. Risico identificatie
3. Identificatie kwetsbaarheid			
4. Analyse van bestaande/ geplande controls			
5. Kans bepaling		03. Maintain a risk profile	
6. Impact analyse			2. Risicoanalyse 3. Risico evaluatie
7. Risico determinatie	Toepassen risicomanagement-strategie	04. Articulate risk 05. Define a risk management action portfolio	Risicobehandeling Communicatie en consultatie
8. Aanbevelen benodigde controls	Inrichten risicobeheersingsprocessen	06. Respond to risk	
9. Documenteren resultaten	Monitoren		Monitoren en rapportage

### Risicobeoordeling en analyse

In de terminologie voor risicomanagement wordt de term waarschijnlijkheid gebruikt om te verwijzen naar de kans dat iets gebeurt, die objectief dan wel subjectief, kwalitatief dan wel kwantitatief is vastgesteld, gemeten of bepaald, en is beschreven in algemene termen dan wel wiskundig de waarschijnlijkheid ('probability') of frequentie over een bepaalde periode (NEN, 2019). De uitkomst van een gebeurtenis waardoor de doelstelling wordt beïnvloed, is het gevolg. Een gevolg kan zeker of onzeker zijn en kan het behalen van de doelstelling positief of negatief direct of indirect beïnvloeden. Ook gevolgen kunnen zowel kwantitatief als kwalitatief worden uitgedrukt. Gevolgen kunnen escaleren door opeenvolgende en cumulatieve effecten. Veelal worden de uitkomsten uit de kans en impact analyse opgenomen in een spreidingsdiagram.

**Figuur 11-8** Voorbeeld van een risicoclassificatie spreidingsdiagram



### Risicomanagementraamwerk - Control framework

Het doel van de controleomgeving is te zorgen voor een consequente reactie op risico's die zich voordoen (Hopkin, 2018). Een goed ontwikkelde controleomgeving zal er ook voor zorgen dat vooraf geplande reacties op een crisissituatie efficiënt en doeltreffend worden uitgevoerd (Hopkin, 2018).

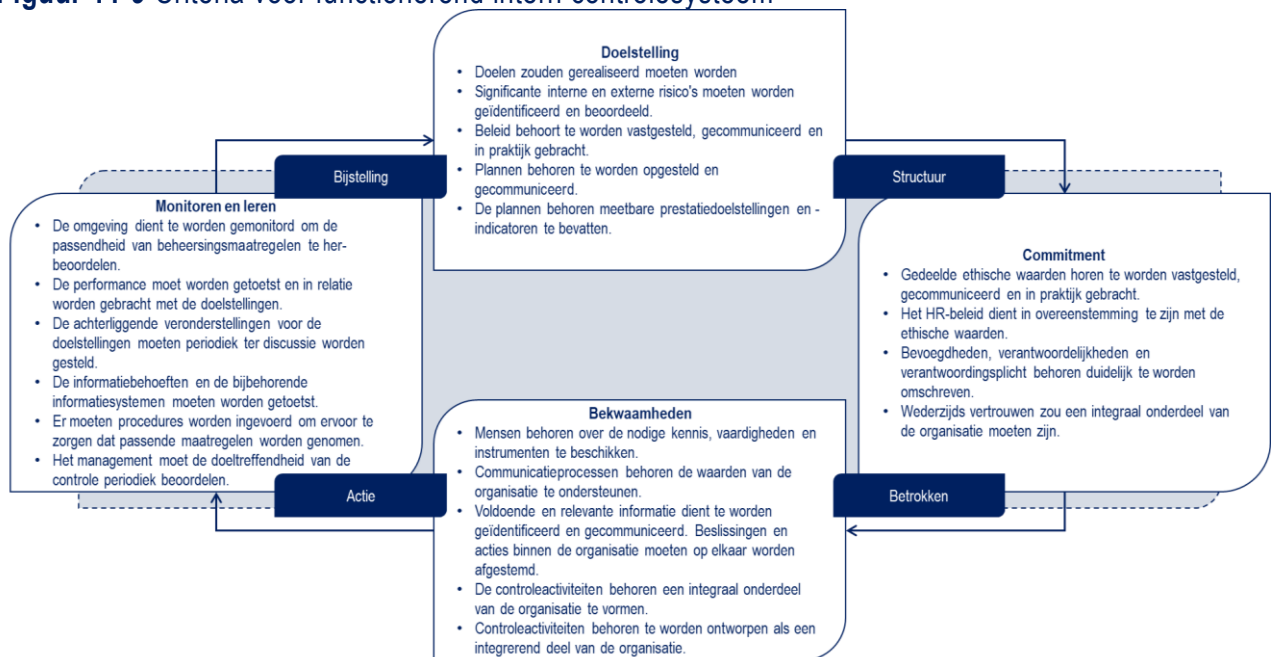
Binnen de context van risicomanagement, volgens ISO 31000, is op organisatieniveau (strategisch) de controleomgeving onderdeel van de organisatie als geheel en haar context. Deze context bestaat uit een interne en externe context. Om de doeltreffendheid van het raamwerk voor risicomanagement te evalueren behoort de organisatie:

- Periodiek de prestaties van het risicomanagementraamwerk te meten aan de hand van het doel ervan, de implementatieplannen, indicatoren en verwacht gedrag;
- Vast te stellen of het raamwerk geschikt blijft om het bereiken van de doelstellingen van de organisatie te ondersteunen (NEN, 2019).

Het door het Canadian Institute of Chartered Accountants (afgekort als "CICA") opgestelde "Criteria of Control Framework", ook bekend als CoCo, is een gestructureerd middel om de kwaliteit van de controleomgeving binnen een organisatie te meten. Deze raamwerkbenadering bestaat uit vier componenten, welke in figuur 11-9 verder zijn uitgewerkt:

- Doelstelling
- Commitment
- Bekwaamheid
- Monitoren en leren

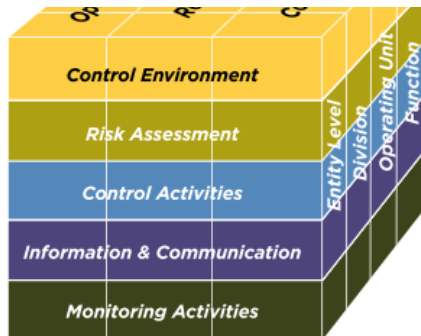
**Figuur 11-9** Criteria voor functionerend intern controlesysteem



Het Control Framework en de Control omgeving kunnen in nauwe samenhang met het Risicomanagementraamwerk worden gezien. Zo heeft The Committee of Sponsoring Organization of the Treadway Commission in het verleden bijvoorbeeld twee kubussen ontwikkeld, te weten: COSO Internal Control (1992 en geüpdatet in 2013) en COSO Enterprise Risk Management (2004 en geüpdatet in 2017). Beide kubussen ofwel raamwerken zijn bedoeld om elkaar aan te vullen, en geen van beide vervangt het andere (COSO, 2013, 2017).

Waar een Risicomanagement raamwerk op organisatieniveau (“Enterprise”) zorgt voor onder meer samenhangende componenten, structuur, risicoarchitectuur, strategie (lees paragraaf **Fout! Verwijzingsbron niet gevonden.**), kunnen de Control omgeving, interne beheersing en een Control Raamwerk (Framework) gezien worden als een onderdeel van een Risicomanagementraamwerk en een op zichzelf staand raamwerk (The Committee of Sponsoring Organizations of the Treadway Commission, 2021).

**Figuur 11-10** COSO Internal Control



De kenmerken van de controleomgeving die door COSO Internal Control als belangrijk worden beschouwd, kunnen als volgt worden samengevat:

- de organisatie is toegewijd aan integriteit en ethische waarden;
- het bestuur houdt toezicht op de ontwikkeling en uitvoering van de interne beheersing;
- het management stelt structuren, rapportagelijnen, bevoegdheden en verantwoordelijkheden vast;
- de organisatie streeft ernaar bekwame personen aan te trekken, te ontwikkelen en te behouden; en
- de organisatie houdt mensen verantwoordelijk voor de verantwoordelijkheden op het gebied van interne beheersing (COSO, 2013).

### Een aantal risicofactoren uitwerkt

#### Ontwrichtende innovatie

Het uitvoeren van platformstrategieën gaat niet zonder uitdagingen, aangezien het proces van het bouwen en testen van een platform een enorme investering van tijd en geld vergt, en aan het einde van het proces kan het aanbod een koude reactie teweegbrengen bij de beoogde doelgroep (Bradford, 2019). Een belangrijk kenmerk van digitale transformatie in relatie tot de doelgroep en het bedrijf is dat het de wereld verandert door zogenoemde ontwrichtende innovatie (Han et al., 2020). Ontwrichtende innovatie werd voor het eerst gedefinieerd en geanalyseerd door de Harvard Business School professor Clayton Christensen (Bower en Christensen 1995; Christensen 1997). Vervolgens werd door verschillende andere wetenschappers hetzelfde betoogd en geconcludeerd dat dit eveneens innovatie van bedrijfsmodellen behoeft. De bedrijfsmodellen worden namelijk sinds enkele jaren aangedreven door digitale technologieën, wat heeft gezorgd voor nieuwe manieren van waardecreatie en -captatie (Han et al., 2020; Alexander Osterwalder et al., 2019). Verder citeren Han et al. (2020) in hun artikel Al Debei en Avison (2010); Gordijn en Akkermans (2001); Lindgardt et al. 2009, deze artikelen geven aan dat met de nieuwe technologieën ook nieuwe uitwisselingsmechanismen, nieuwe transactiearchitecturen en nieuwe grensoverschrijdende organisatievormen in de hand heeft gewerkt.

### **Aanpasbaarheid bedrijfsmodel**

Wat in de huidige omgeving en vandaag logisch is, kan morgen uit de tijd zijn of zelfs onbruikbaar zijn (A Osterwalder & Pigneur, 2019). Een bedrijfsmodel in een veranderende omgeving heeft daardoor te maken met verschillende risicofactoren. Daarbij kan een bedrijf, zoals een Meezijdig platformbedrijf, onderdeel zijn van een keten waar inkomend aanbod invloed heeft op het vermogen van het Meezijdig platformbedrijf om binnen de verwachte/ beoogde kosten en tijd te voldoen aan de vraag van de klant (inclusief eventueel verwachte kwaliteit en kwantiteit) (Bradford, 2019; Manuj & Mentzer, 2008). In lijn hiermee kan een succesvolle klantervaring ontstaan, dat bestaat uit een soepele en onmiddellijk geleverde stimulatie die wordt geleverd met een gevoel van persoonlijke betekenis voor de ontvanger (Bradford, 2019).

### **Veranderende klantbehoeften**

Voor een Meezijdig platformbedrijf betekent dit dat de combinatie van hardware, software en gegevens ten minste het verwachte gevoel van beloning moet opleveren, omdat dan de ervaring van de klant aantrekkelijk genoeg is om het herhalen waard te zijn (Bradford, 2019). Zodoende is er bijvoorbeeld binnen Meezijdig platformbedrijf's ook een combinatie van gratis adverteren en freemium ontstaan (Jarid Lukin geciteerd in A Osterwalder & Pigneur, (2019)). Echter behoeft dit wel een juiste product of dienst in combinatie met veel trafic waardoor het platform interessant wordt voor adverteerders, wat het vervolgens mogelijk maakt fees te berekenen om gratis producten en diensten te subsidiëren voor klanten (A Osterwalder & Pigneur, 2019). Als de klant vervolgens of alsnog geen plezier ervaart bij het kopen, zal de prioriteit van de klant verschuiven van product naar (positieve/ negatieve) ervaring (Bradford, 2019).

### **Nieuwkomers – onrust stokers**

Zoals in het begin van deze paragraaf is verondersteld is dat de ontwrichtende innovatie invloed heeft op de markt, waar zogenoemde ontwrichters als concurrenten aanwezig zijn. Volgens de theorie van Han et al., (2020) zorgen de ontwrichters voor verstoring bij het bedienen van een (nieuwe) markt, wat door door A Osterwalder & Pigneur, (2019) als nieuwkomers/ onruststokers worden bestempeld. Dit ontstaat doordat nieuwkomers beginnen met het aanspreken van low-end of onbediende consumenten en migreren vervolgens naar de mainstream markt (Han et al., 2020). Ook kunnen marktverstoorders succes hebben door een markt te creëren die nog niet eerder of nooit bestond door de marketingregels te veranderen.

### **Netwerkeffecten**

Wallbach et al., (2019) hebben onderzoek gedaan naar de zogenoemde “cross- and same-side netwerk effecten binnen de context van een Meezijdig platformbedrijf voor B2B. Zij stellen dat in het geval van negatieve netwerkeffecten het voordeel van het gebruik van het platform afneemt met een extra abonnee als bijvoorbeeld de performance van het Meezijdig platformbedrijf afneemt. Hierbij is onderscheid gemaakt tussen de “same-side” en “cross-side” netwerkeffecten. “Same-side” netwerkeffecten treden op aan dezelfde kant van het platform tussen de organisaties binnen dezelfde actoren groep. “Cross-side” netwerkeffecten treden daarentegen op tussen de organisaties van de verschillende actorengroepen binnen het Meezijdig platformbedrijf.

### **Leveringsketen**

Zowel nationale als internationale leveringsketens hebben te maken met een bron van concurrentievoordeel en mogelijkheden in een grotere markt via het digitale ecosysteem. Een manager suggereerde in het artikel van Manuj & Mentzer, “als je internationaal gaat, stijgt de complexiteit aanzienlijk en wereldwijde leveringsketens leiden tot meer complexiteit, waardoor ook de risico’s toenemen”. Uit onderzoek blijkt dat dit te relateren is aan (sneller) toegang tot grondstoffen, financieringsmogelijkheden, arbeid, grotere markten, arbitragemogelijkheden en extra stimulansen om extra buitenlands kapitaal aan te trekken (Manuj & Mentzer, 2008). Naast deze voordelen zijn er uiteraard ook onzekerheden en daaruit voortvloeiende risico’s waarmee de wereldwijde leveringsketens worden geconfronteerd. Dit heeft te maken met de verscheidenheid en onderlinge verbondenheid van bedrijven. Leveranciers (samenwerkingsverbanden) die hun afspraken niet kunnen waarmaken vanwege een stagnering in de toeleveringsketen zorgen voor het risico dat het Meezijdig platformbedrijf potentiële omzet en winst dreigt te verliezen (Oduoza, 2020).

### **Afhankelijkheid informatietechnologie versus snelle technologische verandering**

Een van de belangrijkste afhankelijkheden voor de meeste organisaties is tegenwoordig de informatietechnologie-infrastructuur (IT) (Hopkin, 2018). Technologische innovatie is de laatste decennia in een stroomversnelling geraakt en geeft onbetwistbaar vorm aan het concurrentielandschap (Teece, 2012) en binnen de digitale economie. Bovendien is met de komst van het Internet het effect van organisatorische innovatie sterker geworden naarmate nieuwe bedrijfsmodellen de prestaties verbeteren en de levensvatbaarheid van nieuwe soorten ondernemingen mogelijk maken (Teece, 2012). In het bijzonder zorgt een Meezijdig platformbedrijf voor een flexibele en efficiënte informatie-uitwisseling tussen alle deelnemende organisaties (platform actoren), ook omdat tegelijkertijd het aantal interfaces worden verminderd waar anders veel meer communicatie vereist was (Wallbach et al., 2019). Platformen

vereisen geavanceerde hardware om enorme hoeveelheden gegevens door te sturen (Bradford, 2019). Het uitvallen van een computersysteem kan daarom zeer ontwrichtende gebeurtenis zijn (Hopkin, 2018). Het verlies van computergegevens kan zeer ernstig zijn voor een organisatie, en de kans is groter dat het verband houdt met hardware-problemen dan met andere problemen, zoals softwareproblemen, elektrische storingen of menselijke fouten (Hopkin, 2018).

### **Gegevensverlies**

Een ander punt van zorg voor organisaties is bescherming van gegevens en het mogelijke verlies van bedrijf kritische informatie en of persoonsgegevens (klantgegevens) door de organisatie (Hopkin, 2018). Wat in deze eeuw is veranderd, is dat informatietechnologie de noodzaak om fysieke infrastructuur en activa te bezitten, drastisch heeft verminderd. IT maakt het bouwen en opschalen van platforms veel eenvoudiger en goedkoper, maakt bijna wrijvingsloze deelname mogelijk waardoor netwerkeffecten worden versterkt, en verbetert de mogelijkheid om enorme hoeveelheden gegevens vast te leggen, te analyseren en uit te wisselen waardoor de waarde van het platform voor iedereen toeneemt (Van Alstyne et al., 2016).

### **Onethisch gebruik data**

Indien effectief gebruikt, stellen data bedrijven in staat om strategisch analyses uit te voeren om de ervaringswensen van hun klanten beter te voorspellen. Als gegevens echter op een onverwachte en ongewenste wijze door onbevoegden worden verzameld en gebruikt, kan een bedrijf de ervaring van een klant uithollen en sprake zijn van onethisch gebruik van data (Bradford, 2019).

### **Wet- en regelgeving**

Naast innovatieve voordelen voor consumenten, bedrijven, wetenschap en overheden, ontstaat er door de snelle ontwikkeling van online platforms ook wet- en regelgeving. Voorbeelden van risicofactoren hieromtrent zijn de ontwijking of vaagheid van toepasselijke wettelijke voorschriften (Heerschap et al., 2019). Vaak bestaan er ook matige of slechte arbeidsvoorwaarden, bijvoorbeeld in de zogenaamde gig economy (kleine banen) en nieuwe belastingkwesties (Heerschap et al., 2019). Enkele vormen van wet- en regelgeving die risicofactoren bevatten zijn:

- Privacy en consumentbescherming

Er zijn ook risico's met betrekking tot het gedrag van onlineplatforms wat de rechten van consumentenbescherming betreft. Bijvoorbeeld: i) in hoeverre zijn onlineplatforms



verantwoordelijk voor het gedrag en de handelingen van hun aanbieders, gebruikers en adverteerders (bv. terrorisme, pornografie en schendingen van intellectuele-eigendomsrechten); ii) in hoeverre zijn zij verantwoordelijk voor productveiligheid, iii) hoe gaan zij om met consumentenbeschermingsrechten (waaronder geschillenregelingen, behandeling en monitoring van klachten) en iv) hoe werkt het recht om toestemming te geven voor het gebruik van persoonsgegevens in de praktijk. Of meer in het algemeen: wie is de eigenaar van de gegevens? Het vinden van een goed evenwicht tussen privacy enerzijds en innovatiemogelijkheden anderzijds is een andere kwestie. Of in welke mate kunnen gegevens al dan niet worden gedeeld tussen online platforms (Heerschap et al., 2019)?.

- Mededinging

In de context van Meezijdige platformbedrijven binnen een digitale economie zijn de markten regelmatig nauw met elkaar verweven, zodat de beoordeling uit mededingingsoogpunt onvolledig zou zijn zonder een inter-marktanalyse (Holzweber, 2017). In de context van Meezijdige platformbedrijven is de afbakening van de relevante productmarkt een bijzonder delicate en complexe taak, waardoor het juridisch de nodige uitdagingen levert (Holzweber, 2017).

- Eigendomsrechten

In geavanceerde economieën met een goede infrastructuur, een goed overheidsbeleid, een rechtsstaat en sterke eigendomsrechten is innovatie de belangrijkste motor van economische groei (Teece, 2012). Dit betekent niet alleen innovatie in goederen en diensten, maar ook innovatie in de manier waarop bedrijven werken, zowel afzonderlijk als in combinatie (Teece, 2012). Hoewel vaak over het hoofd gezien, zijn organisatorische en managementinnovaties even belangrijk voor economische groei als technologische innovatie (Teece, 2012).

### **Financiële capaciteit**

Het vermogen van de onderneming om financiële steun te verlenen voor de verbetering en het onderhoud van de IT-omgeving kan effect hebben op de continuïteit (financiële gezondheid) van het bedrijf (ISACA, 2013). Gratis producten en diensten genereren bijvoorbeeld wel traffic voor een Meezijdig platformbedrijf en vergroten de aantrekkelijkheid voor adverteerders (A Osterwalder & Pigneur, 2019), echter leveren gratis producten en diensten geen inkomsten om de uitgaven te bekostigen. Daarbij hangen de belangrijkste kosten van een platform veelal samen met het ontwikkelen en onderhouden van het platform: ook kunnen kosten ontstaan voor het genereren van traffic en rentiekosten (A Osterwalder & Pigneur, 2019).

### **Cultuur, ethiek en gedrag**

De cultuur van een organisatie is moeilijk te definiëren, maar het wordt over het algemeen aanvaard dat zij een weerspiegeling is van de algemene houding het management op ieder niveau binnen een bedrijf (Hopkin, 2018; NEN, 2019). De cultuur van een organisatie bepaalt hoe individuen zich in bepaalde omstandigheden zullen gedragen. Zij bepaalt hoe een individu zich in alle omstandigheden verplicht voelt zich te gedragen (Hopkin, 2018). Binnen Cobit 5 for Risk is dit nog eens opgesplitst naar interne en externe belanghebbenden.

Een risicocultuur zal het product zijn van individuele en groepswaarden en van houdingen en gedragspatronen (Hopkin, 2018). Dit zal leiden tot een engagement ten aanzien van de risicomanagementdoelstellingen van de organisatie (COSO, 2017; Hopkin, 2018; NEN, 2019). Organisaties met een risicobewuste cultuur worden gekenmerkt door communicatie die gebaseerd is op wederzijds vertrouwen en een gedeelde perceptie van het belang van risicomanagement (Hopkin, 2018). Ook moet er sprake zijn van wederzijds vertrouwen in de gekozen beheersingsmaatregelen en van de wil om de vastgestelde risicomanagementprocedures na te leven (COSO, 2013; Hopkin, 2018).

### **Governance**

De aandacht voor een meer geformaliseerde aanpak voor risicomanagement is toegenomen in de hele wereld na markante mislukkingen van een aantal grote organisaties. Het is voor deze thesis geen doel om corporate governance volledig uit te kristalliseren. Echter, blijkt uit de verschillende jaarverslagen en de casestudie, dat verantwoordende teksten over “Corporate Governance” zijn opgenomen in combinatie met “risicomanagement” en “interne controle”. Corporate governance, risicomanagement en interne controle bestaan in alle grote economieën en zijn bedoeld om de activa, de winstcapaciteit en de reputatie van organisaties te beschermen (Alphabet Inc., 2019; Amazon.com Inc., 2021; Inc., 2020; Murray-Webster & Williams, 2010; Vostok New Ventures, 2019).

Verschillende landen hebben voor beursgenoteerde bedrijven daarom een Corporate Governance Code opgesteld dat overeenkomt met de geldende lokale wetgeving, zoals in Nederland, United Kingdom en de United States. De Corporate governance gaat over besturen en beheersen, over verantwoordelijkheid en zeggenschap en over toezicht en verantwoording (Strikwerda, 2016). Het doel van de Corporate Governance bij deze beursgenoteerde vennootschappen is het met of in relatie tot wet- en regelgeving bewerkstelligen van een deugdelijk en transparant stelsel van checks and balances en het daartoe reguleren van de verhoudingen tussen het bestuur, de raad van commissarissen en de algemene

vergadering/ aandeelhouders (Strikwerda, 2016). Het doel van corporate governance volgens de UK Het komt erop neer dat corporate Governance Code het bevorderen is van doeltreffend ondernemerschap en prudent management dat een onderneming op lange termijn succes kan bezorgen. Binnen de ISO 31000 geeft governance richting aan de koers van de organisatie, haar externe en interne relaties, de regels, processen en werkwijzen die nodig zijn de doelstellingen van de organisatie te bereiken (NEN, 2019). Hierbij is aangenomen dat de raad van bestuur verantwoordelijk is voor het bepalen van de aard en de omvang van de (significante) risico's die zij bereid is te nemen om haar strategische doelstellingen te bereiken (Bayens & Tönissen, 2015; FRCL, 2018; Strikwerda, 2016). Dit beschrijft de Nederlandse Corporate Governance Code samengevat als; besturen en beheersen, verantwoordelijkheid nemen en zeggenschap hebben, toezicht en verantwoording (Strikwerda, 2016).

Volgens 't Hart, (z.d.); COSO, (2017) en NEN, (2019) hangt de doeltreffendheid van risicomanagement af van de integratie ervan in de governance van de organisatie, met inbegrip van de besturing van de organisatie en de besluitvorming. Volgens Bayens & Tönissen, (2015) en Bosch, (1997) omvat de governance daarom de verantwoordelijkheden en de activiteiten van het ondernemingsbestuur en het management, die tot doel hebben:

- Strategische richting te geven aan het functioneren en de ontwikkeling van de organisatie;
- Zeker te stellen dat de gestelde doelen worden bereikt;
- Dat de risico's afdoende worden beperkt; en
- Dat middelen van de onderneming op een verantwoorde wijze worden ingezet.

### **Bestuurlijke randvoorwaarden**

Governance enablers zijn de organisatorische middelen, zoals kaders, beleid, beginselen, structuren, en praktijken, door middel waarvan of waarop acties worden gericht en doelstellingen kunnen worden bereikt. Tot de enablers behoren ook de bestuurlijke en strategische inzet van capaciteit, zoals dienstverleningscapaciteiten (IT-infrastructuur, toepassingen, enz.), mensen en informatie.

Iedereen binnen de organisatie heeft te maken met eigen verantwoordelijkheden en eigenaarschap ten aanzien van kernprocessen, de organisatie, risicomanagement, e.d. en behoort zich daar bewust van te zijn. Het is belangrijk dat eigen belangen en verwarring inzake verantwoordelijkheden en eigenaarschap worden weggewerkt en toezicht wordt gehouden op de risicomanagementprestaties.

### Three lines of defence

Een aanpak die in de laatste jaren steeds populairder is geworden, wordt meestal aangeduid met de term "three lines of defence". Het 3LoD-model heeft vele ouders en geen ouders. De oorsprong ervan is onduidelijk, maar het is door veel regelgevers en bedrijven overgenomen. Hoewel het concept theoretisch aantrekkelijk is, kan het er ook toe leiden dat de verantwoordelijkheden voor risico's zodanig worden verspreid dat de verantwoordingsplicht eerder afneemt dan toeneemt (Davies & Zhivitskaya, 2018). Een definitief oordeel over de doeltreffendheid ervan kan nog niet worden geveld (Davies & Zhivitskaya, 2018).

De "three lines of defence" is gebaseerd op het idee dat: 1) het management primair verantwoordelijk is voor risicomanagement; 2) specifieke risicomanagementfuncties het management kunnen bijstaan bij het ontwikkelen van een aanpak om hun verantwoordelijkheden na te komen; en 3) de interne-auditfunctie nagaat of het risicomanagementproces en het risicobeheersingskader effectief en efficiënt zijn (Hopkin, 2018; Instituut voor Interne Auditors, 2007). De "three lines of defence" benadering is ook verenigbaar met het concept governance, risicomanagement en compliance (afgekort als "GRC") (Hopkin, 2018; ISACA, 2013). De GRC-benadering is gebaseerd op de algemene opvatting dat de Raad van Bestuur verantwoordelijk is voor governance-aangelegenheden in de hele organisatie (Hopkin, 2018). In deze rol zal de raad van bestuur naar alle drie de verdedigingslijnen kijken om ervoor te zorgen dat er voldoende aandacht aan risico's wordt besteed (Hopkin, 2018). De directie en toezichthoudende organen, voor zover van toepassing, behoren ervoor te zorgen dat de bevoegdheden, verantwoordelijkheden, en verantwoordingsplichten voor relevante rollen met betrekking tot risicomanagement op alle niveaus van de organisatie worden toegewezen en gecommuniceerd en behoren:

- te benadrukken dat risicomanagement een kernverantwoordelijkheid is;
- personen te identificeren met verantwoordingsplicht en bevoegdheid voor het managen van risico's (risico-eigenaren) (NEN, 2019).

Externe auditors moeten de juistheid van de financiële gegevens bevestigen en in sommige gevallen een attest afgeven (Hopkin, 2018; Instituut voor Interne Auditors, 2007). Deze externe auditors kunnen worden beschouwd als de vierde verdedigingslinie (Hopkin, 2018). In het geval van sterk gereguleerde organisaties zullen er bovendien toezichthouders zijn die eisen dat de regels en voorschriften binnen hun werkingssfeer worden nageleefd (Hopkin, 2018). In die omstandigheden kan de regelgever worden beschouwd als de vijfde verdedigingslinie (Hopkin, 2018).

Het is onvermijdelijk dat er variaties op het hierboven beschreven model bestaan en dat verschillende organisaties een structuur voor de vijf verdedigingslijnen ontwikkelen die aansluit bij de specifieke behoeften (Hopkin, 2018). De belangrijkste verbetering ten opzichte van de benadering met drie verdedigingslijnen, zoals die door de vijf verdedigingslijnen wordt geboden, is dat de eerste verdedigingslijn is onderverdeeld in het bestuur, de hogere leidinggevenden en de leiders van de bedrijfseenheden, waarbij elk van deze groepen verantwoordelijk is voor het verschaffen van zekerheid met betrekking tot de aan hen toegewezen verantwoordelijkheden (Hopkin, 2018).

### ***Bijlage C.      Aanvullende verantwoording onderzoek***

#### **Literatuuronderzoek**

Omwillen van drie redenen is een literatuurreview uitgevoerd. De eerste reden voor literatuur review is het plaatsen van het onderzoek in een wetenschappelijk perspectief. De tweede reden voor literatuurreview is het vermijden van duplicatie en replicatie van onderzoek – het uitvoeren van hetzelfde eerder uitgevoerde onderzoek zonder het te verbeteren. De derde reden voor de literatuurreview is pragmatischer. De literatuurreview wordt gebruikt om moeilijkheden die andere onderzoekers in hun onderzoek hebben ondervonden te vermijden of op te lossen. Hierom zal literatuur gezocht over de theorie, methodes en betreffende de data analyses.

Verschillende bestaande literaire bronnen zijn gebruikt en vergeleken. Van de overeenkomende kenmerken binnen de verschillende omschrijvingen is samenvattend begrip gemaakt. Hierbij zijn al wel zoveel mogelijk raakvlakken gezocht met de omgevingscontext van de case Bovemij. Vervolgens is gekozen voor de meest voorkomende beschrijving voor de definitie.

Binnen dit onderzoek is het geen doel om alle definities te analyseren om te komen tot een nieuwe definitie. Naast het definiëren van de kernbegrippen in relatie tot de hoofdvraag is binnen de literatuur gezocht naar begrippen voor de verdere uitwerking binnen het risicomanagementraamwerk voor Bovemij.

#### **Keuze model voor bedrijfskenmerken / typologie bedrijf**

Meerzijdige platformbedrijf hebben de laatste jaren veel aandacht gekregen in het wetenschappelijk onderzoek. Zoals McIntyre et al. in 2018 al aangaven is de invloed van meerzijdige platformbedrijf steeds relevanter geworden in een breed scala van industrieën. Ondanks de theoretische vooruitgang in de wetenschap, blijkt uit de onderzoeken van McIntyre et al. (2018) en Eisape (2019) dat er nog verschillende

kernvragen blijven bestaan over de bedrijfsmodellen van de meezijdige platformbedrijf. In deze thesis is het onderzoeken en ontwikkelen van een bewezen bedrijfsmodel voor een meezijdig platformbedrijf geen onderdeel van de onderzoeksdoelstelling en scope. In verschillende literatuur wordt echter benadrukt dat een business model aanpak voor het onderzoeken, begrijpen en beschrijven van een bepaalde organisatie een nuttig analytisch kader biedt.

### **Novius Architectuur Methode en Osterwalder Canvas**

Voor de kaders van het literatuuronderzoek is, in relatie tot het doel van het onderzoek, gekozen om de Bedrijfsarchitectuur principes te gebruiken op basis van de Novius Architectuur Methode. Deze methode gaat uit van de strategische dialoog tussen bestuurders, managers en de 'inrichters' van het bedrijf, te starten met het bedrijfsinrichtingsplan (BIP) (den Hoed, 2013). Dit sluit eveneens met de principes van COSO en de ISO over het risicomanagementraamwerk. In beide raamwerken is opgenomen dat risicomanagement en risico's behoren aan te sluiten met de bedrijfscontext ofwel het integreren van risicomanagement in de organisatiestructuren en -context (COSO, 2017; NEN, 2019).

De Novius Architectuur Methode levert vooral een bijdrage aan het optimale ontwerp van de bedrijfsinrichting waardoor de klantwaarde kan toenemen en de operationele kosten en ontwikkelkosten lager kunnen blijven (Bayens & Tönissen, 2015; den Hoed, 2013). De methode levert in mindere mate een bijdrage aan het opnemen van een waardepropositie in het bedrijfsmodel, de wijze waarop het bedrijf geld wil verdienen en/ of waarde wil creëren voor de maatschappij (den Hoed, 2013; Alexander Osterwalder et al., 2019). Daarom is - in relatie tot de scope van het onderzoek - voor de beschrijving van het bedrijfsmodel gekozen om het Osterwalder Business Model Canvas te gebruiken als aanvulling op de Novius Architectuur methode. Dit model is een van de onderzochte modellen in de artikelen "The Platform Business Model Canvas a Proposition in a Design Science Approach" van Eisape (2019) en "Virtual Reality Enriched Business Model Canvas Building Blocks for enhancing Customer Retention" van Brunner & Wolfartsberger (2020). In deze artikelen is beschreven dat zij verschillende modellen hebben onderzocht en komen in hun onderzoek uit op het Osterwalder Business Model Canvas voor meezijdige platformbedrijf. Ze noemen dit een dergelijk instrument dat bedrijven die veranderen en innoveren een meerwaarde biedt voor verschillende doeleinden: delen, communicatie (intern en extern), beschrijving, analyse, management, planning en partnering (Brunner & Wolfartsberger, 2020; Eisape, 2019). Daarnaast biedt het Osterwalder Business Model Canvas een pragmatische en toch ook systematische aanpak om een bestaand platformbedrijfsmodel te beschrijven.

Het Osterwalder Canvas model in combinatie met het wetenschappelijke artikel van Yablonsky (2019) is gehanteerd als een wijze om de business- en waarde drivers van een meezijdig platform bedrijf te kunnen structureren en analyseren. Het Canvas model is een conceptueel basiskader en bestaand managementinstrument voor het beschrijven, analyseren en interpreteren van bedrijfsinstrumenten dat in de literatuur over digitale platforms veelvuldig voorkomt. In de combinatie met de Novius Architectuur methode, helpen de kaders van het Canvas model als het artikel van Yablonski (2019) helpen ook voor het gestructureerd en systematisch vastleggen van waarde uit technologie, de grenzen van een bedrijf, het leggen van directe verbanden tussen de bedrijfsstrategie en de bedrijfsprocessen en hoe een Meezijdig platformbedrijf daaruit winst genereert.

### **Risicomanagement theorieën**

Het boek “Fundamentals of Risk Management” van Hopkin, (2018) is gehanteerd voor de structuur van risicomanagement. Dit boek is bedoeld voor iedereen die een uitgebreide inleiding wil in de theorie en de toepassing van risicomanagement. Het geeft een geïntegreerde kijk op risicomanagement in verschillende openbare en particuliere organisaties. Hierdoor is in mindere mate op de neiging in te gaan om het risicomanagement voor banken en verzekeraars toe te passen, omdat dit veelvuldig voorkomt bovenaan de zoeklijsten op het internet.

De risicomanagement richtlijn ISO 31000 en het raamwerk COSO ERM komen veelvuldig voor in de literatuur als onderdeel van “Enterprise Risicomanagement”. Deze raamwerken besteden aandacht aan het opzetten en implementeren van alomvattend risicomanagement binnen bedrijven om te zorgen dat deze bedrijven zich kunnen aanpassen aan onder andere economische globalisering, concurrentie en om internationale markten betreden (COSO, 2017; Guo Yuntao, Li Suike, 2011; NEN, 2019).

Het COBIT raamwerk is aangedragen door de CDOO<sup>22</sup> van Bovemij en op 31-10-2021 is definitief besloten om dit raamwerk te gaan hanteren voor Bovemij. Het COBIT® (Control Objectives for Information and related Technology) raamwerk is vervolgens voor het risicomanagementraamwerk gebruikt omdat dit raamwerk internationaal breed is toegepast binnen organisaties met een sterke informatietechnologie-omgeving (Kagermann C, Kinney H, Kuting W, 2008). Dit raamwerk is in de laatste jaren geüpdatet

---

<sup>22</sup> Chief Digital Operating Officer



waardoor onder andere governance, risicomanagement, compliance en informatiebeveiliging een prominere rol hebben gekregen (Steuperaert, 2019).

Gezien een Meezijdig platformbedrijf kenmerken vertoont van een technologiebedrijf is het artikel “Risk Management Guide for Information Technology Systems” van Stoneburner et al., (2002) gehanteerd. Dit is voornamelijk gehanteerd voor de theorie over het risicomanagementproces zoals dit toegepast kan worden bij een technologiebedrijf.

### **Conceptuele fundamenten voor het multi-case (praktijk) onderzoek**

Het literatuuronderzoek resulteert in eerste instantie naar het construeren van de conceptuele fundamenten om het case onderzoek objectief, systematisch en gestructureerd uit te kunnen voeren. Met de opbouw van de conceptuele fundamenten is gestreefd naar een eenvoudig kader dat bijdraagt aan de analyse van de verschillende cases binnen verschillende industrieën te vereenvoudigen. Deze benadering bleek bijzonder nuttig voor het case onderzoek vanwege het huidige gebrek aan systematische empirische analyse op het gebied onderzoeken naar risicomanagement binnen een Meezijdig platformbedrijf.

## Bijlage D. Resultaten diagnose Bovemij Risicomanagement

### Opstellen criteria & vragenlijst

Gedurende de periode van januari 2021 tot en met september 2021 hebben Bovemij en KPMG gezamenlijk de criteria opgesteld die ten grondslag aan deze volwassenheidsmeting liggen.

Op basis van de volwassenheidscriteria zijn op de volgende onderwerpen vragen geformuleerd ten behoeve van het meten van het volwassenheidsniveau binnen de entiteiten van Bovemij:

- Risicostrategie en risicobereidheid
- Governance en organisatie
- Cultuur en gedrag
- Beleid en proces
- Risicomanagementproces
- GRC tooling

Op de volgende pagina worden per onderwerp de definities getoond die in deze volwassenheidsmeting zijn gehanteerd. Zowel de criteria als de vragenlijst zijn in een eerder stadium opgeleverd en gedeeld met Bovemij d.d. 16-09-2021 in het bestand *Criteria per volwassenheidsniveau\_Definitief.pdf*.

### Uitzetten vragenlijst

Ten behoeve van de privacy van de deelnemers en de kwaliteit van dit onafhankelijke onderzoek heeft KPMG het totaal aantal gevraagde links (98) naar de vragenlijst gegenereerd en gedeeld met Bovemij. Bovemij heeft op haar beurt de links naar de betreffende personen binnen onderstaande bedrijfsentiteiten verzonden om de anonimiteit van de deelnemers te garanderen:

- Bovemij Holding
- Financieringsmaatschappij
- Bovemij Interne Diensten

- ViaBOVAG
- ViaBovemij
- Commercie
- Schadeverzekering-Maatschappij
- RDC
- Stichting Rechtsbijstand Mobiliteit

### Respons op vragenlijst

De vragenlijst is gedurende twee weken beschikbaar geweest. Van de 98 uitgenodigde respondenten hebben 51 personen de vragenlijst geopend, 43 hebben de eerste vraag van het eerste onderwerp beantwoord en 33 van hen hebben de vragenlijst in z'n volledigheid afgerond. In de analyse van de beantwoording van de vragenlijst is ervoor gekozen om ook de respons van de niet afgeronde vragenlijsten mee te nemen en daarmee gehoor te geven aan de mening en het perspectief van de personen die de moeite hebben genomen de vragenlijst te starten.

Bovemij heeft op basis van de respons besloten in deze rapportage te focussen op de volgende (sub)groepen:

- Alle bedrijfsentiteiten, hierna: Bovemij Groep (43 respondenten gestart, 33 afgerond)
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij (25 respondenten gestart, 21 afgerond)
- De bedrijfsentiteit Schadeverzekering-Maatschappij (18 respondenten gestart, 12 afgerond)

Dit rapport beschrijft op bovenstaand (sub)groepsniveau het volwassenheidsniveau per onderwerp en eventuele bijzonderheden die uit de reacties op de vragenlijst volgden.

### Getoetste onderwerpen

Bovemij en KPMG hebben gezamenlijk de criteria opgesteld die ten grondslag aan deze volwassenheidsmeting liggen. De volwassenheidscriteria omvatten de op pagina 5 geïntroduceerde zes onderwerpen, aan de hand waarvan de uiteindelijke vragen geformuleerd zijn. Deze slide bevat een overzicht van deze onderwerpen met bijbehorende definities.

<b>Risicostrategie en risicobereidheid</b>	Uitgangspunten voor de wijze waarop Bovemij omgaat met risico's (vermijden, accepteren, verminderen of delen/overdragen van risico's). De risicobereidheid is de kwalitatieve beschrijving van de risico's die Bovemij bereid is te nemen of wat onmiddellijke actie en aandacht vereist bij het nastreven van de organisatie-doelstellingen.
<b>Governance en organisatie</b>	Onder 'Governance en organisatie' wordt de structuur verstaan waarbinnen Bovemij haar risicomanagementactiviteiten stuurt, monitort en hierover rapporteert. Deze organisatiestructuur omvat naast de rollen, verantwoordelijkheden, taken en bevoegdheden ook de communicatie-, rapportage- en escalatielijnen.
<b>Cultuur en gedrag</b>	Onder cultuur en gedrag vallen de 'shared values' en het tonen van commitment. Daarnaast betreft dit het lerend vermogen van de organisatie door een 'fouten maken mag' houding, aanspreken op eigenaarschap/verantwoordelijkheden en het spreken in een gemeenschappelijke taal om elkaar te helpen de dialoog op gang te brengen en houden. Het gaat over het hebben van een gemeenschappelijk beeld van en visie op risicomanagement en risico's.
<b>Beleid en proces</b>	Onder risicomanagementbeleid en -proces worden de beleidsdocumenten verstaan voor Bovemij (en onderliggende bedrijfsentiteiten) en de bijbehorende processen verstaan die worden gebruikt met als doel het bewerkstelligen van een aantoonbare, adequate beheersing van de risico's in relatie tot de doelstellingen van Bovemij.
<b>Risicomanagementproces</b>	Het risicomanagementproces zijn de activiteiten om risico's te identificeren, te beoordelen, te prioriteren en erover te rapporteren, met als doel inzicht te krijgen in de mate waarin relevante risico's impact hebben op het behalen van de organisatie-doelen. Daarnaast is het de wijze waarop wordt omgegaan met de geïdentificeerde risico's door deze te vermijden, te accepteren, te delen of beheersmaatregelen te implementeren met als doel de risico's te beheersen en te mitigeren.
<b>GRC tooling</b>	Binnen het element 'GRC tooling' is de mate van gebruik van geïntegreerde, bedrijf brede systemen voor risicobeheersing (GRC-tooling) beoordeeld, waarbij ook actie- en incidentenmanagement zijn meegenomen.

### Te toetsen onderwerpen

De onderwerpen waarop het volwassenheidsniveau van de entiteiten van Bovemij is getoetst zijn op de vorige pagina toegelicht aan de hand van de binnen dit onderzoek gehanteerde definities.

Voor het meten van het volwassenheidsniveau op de onderwerpen Risicostategie en risicobereidheid, Governance en organisatie, Beleid en proces en Risicomanagementproces zijn vijf vragen geformuleerd. Voor de onderwerpen GRC tooling en Cultuur en gedrag zijn vier vragen geformuleerd. Voor details over de vragenlijst en de volwassenheidscriteria wordt verwezen naar het document dat eerder met Bovemij gedeeld is.

### Bepaling volwassenheidsniveau

Bij elke vraag zijn 6 antwoordmogelijkheden geformuleerd. Antwoorden 1 t/m 5 komen overeen met de gedefinieerde volwassenheidsniveaus. Met antwoordmogelijkheid 6 kon de respondent aangeven niet te weten wat er met de vraag bedoeld werd. Enerzijds kan de interpretatie van het kiezen voor optie 6 zijn dat de respondent geheel niet bekend is met het onderwerp van de vraag, anderzijds kan het kiezen van optie 6 ook betekenen dat de vraagstelling niet de gewenste associatie heeft opgeleverd bij de respondent. Omdat optie 1 het laagste volwassenheidsniveau representeert en de keuze voor optie 1 betekent dat de respondent de vraag goed begrepen heeft, zijn alleen de responses waarbij voor antwoordmogelijkheid 1 t/m 5 is gekozen gebruikt in het meten van het volwassenheidsniveau.

Vanwege de directe link tussen de volwassenheidsniveaus en de waarde van de antwoordkeuze (1 t/m 5) kan het volwassenheidsniveau per onderwerp, per functie, per entiteitsgroepering en op totaalniveau bepaald worden door het gemiddelde van de waarden van de gegeven antwoorden te nemen, die zijn gewogen met het aantal geldige gegeven antwoorden. De keuze voor antwoordoptie 6 is dus niet als geldig gegeven antwoord geteld in de weging voor de gemiddelden. Vanzelfsprekend zijn niet gegeven antwoorden zoals

door het afbreken van de vragenlijst ook niet meegenomen in de weging voor de gemiddelden.

*Hierbij willen wij nogmaals herhalen bij het lezen van deze rapportage rekening te houden met het feit dat de getoonde scores gebaseerd zijn op de perceptie van de medewerkers in de eerste lijn van Bovemij en daarmee niet per definitie het volwassenheidsniveau dat ook aantoonbaar kan worden gemaakt noch de perceptie van de 2e lijn of KPMG reflecteren.*

### Opsplitsing subgroepen

Bovemij heeft op basis van de respons besloten in deze rapportage te focussen op de onderstaande (sub)groepen:

- Alle bedrijfsentiteiten, hierna: Bovemij Groep (43 respondenten gestart, 33 afgerond)
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij (25 respondenten gestart, 21 afgerond)
  - Bovemij Holding
  - Financieringsmaatschappij
  - Bovemij Interne Diensten
  - ViaBOVAG
  - ViaBovemij
  - Commercie
  - RDC
  - Stichting Rechtsbijstand Mobiliteit
- De bedrijfsentiteit Schadeverzekering-Maatschappij (18 respondenten gestart, 12 afgerond)

De opsplitsing en naamgeving van deze (sub)groepen heeft in overeenstemming met Bovemij plaatsgevonden.

### Beoordelingskader

Onderstaand beoordelingskader bevat een verkorte omschrijving van de criteria zoals geformuleerd in het door Bovemij en KPMG opgestelde document. Dit document is in een eerder stadium opgeleverd en gedeeld met Bovemij d.d. 16-09-2021 in het bestand *Criteria per volwassenheidsniveau\_Definitief.pdf*.

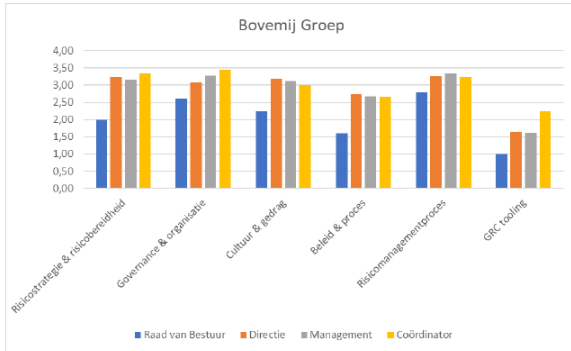
Niveau	Beoordeling	Omschrijving
1	Initieel	Geen strategie of bereidheid geformuleerd, geen integraal risicomanagementbeleid beschikbaar, geen vast systeem of methode en geen inzicht in (beleids-)risico's.
2	Informeel en ad-hoc toepassing	Enige basiskennis aanwezig, maar nog weinig ervaring en onvoldoende besef van wat risicomanagement inhoud en hoe risico's samenhangen in het integrale geheel. Beslissingen op basis van gevoel, documentatie en richtlijnen gedeeltelijk of incompleet beschikbaar en worden weinig geraadpleegd. Risicobereidheid informeel vastgelegd en ad-hoc toegepast.
3	Structureel en gestandaardiseerd	Periodieke communicatie, geringe documentatie omtrent risicostategie- en bereidheid. Risicomanagement draagt bij aan missie, visie en strategie. Risicomanagement formeel vastgelegd en ingebed, maar nog verbetering te halen op het gebied van de beleving van de verantwoordelijkheid organisatie-breed.
4	Integraal en gemanaged	Consistente, periodieke en aantoonbare toepassing van risicomanagementbeleid, ook in de besluitvorming. Tekortkomingen worden geconstateerd en maatregelen worden geformuleerd en nageleefd. Organisatie-brede betrokkenheid bij het risicomanagement. Het risicomanagement wordt ondersteund door tooling.
5	Continu verbeteren/optimaliseren	Risicomanagementbeleid organisatie-breed ingebed en dagelijks toegepast, medewerkers onderkennen het belang van goed risicomanagement. Evaluaties vinden proactief en periodiek plaats. Tekortkomingen worden organisatie-breed geconstateerd, maatregelen worden geformuleerd en actief nageleefd. Tooling vast onderdeel van werkzaamheden en doorlopend getoetst aan interne visie en externe ontwikkelingen.

# Uitkomsten volwassenheidsmeting

## Bovemij Groep

Op basis van de resultaten van de 43 (gestarte) deelnemers scoren de bedrijfsentiteiten van Bovemij gemiddeld een 2,9 op een schaal van 5 voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een niveau dat nog net onder informele en ad-hoc toepassing valt, maar wat een gestructureerd en gestandaardiseerd niveau nadert.

Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten voor de bedrijfsentiteiten van Bovemij worden vanaf pagina 20 in meer detail beschreven.



### Interpretatie van resultaten

De scores die in deze sectie getoond worden bedragen het gemiddelde volwassenheidsniveau van het risicomanagement binnen de subgroepen:

- Bovemij Groep
- De bedrijfsentiteit Schadeverzekering-Maatschappij
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij

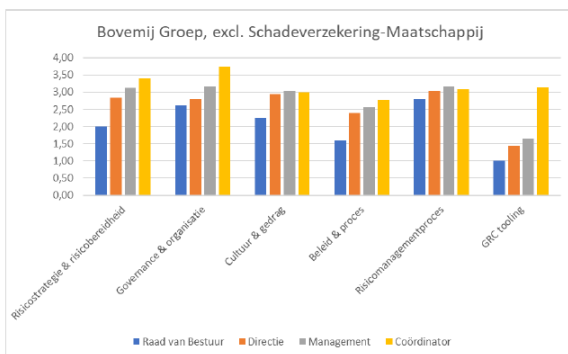
Zoals eerder aangegeven, volgen deze scores uit de perceptie van de medewerkers. Ook wordt er in deze fase van de volwassenheidsmeting nog geen waardeoordeel gegeven over de huidige scores. Teneinde een oordeel te kunnen vellen over het volwassenheidsniveau dat uit de nulmeting volgt, moet in een vervolgstap het ambitieniveau voor het risicomanagement worden vastgesteld voor Bovemij als geheel, of binnen de bedrijfsentiteiten van Bovemij.

# Uitkomsten volwassenheidsmeting

## Bovemij Groep, excl. Schadeverzekering-Maatschappij

Op basis van de resultaten van de 25 (gestarte) deelnemers scoort de Bovemij Groep, excl. Schadeverzekering-Maatschappij een 2,8 op een schaal van 5 voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een niveau dat nog net onder informele en ad-hoc toepassing valt, maar wat een gestructureerd en gestandaardiseerd niveau nadert.

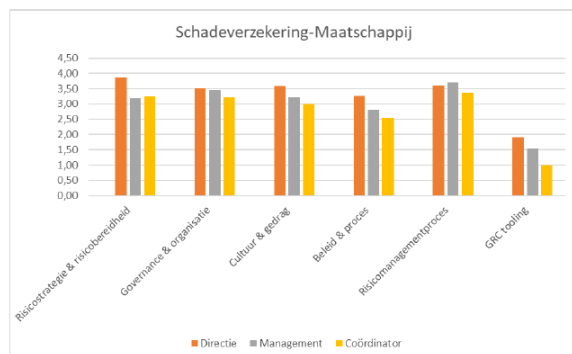
Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten Bovemij Groep, excl. Schadeverzekering-Maatschappij worden vanaf pagina 28 in meer detail beschreven.



## Schadeverzekering-Maatschappij

Op basis van de resultaten van de 18 (gestarte) deelnemers scoort de bedrijfsentiteit Schadeverzekering-Maatschappij gemiddeld een 3,1 op een schaal van 5 voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een gestructureerd en gestandaardiseerd volwassenheidsniveau.

Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten voor de bedrijfsentiteit Schadeverzekering-Maatschappij worden vanaf pagina 35 meer in detail beschreven.



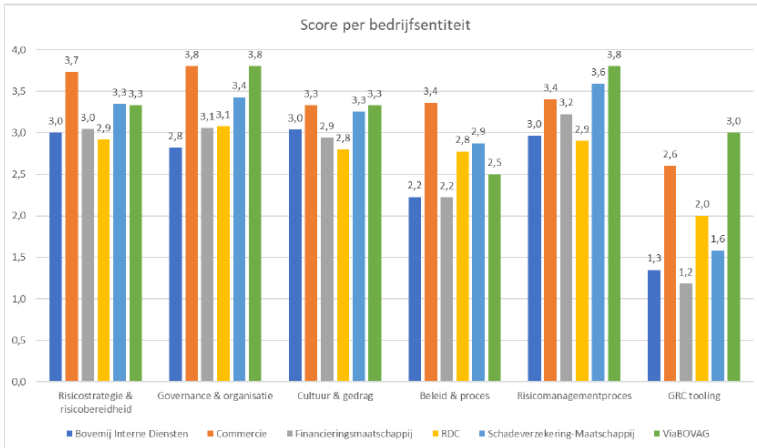
# Uitkomsten volwassenheidsmeting

## Gemiddelde score volwassenheid per bedrijfsentiteit

In de onderstaande figuur wordt het volwassenheidsniveau voor elk element uit het risicomanagementraamwerk per bedrijfsentiteit getoond. In de bepaling van de scores is geen onderscheid gemaakt naar functieomschrijving omwille van de privacy van de deelnemers. Als gevolg van het soms lage aantal respondenten worden daarom de bedrijfsentiteiten Bovemij Holding, ViaBovemij en Stichting Rechtsbijstand Mobiliteit niet getoond.

## Bijzonderheden

- Over het algemeen scoren de bedrijfsentiteiten Commercie en ViaBovag hoger dan de andere bedrijfsentiteiten, met uitzondering van beleid & proces voor ViaBovag.
- Schadeverzekering-Maatschappij scoort daarna het hoogst. Voor het element risicomanagementproces scoort Schadeverzekering-Maatschappij hoger dan Commercie.
- Voor alle bedrijfsentiteiten, behalve ViaBovag, geldt dat de laagste score op het element GRC tooling is.



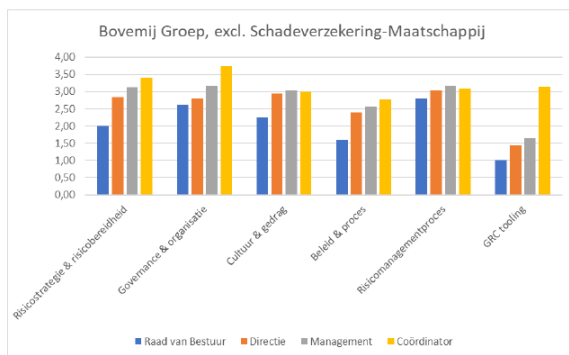
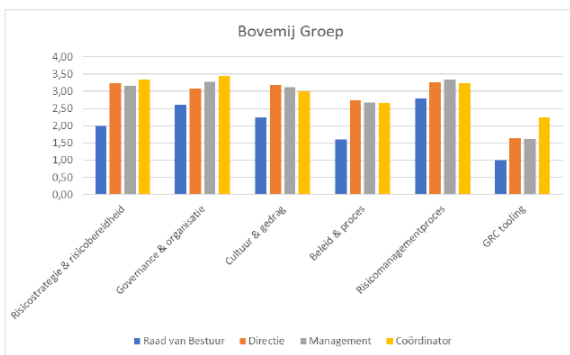
# Generieke aandachtspunten

## Bovemij Groep

- De bedrijfsentiteiten van Bovemij scoren gemiddeld net onder een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- GRC tooling is een aandachtspunt voor alle functies.
- Slechts één medewerker met functieomschrijving Raad van Bestuur heeft de vragenlijst beantwoord. De getoonde scores zijn slechts op één waarneming gebaseerd en mogelijk niet representatief.

## Bovemij Groep, excl. Schadeverzekering-Maatschappij

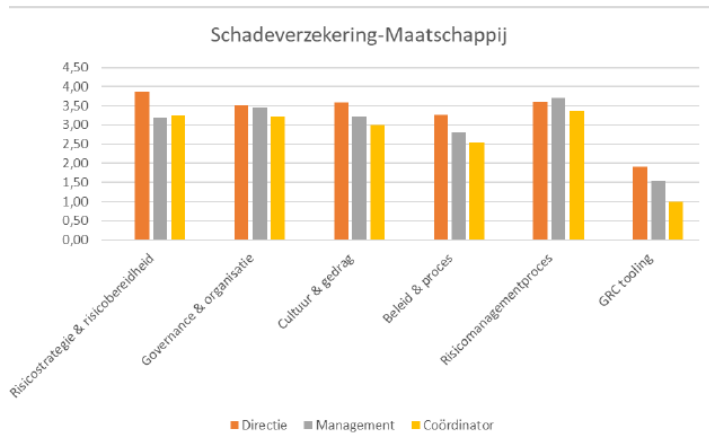
- De bedrijfsentiteiten van Bovemij Groep, excl. Schadeverzekering-Maatschappij scoren gemiddeld net onder een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- Op het element GRC tooling wordt door medewerkers met functieomschrijving Raad van Bestuur, Directie en Management in vergelijking met medewerkers in de functie Coördinator laag gescoord.
- De functieomschrijving Raad van Bestuur scoort lager dan andere functies, maar hier is maar één waarneming voor.



# Generieke aandachtspunten

## Schadeverzekering-Maatschappij

- De bedrijfsentiteit Schadeverzekering-Maatschappij scoort gemiddeld net boven een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- GRC tooling aandachtspunt voor alle functies, ook voor werknemers in de functie van coördinator in tegenstelling tot de andere bedrijfsentiteiten.





## Risicomanagement volwassenheidsmeting Bovemij

# Aanleiding volwassenheidsmeting

### Aanleiding

De risicomanagementfunctie van Bovemij heeft KPMG gevraagd om een nulmeting ter toetsing van de volwassenheid van het risicomanagementsysteem binnen Bovemij uit te voeren, hierna: volwassenheidsmeting. Een volwassenheidsmeting heeft als doel inzichtelijk te maken in welke mate het risicomanagement binnen een organisatie leeft en wordt toegepast in de werkzaamheden. Teneinde ook zicht te hebben op de ontwikkeling van het volwassenheidsniveau van het risicomanagement kan een volwassenheidsmeting gedurende een periode worden uitgevoerd. Hiertoe wordt in de eerste plaats een nulmeting uitgevoerd, waarna een of meerdere malen een toetsing van de resultaten uit de nulmeting kan plaatsvinden.

Bovemij en KPMG zijn overeengekomen dat de volwassenheidsmeting bij Bovemij gefaseerd wordt uitgevoerd, waarbij de volgende twee fasen zijn gedefinieerd:

1. Fase 1 – nulmeting o.b.v. vragenlijst
2. Fase 2 – toetsing resultaten nulmeting

### Fase 1 – nulmeting o.b.v. vragenlijst

De eerste fase betreft de nulmeting o.b.v. een vragenlijst die wordt uitgezet onder de medewerkers van de bedrijfsentiteiten van Bovemij. Aan de basis van de vragen in de vragenlijst liggen criteria die Bovemij samen met KPMG heeft opgesteld. Deze criteria beschrijven de mate van volwassenheid aan de hand van diverse onderwerpen zoals risicostrategie en –bereidheid. De onderwerpen die ten grondslag aan de vragenlijst van Bovemij liggen worden op pagina 5 onder de aanpak van de volwassenheidsmeting nader toegelicht.

De mate van volwassenheid op ieder onderwerp kan worden uitgesplitst naar meerdere niveaus van volwassenheid. Bovemij heeft ervoor gekozen onderscheid te maken naar vijf niveaus (nader toegelicht op pagina 8):

1. Initieel
2. Informele en ad-hoc toepassing
3. Gestructureerd en gestandaardiseerd
4. Integraal en gemanaged
5. Continu verbeteren/optimaliseren

De vragen en antwoordmogelijkheden in de vragenlijst zijn zodanig geformuleerd dat de eerste antwoordmogelijkheid het eerste niveau representeert en de vijfde mogelijkheid het vijfde niveau. Hetzelfde geldt voor de resterende vier niveaus.

In aanvulling op het uitzetten van een vragenlijst kan in de nulmeting ook meer kleur aan de meting worden gegeven door het voeren van gesprekken met de respondenten. Op deze manier kunnen bestaande kennis en ervaringen die niet in een vragenlijst te vatten zijn toch meegenomen worden in de meting. Het voeren van gesprekken heeft geen deel uitgemaakt van fase 1 en zal worden meegenomen in fase 2.

### Scope

Deze rapportage bevat de uitkomsten en bevindingen van fase 1, de nulmeting o.b.v. vragenlijst. Op pagina 5 wordt de aanpak en uitvoering van deze fase nader toegelicht.

*De getoonde scores zijn gebaseerd op de perceptie van de medewerkers in de eerste lijn van Bovemij en reflecteren daarmee niet per definitie het volwassenheidsniveau dat ook aantoonbaar kan worden gemaakt noch de perceptie van de 2e lijn of KPMG.*

# Aanpak volwassenheidsmeting

### Opstellen criteria & vragenlijst

Gedurende de periode van januari 2021 tot en met september 2021 hebben Bovemij en KPMG gezamenlijk de criteria opgesteld die ten grondslag aan deze volwassenheidsmeting liggen.

Op basis van de volwassenheidscriteria zijn op de volgende onderwerpen vragen geformuleerd ten behoeve van het meten van het volwassenheidsniveau binnen de entiteiten van Bovemij:

- Risicostrategie en risicobereidheid
- Governance en organisatie
- Cultuur en gedrag
- Beleid en proces
- Risicomanagementproces
- GRC tooling

Op de volgende pagina worden per onderwerp de definities getoond die in deze volwassenheidsmeting zijn gehanteerd. Zowel de criteria als de vragenlijst zijn in een eerder stadium opgeleverd en gedeeld met Bovemij d.d. 16-09-2021 in het bestand *Criteria per volwassenheidsniveau\_Definitief.pdf*.

### Uitzetten vragenlijst

Ten behoeve van de privacy van de deelnemers en de kwaliteit van dit onafhankelijke onderzoek heeft KPMG het totaal aantal gevraagde links (98) naar de vragenlijst gegenereerd en gedeeld met Bovemij. Bovemij heeft op haar beurt de links naar de betreffende personen binnen onderstaande bedrijfsentiteiten verzonden om de anonimiteit van de deelnemers te garanderen:

- Bovemij Holding
- Financieringsmaatschappij
- Bovemij Interne Diensten

- ViaBOVAG
- ViaBovemij
- Commercie
- Schadeverzekering-Maatschappij
- RDC
- Stichting Rechtsbijstand Mobiliteit

### Respons op vragenlijst

De vragenlijst is gedurende twee weken beschikbaar geweest. Van de 98 uitgenodigde respondenten hebben 51 personen de vragenlijst geopend, 43 hebben de eerste vraag van het eerste onderwerp beantwoord en 33 van hen hebben de vragenlijst in z'n volledigheid afgerond. In de analyse van de beantwoording van de vragenlijst is ervoor gekozen om ook de respons van de niet afgeronde vragenlijsten mee te nemen en daarmee gehoor te geven aan de mening en het perspectief van de personen die de moeite hebben genomen de vragenlijst te starten.

Bovemij heeft op basis van de respons besloten in deze rapportage te focussen op de volgende (sub)groepen:

- Alle bedrijfsentiteiten, hierna: Bovemij Groep (43 respondenten gestart, 33 afgerond)
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij (25 respondenten gestart, 21 afgerond)
- De bedrijfsentiteit Schadeverzekering-Maatschappij (18 respondenten gestart, 12 afgerond)

Dit rapport beschrijft op bovenstaand (sub)groepsniveau het volwassenheidsniveau per onderwerp en eventuele bijzonderheden die uit de reacties op de vragenlijst volgden.



# Aanpak volwassenheidsmeting

## Getoetste onderwerpen

Bovemij en KPMG hebben gezamenlijk de criteria opgesteld die ten grondslag aan deze volwassenheidsmeting liggen. De volwassenheidscriteria omvatten de op pagina 5 geïntroduceerde zes onderwerpen, aan de hand waarvan de uiteindelijke vragen geformuleerd zijn. Deze slide bevat een overzicht van deze onderwerpen met bijbehorende definities.

<b>Risicostrategie en risicobereidheid</b>	Uitgangspunten voor de wijze waarop Bovemij omgaat met risico's (vermijden, accepteren, verminderen of delen/overdragen van risico's). De risicobereidheid is de kwalitatieve beschrijving van de risico's die Bovemij bereid is te nemen of wat onmiddellijke actie en aandacht vereist bij het nastreven van de organisatiedoelstellingen.
<b>Governance en organisatie</b>	Onder 'Governance en organisatie' wordt de structuur verstaan waarbinnen Bovemij haar risicomanagementactiviteiten stuurt, monitort en hierover rapporteert. Deze organisatiestructuur omvat naast de rollen, verantwoordelijkheden, taken en bevoegdheden ook de communicatie-, rapportage- en escalatielijnen.
<b>Cultuur en gedrag</b>	Onder cultuur en gedrag vallen de 'shared values' en het tonen van commitment. Daarnaast betreft dit het lerend vermogen van de organisatie door een 'fouten maken mag' houding, aanspreken op eigenaarschap/verantwoordelijkheden en het spreken in een gemeenschappelijke taal om elkaar te helpen de dialoog op gang te brengen en houden. Het gaat over het hebben van een gemeenschappelijk beeld van en visie op risicomanagement en risico's.
<b>Beleid en proces</b>	Onder risicomanagementbeleid en -proces worden de beleidsdocumenten verstaan voor Bovemij (en onderliggende bedrijfsentiteiten) en de bijbehorende processen verstaan die worden gebruikt met als doel het bewerkstelligen van een aantoonbare, adequate beheersing van de risico's in relatie tot de doelstellingen van Bovemij.
<b>Risicomanagementproces</b>	Het risicomanagementproces zijn de activiteiten om risico's te identificeren, te beoordelen, te prioriteren en erover te rapporteren, met als doel inzicht te krijgen in de mate waarin relevante risico's impact hebben op het behalen van de organisatiedoelen. Daarnaast is het de wijze waarop wordt omgegaan met de geïdentificeerde risico's door deze te vermijden, te accepteren, te delen of beheersmaatregelen te implementeren met als doel de risico's te beheersen en te mitigeren.
<b>GRC tooling</b>	Binnen het element 'GRC tooling' is de mate van gebruik van geïntegreerde, bedrijf brede systemen voor risicobeheersing (GRC-tooling) beoordeeld, waarbij ook actie- en incidentenmanagement zijn meegenomen.

# Toelichting scores volwassenheidsmeting

## Te toetsen onderwerpen

De onderwerpen waarop het volwassenheidsniveau van de entiteiten van Bovemij is getoetst zijn op de vorige pagina toegelicht aan de hand van de binnen dit onderzoek gehanteerde definities.

Voor het meten van het volwassenheidsniveau op de onderwerpen Risicostrategie en risicobereidheid, Governance en organisatie, Beleid en proces en Risicomanagementproces zijn vijf vragen geformuleerd. Voor de onderwerpen GRC tooling en Cultuur en gedrag zijn vier vragen geformuleerd. Voor details over de vragenlijst en de volwassenheidscriteria wordt verwezen naar het document dat eerder met Bovemij gedeeld is.

## Bepaling volwassenheidsniveau

Bij elke vraag zijn 6 antwoordmogelijkheden geformuleerd. Antwoorden 1 t/m 5 komen overeen met de gedefinieerde volwassenheidsniveaus. Met antwoordmogelijkheid 6 kon de respondent aangeven niet te weten wat er met de vraag bedoeld werd. Enerzijds kan de interpretatie van het kiezen voor optie 6 zijn dat de respondent geheel niet bekend is met het onderwerp van de vraag, anderzijds kan het kiezen van optie 6 ook betekenen dat de vraagstelling niet de gewenste associatie heeft opgeleverd bij de respondent. Omdat optie 1 het laagste volwassenheidsniveau representeert en de keuze voor optie 1 betekent dat de respondent de vraag goed begrepen heeft, zijn alleen de responses waarbij voor antwoordmogelijkheid 1 t/m 5 is gekozen gebruikt in het meten van het volwassenheidsniveau.

Vanwege de directe link tussen de volwassenheidsniveaus en de waarde van de antwoordkeuze (1 t/m 5) kan het volwassenheidsniveau per onderwerp, per functie, per entiteitsgroepering en op totaalniveau bepaald worden door het gemiddelde van de waarden van de gegeven antwoorden te nemen, die zijn gewogen met het aantal geldige gegeven antwoorden. De keuze voor antwoordoptie 6 is dus niet als geldig gegeven antwoord geteld in de wegging voor de gemiddelden. Vanzelfsprekend zijn niet gegeven antwoorden zoals

door het afbreken van de vragenlijst ook niet meegenomen in de wegging voor de gemiddelden.

*Hierbij willen wij nogmaals herhalen bij het lezen van deze rapportage rekening te houden met het feit dat de getoonde scores gebaseerd zijn op de perceptie van de medewerkers in de eerste lijn van Bovemij en daarmee niet per definitie het volwassenheidsniveau dat ook aantoonbaar kan worden gemaakt noch de perceptie van de 2e lijn of KPMG reflecteren.*

## Opsplitsing subgroepen

Bovemij heeft op basis van de respons besloten in deze rapportage te focussen op de onderstaande (sub)groepen:

- Alle bedrijfsentiteiten, hierna: Bovemij Groep (43 respondenten gestart, 33 afgerond)
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij (25 respondenten gestart, 21 afgerond)
  - Bovemij Holding
  - Financieringsmaatschappij
  - Bovemij Interne Diensten
  - ViaBOVAG
  - ViaBovemij
  - Commercie
  - RDC
  - Stichting Rechtsbijstand Mobiliteit
- De bedrijfsentiteit Schadeverzekering-Maatschappij (18 respondenten gestart, 12 afgerond)

De opsplitsing en naamgeving van deze (sub)groepen heeft in overeenstemming met Bovemij plaatsgevonden.

# Toelichting scores volwassenheidsmeting

## Beoordelingskader

Onderstaand beoordelingskader bevat een verkorte omschrijving van de criteria zoals geformuleerd in het door Bovemij en KPMG opgestelde document. Dit document is in een eerder stadium opgeleverd en gedeeld met Bovemij d.d. 16-09-2021 in het bestand *Criteria per volwassenheidsniveau\_Definitief.pdf*.

Niveau	Beoordeling	Omschrijving
1	Initieel	Geen strategie of bereidheid geformuleerd, geen integraal risicomanagementbeleid beschikbaar, geen vast systeem of methode en geen inzicht in (beleids-)risico's.
2	Informeel en ad-hoc toepassing	Enige basiskennis aanwezig, maar nog weinig ervaring en onvoldoende besef van wat risicomanagement inhoud en hoe risico's samenhangen in het integrale geheel. Beslissingen op basis van gevoel, documentatie en richtlijnen gedeeltelijk of incompleet beschikbaar en worden weinig geraadpleegd. Risicobereidheid informeel vastgelegd en ad-hoc toegepast.
3	Structureel en gestandaardiseerd	Periodieke communicatie, geringe documentatie omtrent risicostrategie- en bereidheid. Risicomanagement draagt bij aan missie, visie en strategie. Risicomanagement formeel vastgelegd en ingebed, maar nog verbetering te halen op het gebied van de beleving van de verantwoordelijkheid organisatie-breed.
4	Integraal en gemanaged	Consistente, periodieke en aantoonbare toepassing van risicomanagementbeleid, ook in de besluitvorming. Tekortkomingen worden geconstateerd en maatregelen worden geformuleerd en nageleefd. Organisatie-brede betrokkenheid bij het risicomanagement. Het risicomanagement wordt ondersteund door tooling.
5	Continu verbeteren/optimaliseren	Risicomanagementbeleid organisatie-breed ingebed en dagelijks toegepast, medewerkers onderkennen het belang van goed risicomanagement. Evaluaties vinden proactief en periodiek plaats. Tekortkomingen worden organisatie-breed geconstateerd, maatregelen worden geformuleerd en actief nageleefd. Tooling vast onderdeel van werkzaamheden en doorlopend getoetst aan interne visie en externe ontwikkelingen.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

8

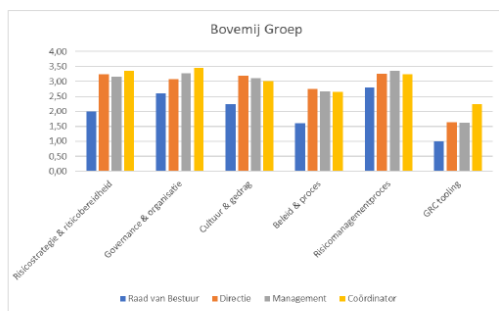
## Management Samenvatting van de volwassenheidsmeting

# Uitkomsten volwassenheidsmeting

### Bovemij Groep

Op basis van de resultaten van de 43 (gestarte) deelnemers scoren de bedrijfsentiteiten van Bovemij gemiddeld een **2,9** op een schaal van **5** voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een niveau dat nog net onder informele en ad-hoc toepassing valt, maar wat een gestructureerd en gestandaardiseerd niveau nadert.

Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten voor de bedrijfsentiteiten van Bovemij worden vanaf pagina 20 in meer detail beschreven.



### Interpretatie van resultaten

De scores die in deze sectie getoond worden bedragen het gemiddelde volwassenheidsniveau van het risicomanagement binnen de subgroepen:

- Bovemij Groep
- De bedrijfsentiteit Schadeverzekering-Maatschappij
- De bedrijfsentiteiten onder Bovemij Groep, excl. Schadeverzekering-Maatschappij

Zoals eerder aangegeven, volgen deze scores uit de perceptie van de medewerkers. Ook wordt er in deze fase van de volwassenheidsmeting nog geen waardeoordeel gegeven over de huidige scores. Teneinde een oordeel te kunnen vellen over het volwassenheidsniveau dat uit de nulmeting volgt, moet in een vervolgstap het ambitieniveau voor het risicomanagement worden vastgesteld voor Bovemij als geheel, of binnen de bedrijfsentiteiten van Bovemij.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

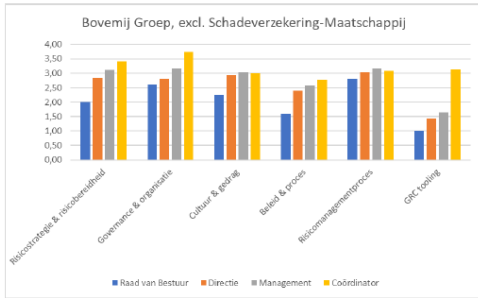
10

# Uitkomsten volwassenheidsmeting

## Bovemij Groep, excl. Schadeverzekering-Maatschappij

Op basis van de resultaten van de 25 (gestarte) deelnemers scoort de Bovemij Groep, excl. Schadeverzekering-Maatschappij een **2,8** op een schaal van **5** voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een niveau dat nog net onder informele en ad-hoc toepassing valt, maar wat een gestructureerd en gestandaardiseerd niveau nadert.

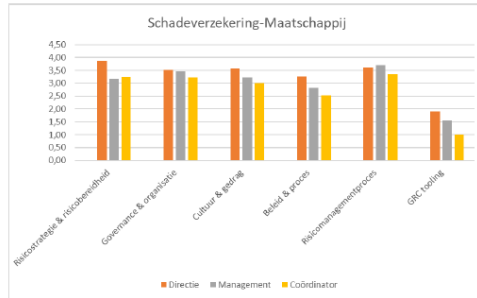
Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten Bovemij Groep, excl. Schadeverzekering-Maatschappij worden vanaf pagina 28 in meer detail beschreven.



## Schadeverzekering-Maatschappij

Op basis van de resultaten van de 18 (gestarte) deelnemers scoort de bedrijfsentiteit Schadeverzekering-Maatschappij gemiddeld een **3,1** op een schaal van **5** voor het volwassenheidsniveau van het risicomanagement. Dit getal representeert een gestructureerd en gestandaardiseerd volwassenheidsniveau.

Onderstaande figuur laat zien dat zowel per onderwerp als per functie verschillend gescoord is. De resultaten voor de bedrijfsentiteit Schadeverzekering-Maatschappij worden vanaf pagina 35 meer in detail beschreven.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

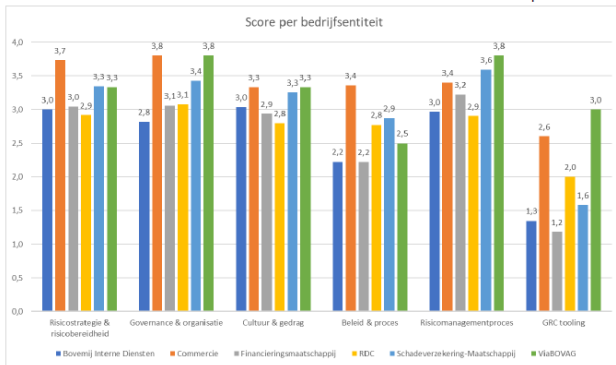
# Uitkomsten volwassenheidsmeting

## Gemiddelde score volwassenheid per bedrijfsentiteit

In de onderstaande figuur wordt het volwassenheidsniveau voor elk element uit het risicomanagementtraamwerk per bedrijfsentiteit getoond. In de bepaling van de scores is geen onderscheid gemaakt naar functietoetsing omwille van de privacy van de deelnemers. Als gevolg van het soms lage aantal respondenten worden daarom de bedrijfsentiteiten Bovemij Holding, ViaBovemij en Stichting Rechtsbijstand Mobiliteit niet getoond.

## Bijzonderheden

- Over het algemeen scoren de bedrijfsentiteiten Commercie en ViaBovag hoger dan de andere bedrijfsentiteiten, met uitzondering van beleid & proces voor ViaBovag.
- Schadeverzekering-Maatschappij scoort daarna het hoogst. Voor het element risicomanagementproces scoort Schadeverzekering-Maatschappij hoger dan Commercie.
- Voor alle bedrijfsentiteiten, behalve ViaBovag, geldt dat de laagste score op het element GRC tooling is.

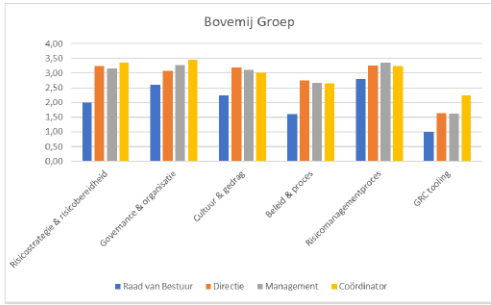


© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

# Generieke aandachtspunten

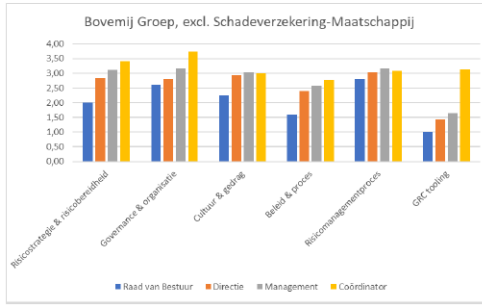
## Bovemij Groep

- De bedrijfsentiteiten van Bovemij Groep scoren gemiddeld net onder een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- GRC tooling is een aandachtspunt voor alle functies.
- Slechts één medewerker met functieomschrijving Raad van Bestuur heeft de vragenlijst beantwoord. De getoonde scores zijn slechts op één waarneming gebaseerd en mogelijk niet representatief.



## Bovemij Groep, excl. Schadeverzekering-Maatschappij

- De bedrijfsentiteiten van Bovemij Groep, excl. Schadeverzekering-Maatschappij scoren gemiddeld net onder een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- Op het element GRC tooling wordt door medewerkers met functieomschrijving Raad van Bestuur, Directie en Management in vergelijking met medewerkers in de functie Coördinator laag gescoord.
- De functieomschrijving Raad van Bestuur scoort lager dan andere functies, maar hier is maar één waarneming voor.

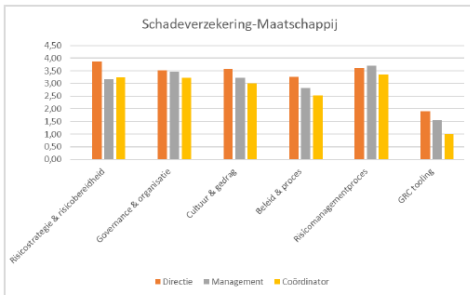


© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

# Generieke aandachtspunten

## Schadeverzekering-Maatschappij

- De bedrijfsentiteit Schadeverzekering-Maatschappij scoort gemiddeld net boven een gestructureerd en gestandaardiseerd volwassenheidsniveau.
- GRC tooling aandachtspunt voor alle functies, ook voor werknemers in de functie van coördinator in tegenstelling tot de andere bedrijfsentiteiten.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

## Resultaten per onderdeel volwassenheid

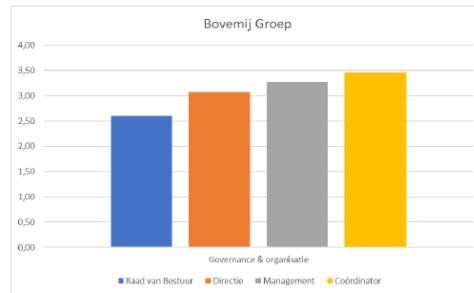
### Governance en organisatie

#### Uitkomsten vragenlijst

- Op het gebied van governance en organisatie bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	2,6	3,1	3,3	3,5
Niveau	Informeel en ad-hoc toepassing	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd

- 35 personen hebben de eerste vraag beantwoord, 35 personen hebben alle vijf de vragen over governance en organisatie doorlopen.
- Van de 35 personen die de vraag over de overlegstructuren voor risicomanagement binnen Bovemij hebben beantwoord hebben 5 personen aangegeven niet te weten wat hiermee bedoeld wordt.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	20	6

Onder **Governance en organisatie** wordt de structuur verstaan waarbinnen Bovemij haar risicomanagementactiviteiten stuurt, monitort en hierover rapporteert. Deze organisatiestructuur omvat naast de rollen, verantwoordelijkheden, taken en bevoegdheden ook de communicatie-, rapportage- en escalatielijnen.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

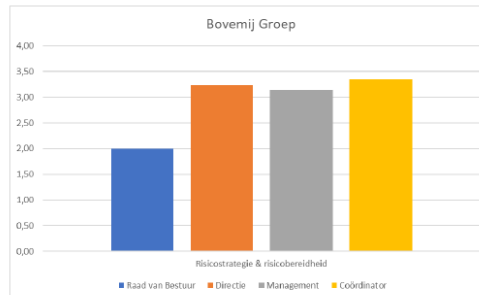
### Risicostrategie en risicobereidheid

#### Uitkomsten vragenlijst

- Op het gebied van risicostrategie en -bereidheid bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	2,0	3,2	3,1	3,3
Niveau	Informeel en ad-hoc toepassing	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd

- 43 personen hebben de eerste vraag beantwoord, 36 personen hebben alle vijf de vragen over de risicostrategie en risicobereidheid doorlopen.
- Van de 37 personen die de vraag over de beheersingsdoelstellingen van Bovemij hebben beantwoord hebben 6 personen aangegeven niet te weten wat hiermee bedoeld wordt.
- Opvallend is ook dat 4 personen de vragenlijst hebben afgebroken bij de vraag over beheersingsdoelstellingen.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	22	12

De **risicostrategie** betreft de uitgangspunten van het bedrijf voor de wijze waarop Bovemij omgaat met risico's (vermijden, accepteren, verminderen of delen/overdragen van risico's).

De **risicobereidheid** betreft de kwalitatieve omschrijving van de risico's die Bovemij bereid is te nemen of wat onmiddellijke actie en aandacht vereist bij het nastreven van de organisatiedoelstellingen.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

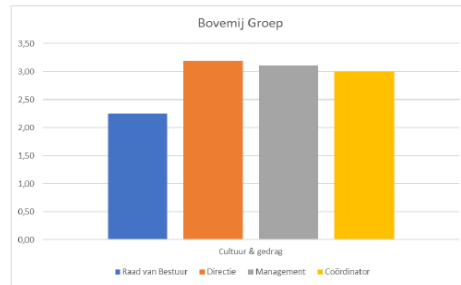
## Cultuur en gedrag

### Uitkomsten vragenlijst

- Op het gebied van cultuur en gedrag bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	2,3	3,2	3,1	3,0
Niveau	Informele en ad-hoc toepassing	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd

- 34 personen hebben de eerste vraag beantwoord, 34 personen hebben alle vier de vragen over cultuur en gedrag doorlopen.
- Van de 34 personen die de vraag over de jaarlijkse performance gesprekken hebben beantwoord hebben 2 personen aangegeven niet te weten wat hiermee bedoeld wordt.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	19	6

Onder **cultuur en gedrag** vallen de 'shared values' en het tonen van commitment. Daarnaast betreft dit het lerend vermogen van de organisatie door een 'fouten maken mag' houding, aanspreken op eigenaarschap/ verantwoordelijkheden en het spreken in een gemeenschappelijke taal om elkaar te helpen de dialoog op gang te brengen en houden. Het gaat over het hebben van een gemeenschappelijk beeld van en visie op risicomanagement en risico's.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

23

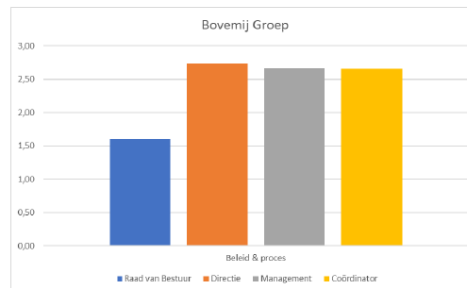
## Beleid en proces

### Uitkomsten vragenlijst

- Op het gebied van beleid en proces bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	1,6	2,7	2,7	2,7
Niveau	Initieel	Informele en ad-hoc toepassing	Informele en ad-hoc toepassing	Informele en ad-hoc toepassing

- 34 personen hebben de eerste vraag beantwoord, 34 personen hebben alle vijf de vragen over beleid en proces doorlopen.
- Van de 34 personen die de vraag over de beleidsdocumenten van Bovemij hebben beantwoord hebben 6 personen aangegeven niet te weten wat hiermee wordt bedoeld.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	19	6

Onder **risicomanagementbeleid en -proces** worden de beleidsdocumenten voor Bovemij (en onderliggende bedrijfsentiteiten) en de bijbehorende procesbeschrijvingen verstaan die worden gebruikt met als doel het bewerkstelligen van een aantoonbare, adequate beheersing van de risico's in relatie tot de doelstellingen van Bovemij.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

24



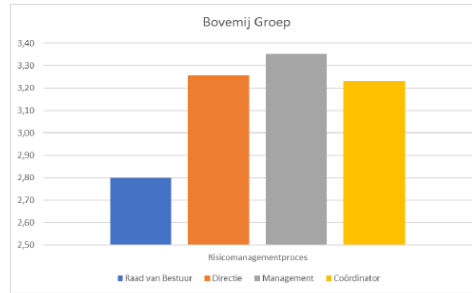
## Risicomanagementproces

### Uitkomsten vragenlijst

- Op het gebied van het risicomanagementproces bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	2,8	3,3	3,4	3,2
Niveau	Informeel en ad-hoc toepassing	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd	Structureel en gestandaardiseerd

- 34 personen hebben de eerste vraag beantwoord, 33 personen hebben alle vijf de vragen over het risicomanagementproces doorlopen.
- Van de 34 personen die de vraag over de risicomanagementcyclus van Bovemij hebben beantwoord hebben 6 personen aangegeven niet te weten wat hiermee bedoeld wordt.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	19	6

Het **risicomanagementproces** zijn de activiteiten om risico's te identificeren, te beoordelen, te prioriteren en erover te rapporteren, met als doel inzicht te krijgen in de mate waarin relevante risico's impact hebben op het behalen van de organisatiedoelen. Daarnaast is het de wijze waarop wordt omgegaan met de geïdentificeerde risico's door deze te vermijden, te accepteren, te delen of beheersmaatregelen te implementeren met als doel de risico's te beheersen en te mitigeren.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

25

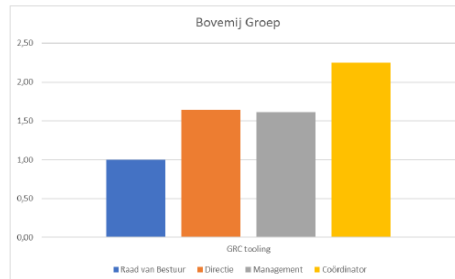
## GRC tooling

### Uitkomsten vragenlijst

- Op het gebied van GRC tooling bedragen de scores per functieomschrijving het volgende:

Functie	Raad van Bestuur	Directie	Management	Coördinator
Score	1,0	1,6	1,6	2,3
Niveau	Initieel	Initieel	Initieel	Informeel en ad-hoc toepassing

- 33 personen hebben de eerste vraag beantwoord, 33 personen hebben alle vier de vragen over GRC tooling doorlopen.
- Van de 34 personen die de vraag over de doelstellingen op het gebied van GRC tooling hebben beantwoord hebben 10 personen aangegeven niet te weten wat hiermee bedoeld wordt.
- Van de 34 personen die de vraag over de mogelijkheden op het gebied van data analyse hebben beantwoord hebben 6 personen aangegeven niet te weten wat hiermee bedoeld wordt.



Functie	Raad van Bestuur	Directie	Management	Coördinator
Aantal gestart	1	8	18	6

Binnen het element **GRC tooling** is de mate van gebruik van geïntegreerde, bedrijf brede systemen voor risicobeheersing (GRC-tooling) beoordeeld, waarbij ook actie-en incidentenmanagement zijn meegenomen.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

26



## Overige opmerkingen

Uit het open tekstveld in de afsluiting van de vragenlijst

- Een van de respondenten heeft inzake GRC tooling aangegeven dat (in beperkte mate) gebruik gemaakt wordt van rapportages uit PowerBI voor het monitoren van risico's, en dat deze persoon PowerBI in het beantwoorden van de vragen niet als GRC tooling geclassificeerd heeft.
- Ook is aangegeven dat deze persoon binnen de betreffende bedrijfsentiteit een goede transitie op het gebied van risicomanagement ervaart, maar dat dit niet voor alle bedrijfsentiteiten van Bovemij geldt.
- Een respondent heeft aangegeven het lastig te hebben gevonden vragen over Bovemij-breed te beantwoorden, omdat de persoon enkel goed zicht heeft op de stand van zaken binnen de eigen bedrijfsentiteit.
- Een respondent uit de bedrijfsentiteit RDC heeft aangegeven dat RDC als onderdeel van Bovemij wordt beschouwd, maar dat veel beleid en procedures nog niet bedrijfsbreed zijn doorgevoerd. De antwoorden zijn vanuit het RDC-perspectief gegeven.
- Een van de respondenten heeft aangegeven de antwoordoptie *ik weet niet hoe dit is ingeregeld* te hebben gemist.
- Een respondent heeft aangegeven te ervaren dat de bewustwording de afgelopen jaren sterk is toegenomen, maar dat de manier waarop het risicomanagement nu een rol speelt de agile organisatie in de weg staat. Helder opgeschreven procedures en processen zouden hieraan kunnen bijdragen.



© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

27

## Bijlage E. Conceptuele ontwerpen

Hooflijnen van het conceptuele ontwerpen zijn besproken met de compliance functionaris, externe risicomanagementadviseur, en externe adviseur voor de transformatie van huidig Bovemij naar Bovemij als Meerzijdig platformbedrijf.

**Requirements vanuit stakeholders:**

Aantoonbaar in contol zijn richting toezichthouders.  
**RACI**  
 Eigenaarschap  
 Leiderschapstijlen binnen beleidscyclus  
 Binnen de RvB, wie heeft wat in en welke portefeuille.

**1<sup>ste</sup> lijn beleid.**

- Stelt beleid op
- Eigenaar van het beleid
- Goedkeurings- en vaststellingsproces...
- Besturing o.b.v. beleid
- Aantoonbaar in control over de processen waar dit beleid iets over zegt.

**2<sup>e</sup> lijn beleid.**

- Bij de opzet van beleid door de 1<sup>ste</sup> lijn, de kaders vanuit R&C / review&opinie rol.
- Vanuit de 2<sup>e</sup> lijn monitoring op doeltreffendheid beleid en operationeel in control zijn van processen....

**Wat is de 1<sup>ste</sup> lijn versus 2<sup>e</sup> lijn rol voor:**

- Propositie,
- Product,
- Product,
- Etc.

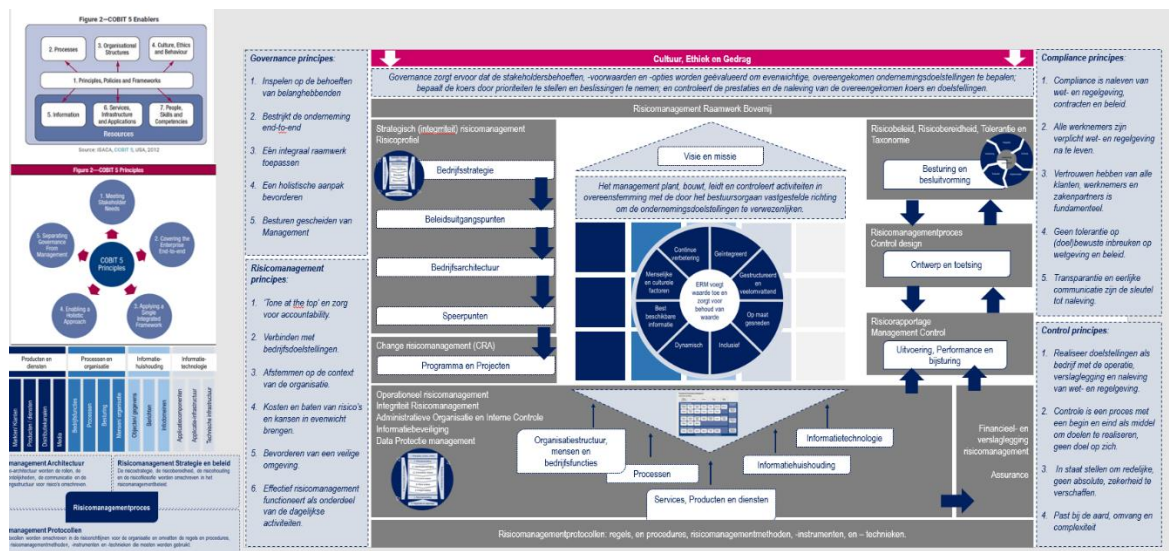
- Wie is eigenaar van het beleidsmanagementproces en beleidshuis beheer.
- Voorbeeld volkbank: Richtinggevende processen en operationele processen. -> rol van GRC Comité en Operationeel Risk Comité. Verantwoordelijkheden t.a.v. beleid en processen.

**Risicomanagement Architectuur**  
 In de risico-architectuur worden de rollen, de verantwoordelijkheden, de communicatie en de rapporteringsstructuur voor risico's omschreven.

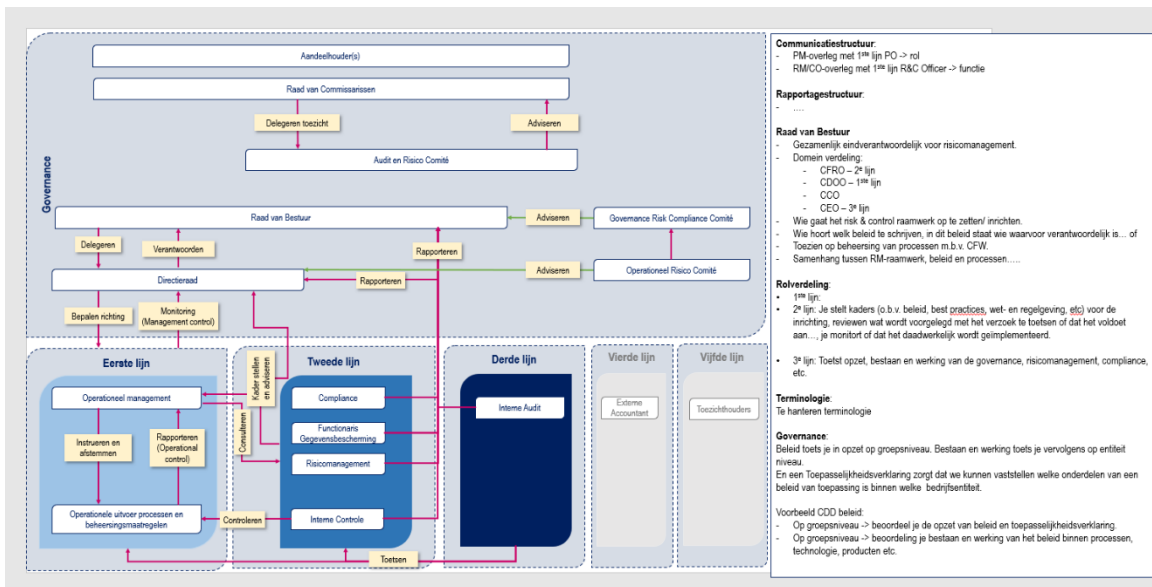
**Risicomanagement Strategie en beleid**  
 De risicostrategie, de risicobereidheid, de risicohouding en de risicofilosofie worden omschreven in het risicomanagementbeleid.

**Risicomanagement Protocollen**  
 Risicoprotocollen worden omschreven in de risicorichtlijnen voor de organisatie en omvatten de regels en procedures, alsook de risicomanagementmethoden, -instrumenten en -technieken die moeten worden gebruikt.

Eerste conceptueel raamwerk besproken en inhoudelijk gediscussieerd op basis van COBIT Framework en de invulling van Bayens voor bedrijfsarchitectuur.



Initieel ontwerp Governance en risicomanagementarchitectuur, gebruikt in brainstorm – discussie op 6 december 2021.



Binnen het Groep Risico Comité dat Bovemij in het jaar 2021 is gestart zijn de ontwerpen voor de governance besproken en van feedback voorzien. De CFRO heeft n.a.v. het overleg de feedback formeel teruggekoppeld. Gedurende het thesis onderzoek is de Risk Governance als zogenoemde Enabler opgenomen in het Target Operating Model, in plaats van standalone.

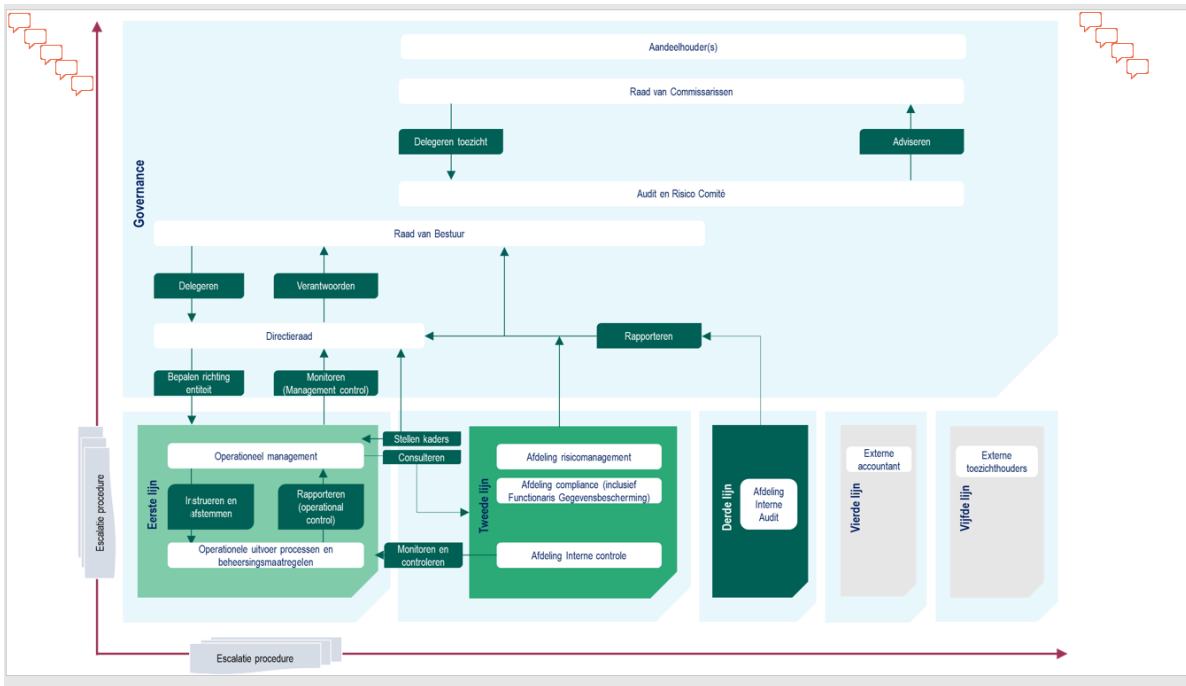


### Vraagstukken te bespreken voor de Risk Governance

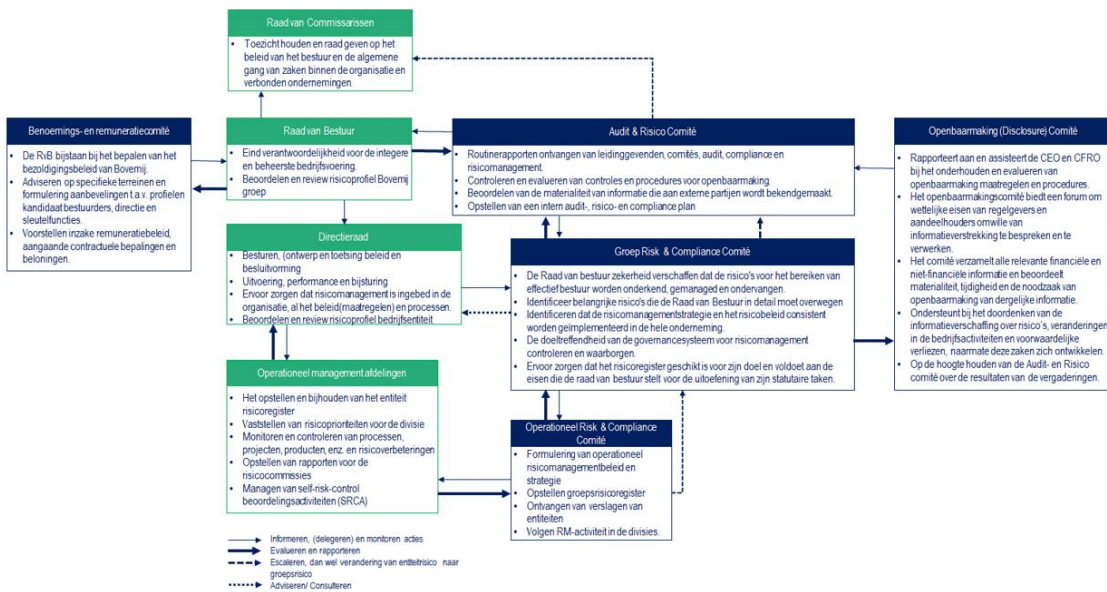
Als onderdeel van het Target Operating Model wordt gewerkt aan de zogenoemde risk governance.

Voor de verdere invulling en uitwerking worden twee vraagstukken ter tafel aangeboden:

1. Welke procedure moet gehanteerd worden voor escalaties binnen de 3LoD?
2. Een voorstel is op de vierde dia gedaan voor de invulling van zogenoemde Risico comités.
  - Na het GRC Comité graag inhoudelijk feedback; voor nu
  - Op hoofdlijnen: welke comités ontbreken wat jullie betreft?



**Risicomanagement Governance risicomanagement architectuur (samengevat overzicht)**



## Bijlage F. Resultaten Equivalente bedrijven

### Vragenlijst

Vragenlijst Multi-Case onderzoek			
<b>1.0.0 Achtergrondinformatie</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
1.0.1 Bedrijfsnaam:			
1.0.2 Type MZP:			
1.0.3 Juridische vorm:			
1.0.4 Aantal FTE:			
1.0.5 Nationaal/ Internationaal:			
1.0.6 Bruto omzet (2019):			
1.0.7 Netto resultaat (2019):			
1.0.12 Datum en tijd documentstudie bedrijfsinformatie:			
<b>2.0.0 Vragen risicomanagement begrippen</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
2.0.1 Wat is de gehanteerde definitie voor risicomanagement?			
2.0.2 Wat is de gehanteerde definitie voor risico factoren?			
2.0.3 Wat is de gehanteerde definitie voor onzekerheid?			
2.0.4 Wat is de gehanteerde definitie voor risicoprofiel?			
2.0.5 Wat is de gehanteerde definitie voor risicomanagementraamwerk?			
<b>3.0.0 Vragen risicoprofiel</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
3.1.0 Welke overkoepelende risico thema's (risicotaxonomie) bevat het risicoprofiel van de organisatie?			
3.1.1 Welke risicomanagementbereidheid wordt gehanteerd?			
3.1.2 Welke risicomanagementspecialismes zijn (eventueel) aanwezig?			
3.1.3 Welk modellen/ methodieken wordt in de basis voor risicomanagement gehanteerd?			
<b>4.0.0 Business strategie</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
4.1 Welke bedrijfsstrategie hanteert de organisatie?			
4.2 Welke algemene interne risicofactoren worden genoemd in relatie tot de bedrijfsstrategie?			
4.3 Welke algemene externe risicofactoren worden genoemd in relatie tot de bedrijfsstrategie?			
<b>5.0.0 Producten en diensten</b>			
<b>5.1.0 Markten/ klanten</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
5.1.1 Welke marktsegmenten betreft de organisatie?			
5.1.2 Welke klanten (afnemers) zijn de doelgroep van de onderneming?			
5.1.3 Op welke wijze is binnen de markten/ klanten rekening gehouden met risicomanagement?			
5.1.4 Welke risico factoren geeft het MZP aan in relatie tot markten?			
5.1.5 Welke risico factoren geeft het MZP aan in relatie tot klanten?			
<b>5.2.0 Producten/ diensten</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
5.2.1 Welke producten biedt het MZP aan?			
5.2.2 Welke diensten biedt het MZP aan?			
5.2.3 Op welke wijze is binnen de producten/ diensten rekening gehouden met risicomanagement?			
5.2.4 Welke risico factoren geeft het MZP aan in relatie tot producten?			
5.2.5 Welke risico factoren geeft het MZP aan in relatie tot diensten?			
<b>5.3.0 Distributiekkanalen</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
5.3.1 Welke productleveranciers heeft het MZP?			
5.3.2 Welke dienstleveranciers heeft het MZP?			
5.3.3 Op welke wijze is binnen de distributiekkanalen rekening gehouden met risicomanagement?			
5.3.4 Welke risico factoren geeft het MZP aan in relatie tot het verspreiden van informatie over diensten/ producten?			
5.3.5 Welke risico factoren geeft het MZP aan in relatie tot productleveranciers?			
5.3.6 Welke risico factoren geeft het MZP aan in relatie tot dienstleveranciers?			
<b>5.4.0 Media</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
5.4.1 Aan welke (type) partijen verspreidt de organisatie informatie over diensten/ producten?			
5.4.2 Hoe/ via welke media kanalen verspreidt de organisatie informatie over diensten/ producten aan interne klanten?			
5.4.3 Hoe/ via welke media kanalen verspreidt de organisatie informatie over diensten/ producten aan externe klanten?			
5.4.4 Op welke wijze is binnen de media rekening gehouden met risicomanagement?			
5.4.5 Welke risico factoren geeft het MZP aan in relatie tot het verspreiden van informatie over diensten/ producten?			
5.4.6 Welke risico factoren geeft het MZP aan in relatie tot het medium voor de verspreiding van informatie over diensten/ producten?			

8.0.0 Bedrijfsfuncties, processen en organisatie			
<b>8.1.0 Bedrijfsfuncties</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
8.1.1	Welke bedrijfsfuncties zijn aanwezig?		
8.1.2	Welke prestaties moeten deze bedrijfsfuncties leveren?		
8.1.3	Op welke wijze is binnen de bedrijfsfuncties rekening gehouden met risicomanagement?		
8.1.4	Welke risico factoren geeft het MZP aan in relatie tot de (verschillende) bedrijfsfuncties?		
<b>8.2.0 Processen</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
8.2.1	Welke processen heeft het MZP ingericht?		
8.2.2	Welke principes/ normen voor processen worden gehanteerd?		
8.2.3	Op welke wijze is binnen de processen rekening gehouden met risicomanagement?		
8.2.4	Welke risico factoren geeft het MZP aan in relatie tot de (verschillende) processen?		
<b>8.3.0 Besturing</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
8.3.1	Op welke niveaus heeft het MZP besturingsprocessen ingericht?		
8.3.2	Wat valt bij het MZP onder besturing van de organisatie?		
8.3.3	Welke overleggrema/ welke overlegmodel is ingericht voor het MZP?		
8.3.4	Op welke wijze wordt binnen de besturing van de organisatie rekening gehouden met risicomanagement?		
8.3.5	Welke risico factoren geeft het MZP aan in relatie tot de besturingprocessen/ besturing van de organisatie?		
<b>8.4.0 Mensen/ organisatie</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
8.4.1	Heeft het MZP een functionele of productgerichte organisatiearchitectuur?		
8.4.2	Is sprake van een regionale spreiding of centrale?		
8.4.3	Is er sprake van centrale stafunctions of gekoppeld aan decentrale bedrijfsonderdelen?		
8.4.4	Op welke wijze(n) wordt binnen het aandachtsgebied mens rekening gehouden met risicomanagement?		
8.4.5	Op welke wijze(n) wordt binnen het aandachtsgebied organisatie rekening gehouden met risicomanagement?		
8.4.6	Welke risico factoren geeft het MZP aan in relatie tot de mens?		
8.4.7	Welke risico factoren geeft het MZP aan in relatie tot de organisatie?		
<hr/>			
<b>9.0.0 Informatievoorziening</b>			
<b>9.1.0 Objecten/ gegevens</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
9.1.1	Welke bedrijfsobjecten worden in het bedrijf onderscheiden?		
9.1.2	Op welke wijze worden bedrijfsobjecten en gegevens beschreven en vastgelegd?		
9.1.3	Hoe zijn verantwoordelijkheden, eigenaarschap en beheer van gegevens belegd?		
9.1.4	Op welke manier worden gegevensverzamelingen beschikbaar gesteld aan gebruikers?		
9.1.5	Op welke wijze(n) wordt binnen het aandachtsgebied objecten rekening gehouden met risicomanagement?		
9.1.6	Op welke wijze(n) wordt binnen het aandachtsgebied gegevens rekening gehouden met risicomanagement?		
9.1.7	Welke risico factoren geeft het MZP aan in relatie tot de objecten?		
9.1.8	Welke risico factoren geeft het MZP aan in relatie tot gegevens?		
<b>9.2.0 Berichten</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
9.2.1	Waar bestaat het berichtenverkeer van de MZP uit?		
9.2.2	Op welke wijze worden berichten uitgewisseld?		
9.2.3	Op welke wijze(n) wordt binnen het aandachtsgebied berichten uitwisselen rekening gehouden met risicomanagement?		
9.2.4	Welke risico factoren geeft het MZP aan in relatie tot de berichten uitwisseling?		



<b>10.0.0 Informatietechnologie</b>			
<b>10.1.0 Applicatiecomponenten</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
10.1.1	Welke primaire applicaties heeft het MZP?		
10.1.2	Welke service levert het platform middels het applicatielandschap?		
10.1.4	Op welke wijze(n) wordt binnen het aandachtsgebied applicatie rekening gehouden met risicomanagement?		
10.1.5	Welke risico factoren geeft het MZP aan in relatie tot applicaties?		
<b>10.2.0 Applicatie infrastructuur</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
10.2.1	Hoe wordt invulling gegeven aan applicatie-infrastructuur door het MZP?		
10.2.4	Op welke wijze(n) wordt binnen het aandachtsgebied applicatie infrastructuur rekening gehouden met risicomanagement?		
10.2.5	Welke risico factoren geeft het MZP aan in relatie tot applicatie infrastructuur?		
<b>10.3.0 Technische infrastructuur</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
10.3.1	Wat is bekend over de technische infrastructuur van het MZP?		
10.3.2	Op welke wijze(n) wordt binnen het aandachtsgebied technische infrastructuur rekening gehouden met risicomanagement?		
10.3.3	Welke risico factoren geeft het MZP aan in relatie tot technische infrastructuur?		
<b>10.4.0 Netwerken</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
10.4.1	Wat is bekend over de netwerkcomponenten bij het MZP?		
10.4.2	Op welke wijze(n) wordt binnen het aandachtsgebied netwerken rekening gehouden met risicomanagement?		
10.4.3	Welke risico factoren geeft het MZP aan in relatie tot technische infrastructuur?		
<b>11.0.0 Financieel - Inkomsten en uitgaven*</b>	<b>Antwoord</b>	<b>1ste Bron antwoord</b>	<b>2e Bron antwoord</b>
11.1.0	Uit welke componenten bestaat de kostenstructuur van het MZP?		
11.1.1	Uit welke componenten bestaat de inkomstenstromen van het MZP?		
11.1.2	Welke risicofactoren geeft het MZP aan in relatie tot de financiële bedrijfsresultaten?		
11.1.3	Welke risico's geeft het MZP aan in relatie tot de kostenstructuur?		
11.1.4	Welke risico's geeft het MZP aan in relatie tot de inkomstenstroom?		

\* De inkomsten en uitgaven zijn tijdens het onderzoek naar risicomanagement en risicofactoren bij equivalente bedrijven toegevoegd, doordat dit in ieder jaarverslag was opgenomen.



## Bijlage G. Gerapporteerde risicofactoren equivalente bedrijven per risicocategorie

Aantal van Type risico	Kolomlabels					
Rijlabels	Amazon.com, Inc.	(leeg)	Alphabet Inc	VNV Global	NewLink Technology	Eindtotaal
<b>Applicatie infrastructuur</b>	<b>3</b>					<b>3</b>
Onderbreking_communicatie_systemen	1					1
Systeemonderbreking	1					1
Kwetsbaarheid_digitale_systemen	1					1
<b>Bedrijfsfuncties</b>	<b>1</b>				<b>1</b>	<b>2</b>
Juridisch_intern	1					1
Wet_en_regelgeving					1	1
<b>Bedrijfsinvestering(en)</b>	<b>1</b>	<b>2</b>	<b>8</b>			<b>11</b>
Bedrijfsovername			2			2
Juridisch_intern	1					1
Waardevermindering_(im)materiële_activa_goodwill			1			1
Afhankelijkheid_dochters		1				1
Onderbreking_bedrijfsvoering		1				1
Markt_algemeen_en_merk_in_markt				1		1
Beleggingen_krediet_rente_liquiditeit				2		2
Onderbreking_processen				1		1
Economisch				1		1
<b>Bedrijfsovername</b>	<b>9</b>	<b>3</b>			<b>1</b>	<b>13</b>
Bedrijfsovername	5					5
Bijkomende_exploitatiekosten	1					1
Investeringen	1					1
Juridisch_intern		1				1
Strategische_allianties					1	1
Waardedaling_organisatie_onderdeel_door_verminderde_financiële_prestaties	1					1
Waardevermindering_(im)materiële_activa_goodwill	1					1
Bedrijfsmutaties		1				1
Bedrijfsafstoting		1				1
<b>Distributiekkanalen</b>	<b>11</b>	<b>1</b>				<b>12</b>
Aansprakelijkheid_producten_bij_verkoop_door_leverancier	1					1
Product_aansprakelijkheid	1					1
Strategische_allianties	1					1
Tekorten_of_overschot_voorraad	1					1
Veranderingen_in_klantvraag	1					1
Verstoring_in_de_keten_door_samenwerkingspartner	1					1
Vertraging_keten_sterk_gereguleerde_diensten	1					1
Wet_en_regelgeving	4					4
Verstoring_in_de_keten_door_productleverancier		1				1
<b>Internationale_bedrijfsvoering</b>	<b>5</b>	<b>9</b>	<b>3</b>		<b>34</b>	<b>51</b>
Nieuwe_Bestaande_concurrenten	1				1	2
Schommelingen_bedrijfsresultaten					1	1
Verstoring_in_de_keten_door_samenwerkingspartner		1			1	2
Wet_en_regelgeving	3	4			5	12
Sociaal_Maatschappelijk_Etnisch		1				1
Volatile_waarde_handelsprijs_bedrijfsaandelen					4	4
Voor_bedrijf_onbeïnvloedbare_factoren_op_aandelenmarkt					1	1
Technologisch					2	2
Onderbreking_bedrijfsvoering					1	1
Markt_integriteit		1				1
Wisselkoersschommelingen_valuta					1	1
Politiek_incl_fiscaal_en_overheidsbeleid	1	2	1		2	6
Markt_algemeen_en_merk_in_markt					1	1
Beleggingen_krediet_rente_liquiditeit					1	1
Economisch					2	2
Aandeelhouder				1		1
Juridisch				1		3
Seizoengebondenheid					1	1
Evolueren_bedrijfsmodel					1	1
Continuïteit_dienst_service					1	1
Onvoldoende_kapitaal_beschikbaar					3	3
Slecht_verzekerd_bedrijfsaansprakelijkheidsverzekering					1	1
Data-authenticiteit_onbekend					1	1
<b>Kostenstructuur</b>	<b>1</b>					<b>1</b>
Schommelingen_bedrijfsresultaten	1					1

Aantal van Type risico	Kolomlabels				
Rijlabels	Amazon.com, Inc. (leeg)	Alphabet Inc	VNV Global	NewLink Technology	Eindtotaal
<b>Markten_Klanten</b>	<b>7</b>	<b>6</b>		<b>2</b>	<b>15</b>
Commerciële_relaties				1	1
Indienen_claims_en_klachten_door_klanten	1				1
Investerings_tov_rendement	2				2
Klanten_Afnemers	2				2
Nieuwe_Bestaande_concurrenten		3			3
Onbekendheid_marktsegment_hierdoor_falend_product_dienst	2				2
Lage_marges		1			1
Slecht_intern_vermogen_klanten_aantrekken		1			1
Markt_algemeen_en_merk_in_markt		1			1
Juridisch_klanten				1	1
<b>Mensen_Organisatie</b>	<b>7</b>	<b>2</b>	<b>1</b>	<b>3</b>	<b>13</b>
Afhankelijkheid_sleutelfiguren	6	2	1	2	11
Door_mens_veroorzaakte_fouten	1				1
Ecologisch				1	1
<b>Nationale_bedrijfsvoering</b>	<b>3</b>	<b>3</b>		<b>6</b>	<b>12</b>
Complexiteit_omvang_organisatie	3				3
Juridisch_intern		2		1	3
Waardevermindering_(im)materiële_activa_goodwill				1	1
Wet_en_regelgeving		1			1
Politiek_incl_fiscaal_en_overheidsbeleid				1	1
Tegenpartijen				1	1
Geen_effectief_intern_controle_systeem				1	1
Negatieve_publiciteit				1	1
<b>Objecten_Gegevens</b>	<b>1</b>	<b>2</b>		<b>2</b>	<b>5</b>
Gebrekkige_security	1				1
Kwetsbaarheid_digitale_systemen		1			1
Storingen_met_opslagapparatuur		1			1
Data_corruptie				1	1
Openbaarmaking_data				1	1
<b>Processen</b>	<b>2</b>				<b>2</b>
Door_mens_veroorzaakte_fouten	1				1
Onaanvaardbare_onuitvoerbaar_voorwaarden_leveranciers	1				1
<b>Producten_Diensten</b>	<b>2</b>	<b>8</b>		<b>3</b>	<b>13</b>
Ecologisch	1				1
Fraude_Intern_extern	1				1
Gebrekkige_security		1			1
Indienen_claims_en_klachten_door_klanten		2			2
Verlieslatend_product_dienst		1			1
Intellectueel_eigendom		1		2	3
Kwaliteitsproblemen		1		1	2
Hoge_of_geen_grip_op_investeringen_kosten		1			1
Beschikbaarheid_advertenties		1			1
<b>Propositie</b>	<b>1</b>				<b>1</b>
Commerciële_relaties	1				1
<b>Technische_infrastructuur</b>	<b>3</b>	<b>5</b>			<b>8</b>
Capaciteit_techische_componenten	1				1
Complexiteit_ICT_infrastructuur	1				1
Slechte_optimalisatie_exploitatie_toeleveringsnetwerk_datacenters	1				1
Kwetsbaarheid_digitale_systemen		5			5
<b>Uitgaven</b>	<b>1</b>	<b>1</b>	<b>3</b>		<b>5</b>
Wisselkoersschommelingen	1				1
Kasstroom_Daling_liquide_middelen			1		1
Wisselkoersschommelingen_valuta		1			1
Beleggingen_krediet_rente_liquiditeit			1		1
Tegenpartijen			1		1
<b>(leeg)</b>		<b>1</b>	<b>1</b>		<b>2</b>
Wet_en_regelgeving			1		1
(leeg)					
Technologisch		1			1
<b>Inkomsten</b>		<b>9</b>	<b>3</b>	<b>3</b>	<b>15</b>
Volatile_waarde_handelsprijs_bedrijfsaandelen		3			3
Voor_bedrijf_onbeïnvloedbare_factoren_op_aandelenmarkt		1			1
Kasstroom_Daling_liquide_middelen		2		2	4
Economische_omstandigheden_adverteerders		2			2
Wisselkoersschommelingen_valuta			2	1	3
Beleggingen_krediet_rente_liquiditeit		1			1
Financieringen			1		1
<b>Besturing</b>		<b>2</b>			<b>2</b>
Nieuwe_Bestaande_concurrenten		1			1
Belangenverstrengeling		1			1
<b>Netwerken</b>		<b>3</b>			<b>3</b>
Kwetsbaarheid_digitale_systemen		3			3
<b>Project</b>				<b>1</b>	<b>1</b>
Schommelingen_bedrijfsresultaten				1	1
<b>Eindtotaal</b>	<b>58</b>	<b>57</b>	<b>19</b>	<b>56</b>	<b>190</b>

**Bijlage H. Case 1 – Amazon****Amazon bedrijf en grootste risico's**

Onderdeel van de visie van Amazon is dat zij zich laten leiden door vier principes: en obsessie voor de klant in plaats van een focus op de concurrent, passie voor uitvinden, toewijding aan operationele uitmuntendheid, en langetermijndenken. Amazon bedient verschillende marktsegmenten, waarbinnen de doelgroepen bestaan uit consumenten, verkopers, ontwikkelaars, ondernemingen en concent ontwikkelaars. Daarnaast levert Amazon diensten aan via programma (vb. gesponsorde advertenties, display- en video advertenties) aan hun zakelijke klanten, dit zijn diensten als: adverteren aan verkopers, leveranciers, uitgevers, en anderen. De producten en diensten die worden aangeboden gaan via verschillende bedrijfsactiviteiten die zijn onderverdeeld naar drie segmenten: Noord-Amerika, Internationaal, en Amazon Web Services.

De bedrijfsactiviteiten van Amazon omvatten een grote verscheidenheid aan producttypes, dienstenaanbod en leveringskanalen. De wereldmarkt waar Amazon haar bedrijfsactiviteiten uitvoert evolueert snel en is zeer competitief. Ook heeft zij te maken met een brede waaier van concurrenten uit vele verschillende industriesectoren over de hele wereld. De belangrijkste risicofactoren binnen concurrentie hebben voor de detailhandelsactiviteiten te maken met de selectie van producten, prijs, gemak en een snelle en betrouwbare afhandeling. Deze factoren houden verband met de risicofactoren die ontstaan vanuit de inkoop-, verkoop- en leveringskanalen, waarbij juridische overeenkomsten een deel van mogelijk risico's mitigeren. Een ander deel van de risicofactoren hebben te maken met het leveren van diensten en producten via derden, online of offline, afhankelijkheid van bedrijven die de informatietechnologiediensten of -producten leveren (waaronder websiteontwikkeling en -hosting, omnichannelverkoop etc.)

Verder wordt Amazon sterk beïnvloed door seizoenen, wat historisch gezien resulteert in hogere verkoopvolumes gedurende het vierde kwartaal van het jaar. Dit risicofactoren die te maken hebben met arbeidsomstandigheden (hoge werkdruk) en financiële risicofactoren door een lagere verkoop in de andere seizoenen.

## Waar bestaat het risico universum van Amazon uit?

Bedrijfsnaam	Amazon.com, Inc.	
<b>Rijlabels</b>	<b>Aantal van Omschrijving Risico_factoren</b>	
<b>Data_informatie_risico</b>		<b>1</b>
Gebrekkige_security		1
<b>Financieelrisico</b>		<b>6</b>
Bijkomende_exploitatiekosten		1
Investeringen		1
Schommelingen_bedrijfsresultaten		1
Waardedaling_organisatie_onderdeel_door_verminderde_financiële_prestaties		1
Waardevermindering_(im)materiële_activa_goodwill		1
Wisselkoersschommelingen		1
<b>Informatietechnologierisico</b>		<b>4</b>
Capaciteit_technische_componenten		1
Complexiteit_ICT_infrastructuur		1
Kwetsbaarheid_digitale_systemen		1
Slechte_optimalisatie_exploitatie_toeleveringsnetwerk_datacenters		1
<b>Integriteitsrisico</b>		<b>1</b>
Fraude_Intern_extern		1
<b>Ketenrisico_supply_chain</b>		<b>6</b>
Aansprakelijkheid_producten_bij_verkoop_door_leverancier		1
Onaanvaardbare_onuitvoerbare_voorwaarden_leveranciers		1
Tekorten_of_overschot_voorraad		1
Veranderingen_in_klantvraag		1
Verstoring_in_de_keten_door_samenwerkingspartner		1
Vertraging_keten_sterk_gereguleerde_diensten		1
<b>Procesrisico_operationeel</b>		<b>4</b>
Door_mens_veroorzaakte_fouten		2
Onderbreking_communicatie_systemen		1
Systeemonderbreking		1
<b>Product_Dienst_Service_risico</b>		<b>6</b>
Indienen_claims_en_klachten_door_klanten		1
Investeringen_tov_rendement		2
Onbekendheid_marktsegment_hierdoor_falend_product_dienst		2
Product_aansprakelijkheid		1
<b>Strategisch_omgevingsrisico</b>		<b>12</b>
Ecologisch		1
Klanten_Afnemers		2
Nieuwe_Bestaande_concurrenten		1
Politiek_incl_fiscaal_en_overheidsbeleid		1
Wet_en_regelgeving		7
<b>Strategisch_organisatierisico</b>		<b>18</b>
Afhankelijkheid_sleutelfiguren		6
Bedrijfsovername		5
Commerciële_relaties		1
Complexiteit_omvang_organisatie		3
Juridisch_intern		2
Strategische_allianties		1
<b>Eindtotaal</b>		<b>58</b>

**Bijlage I. Case 2 – Alphabet****Alphabet bedrijf en grootste risico's**

Oorspronkelijk werd Alphabet Inc. opgericht in 1998 onder de naam Google Inc., waarbij zij een zoekmachinebedrijf werd en uitgroeide tot werelds bekendste zoekmachine wereldwijd. Het bedrijf is in de afgelopen twee decennia verder gediversifieerd door de overname van verschillende bedrijven. Google Inc. reorganiseerde in 2015 naar de holding genaamd Alphabet. Deze (nu) moedermaatschappij bezit Google als haar grootste dochteronderneming, en een aantal andere bedrijven.

Het grootste deel van de inkomsten van Alphabet wordt gegenereerd uit reclame. Alphabet biedt performance advertising, waarmee adverteerders in contact komen met platformgebruikers. Verder verkoopt Alphabet merkreclame, met het doel het bewustzijn van gebruikers en hun affiniteit met merken te vergroten. Reclame is dus een kernonderdeel van de strategie van Alphabet. Google genereert ook zelf inkomsten uit andere bronnen, waaronder de verkoop van apps, in-app aankopen, hardware, en licentie- en servicevergoedingen, waaronder die voor Google Cloud en andere producten. Hierbij heeft Google ook bedrijven overgenomen om de verkoop van deze producten en diensten te kunnen uitbreiden en bestendigen als beheersing van de betreffende risico factoren. Dit zijn bijvoorbeeld de risico factoren onder dienst en services. Opvallende risico factoren hangen samen met de beschikbaarheid van advertenties en klant specifieke factoren. Dit in de combinatie met concurrenten, is het logisch dat zowel Alphabet als Google bedrijven overnemen die zij als concurrent beschouwen.

Alphabet is voortdurend op zoek naar nieuwe technologieën die de portefeuille van bedrijven kunnen verrijken. Een opvallende bedrijfsovername in maart 2022 Mandiant . Dit bedrijf focust op het security testen en security incident respons omwille van het risico kwetsbaarheid van digitale systemen. Al sinds geruime tijd ervaren Alphabet en haar dochters een aanzienlijk aantal cyber aanvallen, waardoor zij al een flink aantal jaren investeren in security (komt terug in jaarverslagen > 5 Jaar). Verder worden door de overname van kleinere bedrijven, opkomende rivalen/ concurrenten (lees voorgaande alinea), uitgeschakeld, waardoor het concurrentierisico afneemt. Dit is echter ook een van de redenen waarom Alphabet momenteel het doelwit is van een antitrustrechtszaak die in oktober 2020 is aangespannen door het Amerikaanse ministerie van Justitie (DOJ) en elf procureurs-generaal van staten.

## Waar bestaat het risico universum van Alphabet uit?

Bedrijfsnaam	Alphabet Inc
Rijlabels	Aantal van Omschrijving Risico_factoren
<b>Data_informatie_risico</b>	<b>2</b>
Gebrekkige_security	1
Storingen_met_opslagapparatuur	1
<b>Financieelrisico</b>	<b>12</b>
Beleggingen_krediet_rente_liquiditeit	1
Economische_omstandigheden_adverteerders	2
Hoge_of_geen_grip_op_Investeringen_kosten	1
Kasstroom_Daling_liquide_middelen	2
Lage_marges	1
Volatile_waarde_handelsprijs_bedrijfsaandelen	3
Voor_bedrijf_onbeïnvloedbare_factoren_op_aandelenmarkt	1
Wisselkoersschommelingen_valuta	1
<b>Informatietechnologierisico</b>	<b>9</b>
Kwetsbaarheid_digitale_systemen	9
<b>Integriteitsrisico</b>	<b>2</b>
Belangenverstremgeling	1
Markt_integriteit	1
<b>Ketenrisico_supply_chain</b>	<b>2</b>
Verstoring_in_de_keten_door_productleverancier	1
Verstoring_in_de_keten_door_samenwerkingspartner	1
<b>Product_Dienst_Service_risico</b>	<b>6</b>
Beschikbaarheid_advertenties	1
Indienen_claims_en_klachten_door_klanten	2
Intellectueel_eigendom	1
Kwaliteitsproblemen	1
Verlieslatend_product_dienst	1
<b>Strategisch_omgevingsrisico</b>	<b>14</b>
Markt_algemeen_en_merk_in_markt	1
Nieuwe_Bestaande_concurrenten	4
Politiek_incl_fiscaal_en_overheidsbeleid	2
Sociaal_Maatschappelijk_Etnisch	1
Technologisch	1
Wet_en_regelgeving	5
<b>Strategisch_organisatierisico</b>	<b>10</b>
Afhankelijkheid_dochters	1
Afhankelijkheid_sleutelfiguren	2
Bedrijfsafstoting	1
Bedrijfsmutaties	1
Juridisch_intern	3
Onderbreking_bedrijfsvoering	1
Slecht_intern_vermogen_klanten_aantrekken	1
<b>Eindtotaal</b>	<b>57</b>

**Bijlage J. Case 3 - VNV Global****VNV Global bedrijf en grootste risico's**

VNV Global is een in Stockholm (Zweden) opgericht investeringsmaatschappij. VNV Global heeft de bedrijfsstrategie dat met name gericht is op het investeren in aandelenparticipaties in particuliere ondernemingen met een hoog rendementspotentieel. Dit zijn (snelgroeiende), op technologie gebaseerde, bedrijven die profiteren van netwerkeffecten. Ze investeren in sectoren met hoge toetredingsdrempels waarbij zij lange termijnrendementen kunnen voorzien, zoals mobiliteit, marktplaatsen en digitale gezondheid in Europa, Midden-Oosten en Noord-Afrika.

In het kader van corporate governance heeft VNV Global meer risico's in opkomende markten, dan in de meer (door)ontwikkelde markten. Een van de manieren om de risico's van corporate governance in de ondernemingen in portefeuille te beheersen, is het voeren van een actief aandeelhoudersbeleid. Actief aandeelhouderschap is belangrijk in alle markten, maar vooral in opkomende markten omdat deze meer extra dimensies kunnen aannemen dan in meer ontwikkelde markten.

Wat bij VNV Global opvalt is het ontbreken van een hoofd categorie operationeel risico. Ze spreken wel over risico factoren die effect kunnen hebben op de operatie, maar dit zijn met name de operationele risico's binnen de bedrijfsentiteiten die de administratieve verwerkingen doen.

VNV Global is binnen het case onderzoek het enige bedrijf dat in het jaarverslag rapporteert over de interne controle van de vennootschap voor de financiële verslaglegging. De interne controle is met name gericht op het waarborgen van een efficiënt en betrouwbaar proces voor het beheren van en rapporteren over aankopen, verkoop en bezig van aandelen en -instrumenten. Volgens de Zweedse Corporate Governance Code moet de Raad van Bestuur ervoor zorgen dat de vennootschap een adequate interne controle heeft en moet voortdurend het interne controlesysteem van de vennootschap evalueren. Het systeem van interne controle wordt gewoonlijk beschreven in termen van vijf verschillende gebieden die deel uitmaken van het internationaal erkend kader COSO ERM.

Voor de naleving van regelgeving van internationale wetgeving op gebieden als anti-omkoping, anti-witwassen en internationale sancties, heeft VNV een op maat gemaakte Compliance Tool Box in gebruik genomen. Dit bevat onder meer checklists voor investeringen, due diligence vragenlijsten en modelcontractclausules, dit alles met het doel ervoor te zorgen dat alle aspecten van het



investeringsproces voldoen aan wet- en regelgeving.

### Waar bestaat het risico universum van VNV Global uit?

Bedrijfsnaam	VNV Global	
<b>Rijlabels</b>	<b>Aantal van Omschrijving</b>	<b>Risico_factoren</b>
<b>Financieelrisico</b>		<b>9</b>
Beleggingen_krediet_rente_liquiditeit		3
Financieringen		1
Kasstroom_Daling_liquide middelen		1
Tegenpartijen		1
Waardevermindering_(im)materiële_activa_goodwill		1
Wisselkoersschommelingen_valuta		2
<b>Procesrisico_operationeel</b>		<b>1</b>
Onderbreking_processen		1
<b>Strategisch_omgevingsrisico</b>		<b>5</b>
Economisch		1
Juridisch		1
Markt_algemeen_en_merk_in_markt		1
Politiek_incl._fiscaal_en_overheidsbeleid		1
Wet_en_regelgeving		1
<b>Strategisch_organisatierisico</b>		<b>4</b>
Aandeelhouder		1
Afhankelijkheid_sleutelfiguren		1
Bedrijfsovername		2
<b>Eindtotaal</b>		<b>19</b>

**Bijlage K. Case 4 - Newlink Technology****NewLink bedrijf en grootste risico's**

NewLink Technology, Inc (NewLink) is een leverancier van IT-oplossingen uit China die zich voornamelijk richt op traditionele software gestuurde oplossingen voor financiële instellingen tijdens de vastleggings- en verslagleggingsperiode. NewLink helpt onder andere bedrijven (financiële- en zorginstellingen) die de traditionele software gestuurde oplossingen willen veranderen naar oplossingen die de digitalisering van deze instellingen vereenvoudigt. En waarbij de eerdere technologie zich richtte op het verzamelen en opslaan van gegevens, voornamelijk op basis van software of lokaal ingezette IT-systemen, zorgt NewLink dat innovatieve software gestuurde oplossingen met data gestuurde systemen met beeld- en tekstherkenning technologie, geavanceerde analyses en technologieën ingezet gaat worden, waaronder Cloud computing, Artificial Intelligence, Internet of Things, enzovoort, waarbij gebruikersdata en feedback worden gedeeld en geanalyseerd voor verdere toepassingen. De oplossingen stellen organisaties in staat om intelligente zakelijke verwerking en gegevensvisualisatie te realiseren, de operationele efficiëntie te verbeteren en de kwaliteit van de dienstverlening te optimaliseren.

NewLink heeft op twee wijzen te maken met risico's en wet- en regelgeving. Enerzijds heeft NewLink als bedrijf binnen de eigen context risico factoren. Anderzijds moet NewLink zorgen dat de oplossingen die door hen worden geboden voldoen aan de wet- en regelgeving van klanten en de wijze waarop zij hun risicomanagement moeten inrichten. Zodoende is de bankensector in China bijvoorbeeld onderhevig aan de Guidelines on Information Technology Risk Management of Commercial Banks.

Omdat NewLink een internationaal opererend en beursgenoteerd bedrijf is hebben zij een onafhankelijke consultant aangesteld op het gebied van interne controle voor de periodieke evaluatie van het interne controlesysteem. Dit systeem ziet toe op aspecten als de verkoop, inkoop, human resources, corporate governance, boekhouding, financiële procedures en informatiemanagement.

NewLink heeft diverse beleidslijnen en procedures ingevoerd om een functionerend risicomanagement te waarborgen in elk aspect van de bedrijfsactiviteiten, waaronder de administratie van de dagelijkse activiteiten, financiële verslaglegging en registratie, vermogensbeheer, naleving van toepasselijke wetten en voorschriften. De Raad van Bestuur houdt toezicht op en managet de algemene risico's in verband met de bedrijfsactiviteiten. Ook is een auditcomité opgericht om het financiële

verslagleggingsproces en het interne controlesysteem van de Groep te beoordelen en hierop toezicht te houden.

### Waar bestaat het risico universum van NewLink uit?

Bedrijfsnaam	NewLink Technology
Rijlabels	Aantal van Omschrijving Risico_factoren
<b>Data_informatie_risico</b>	<b>3</b>
Data_corruptie	1
Data-authenticiteit_onbekend	1
Openbaarmaking_data	1
<b>Financieelrisico</b>	<b>14</b>
Beleggingen_krediet_rente_liquiditeit	1
Kasstroom_Daling_liquide_middelen	2
Schommelingen_bedrijfsresultaten	2
Tegenpartijen	1
Volatile_waarde_handelsprijs_bedrijfsaandelen	4
Voor_bedrijf_onbeïnvloedbare_factoren_op_aandelenmarkt	1
Waardevermindering_(im)materiële_activa_goodwill	1
Wisselkoersschommelingen_valuta	2
<b>Ketenrisico_supply_chain</b>	<b>1</b>
Verstoring_in_de_keten_door_samenwerkingspartner	1
<b>Product_Dienst_Service_risico</b>	<b>4</b>
Continuïteit_dienst_service	1
Intellectueel_eigendom	2
Kwaliteitsproblemen	1
<b>Strategisch_omgevingsrisico</b>	<b>18</b>
Ecologisch	1
Economisch	2
Juridisch	3
Markt_algemeen_en_merk_in_markt	1
Nieuwe_Bestaande_concurrenten	1
Politiek_incl._fiscaal_en_overheidsbeleid	3
Technologisch	2
Wet_en_regelgeving	5
<b>Strategisch_organisatierisico</b>	<b>16</b>
Afhankelijkheid_sleutelfiguren	2
Commerciële_relaties	1
Evolueren_bedrijfsmodel	1
Geen_effectief_intern_controle_systeem	1
Juridisch_intern	1
Juridisch_klanten	1
Negatieve_publiciteit	1
Onderbreking_bedrijfsvoering	1
Onvoldoende_kapitaal_beschikbaar	3
Seizoengebondenheid	1
Slecht_verzekerd_bedrijfsaansprakelijkheidsverzekering	1
Strategische_allianties	1
Wet_en_regelgeving	1
<b>Eindtotaal</b>	<b>56</b>

**Bijlage L. Begrippenlijst**

Term	Definitie
<b>Beheersingsmaatregelen</b>	Een beheersmaatregel houdt een risico in stand en of wijzigt deze. Een beheersmaatregel kan onder andere elke vorm van proces, beleid, voorziening, werkwijze of andere omstandigheid of maatregel zijn waarmee het risico in stand wordt gehouden en of wordt gewijzigd (NEN, 2019).
<b>Compliance</b>	Compliance de naleving van relevante wetten, voorschriften, contractuele overeenkomsten en intern beleid (ISACA, 2013).
<b>Cyber criminaliteit</b>	De resultante van ongunstige gebeurtenissen die een bedreiging vormen voor de veiligheid personeel, integriteit van de organisatie, en informatiesystemen; en wat mogelijk kan leiden tot inbreuken op de beveiliging, gestolen data of ander bedrijfsinformatie en/ of kennis hiervan, vandalisme, criminaliteit en sabotage.
<b>Corporate Governance</b>	Corporate governance gaat over besturen van de organisatie, beheersen van risico's, besluitvorming, over verantwoordelijkheid nemen, zeggenschap (bevoegdheden) hebben en over toezicht houden en verantwoording afleggen ('t Hart, z.d.; Bayens & Tönissen, 2015; Bosch, 1997; NEN, 2019).
<b>Governance</b>	Governance zorgt ervoor dat de behoeften, voorwaarden en opties van de belanghebbenden (stakeholders) worden geëvalueerd om evenwichtige, in onderling overleg vastgestelde ondernemingsdoelstellingen te bepalen; bepaalt de koers door prioriteiten te stellen en beslissingen te nemen; en controleert de prestaties en de naleving van de overeengekomen beleidslijnen en doelstellingen (ISACA, 2018).
<b>Operationeel risico</b>	De resultante van ongunstige gebeurtenissen binnen de organisatie die van invloed zijn op het interne vermogen van de organisatie om producten en diensten te produceren, op de kwaliteit en de tijdigheid van de productie, en/ of op de winstgevendheid (Manuj & Mentzer, 2008).
<b>Financieel risico</b>	De resultante van ongunstige gebeurtenissen die effect hebben op de wijze waarop geld door de organisatie wordt/ is gemanaged en de wijze waarop winstgevendheid wordt bereikt (FIRM).
<b>Risicoprotocollen</b>	Risicoprotocollen worden omschreven als het hebben van beleid, risicorichtlijnen voor de organisatie en omvatten de regels en procedures, alsook de risicomanagement- en monitoringsmethoden, -instrumenten en -technieken die moeten worden gebruikt (Hopkin, 2018)s.
<b>Risicobereidheid (Risk Appetite)</b>	Risicobereidheid is de hoeveelheid risico's in verschillende opzichten die de organisatie op korte termijn bereid is te aanvaarden om een activiteit te ondernemen die risico's inhoudt om haar missie (of visie) te verwezenlijken (Hopkin, 2018; ISACA, 2013).
<b>Risico capaciteit (Risk Capacity)</b>	Risicocapaciteit is de objectieve hoeveelheid verlies die de organisatie kan nemen zonder haar voortbestaan in gevaar te brengen (ISACA, 2013) ofwel het feitelijke vermogen om de risico's te nemen (Hopkin, 2018). Dit verschilt ten opzichte van de risicobereidheid, dat meer een beslissing van de raad van bestuur/ het management is over hoeveel risico wenselijk is (ISACA, 2013).

<b>Risicoblootstelling (Risk Exposure)</b>	Het cumulatieve totaal van alle individuele risicowaarden die samenhangen met de risico's waarmee de organisatie feitelijk wordt geconfronteerd is de totale risicoblootstelling. (Hopkin, 2018)
<b>Risicofunctie perspectief</b>	Beschrijft wat binnen een onderneming nodig is om efficiënte en effectieve kernactiviteiten inzake governance en risicomanagement op te zetten en in stand te kunnen houden.
<b>Risicohouding (Risk Attitude)</b>	De risicohouding (en risicocriteria) vertegenwoordigt de houding ten opzichte van risico's bij een lange termijn visie binnen de context van andere bedrijfsbesluiten (niet zozeer op een op zichzelf staand besluit).
<b>Risicomanagement perspectief</b>	Beschrijft hoe het kernproces van risicomanagement, namelijk het identificeren, analyseren, reageren op en rapporteren over risico's de bedrijfsstrategie, besturing, beleid, besluitvorming en bedrijfsperformance ondersteunt.
<b>Risicoprofiel</b>	Het risicoprofiel is een overzicht van risico's inclusief de waarschijnlijkheid waarmee zij zullen optreden en een inschatting van hun impact als ze zich manifesteren (Hopkin, 2018; Stoneburner et al., 2002). Het risicoprofiel van een (onderdeel van een) organisatie vloeit voort uit de bedrijfsdoelstellingen ('missie') en de voor het realiseren van die doelstellingen gekozen strategie (Hopkin, 2018). Risicomanagement is daarmee een discipline die tot de kern van elke onderneming behoort en andersom beïnvloeden de activiteiten het risicoprofiel (Hopkin, 2018; Stoneburner et al., 2002).
<b>Risicotaxonomie</b>	Risicotaxonomie is het verschaffen van een duidelijk inzicht in de terminologie en de gehanteerde meeteenheden voor de belanghebbenden bij het bespreken en communiceren over risico's. De taxonomie moet worden medegedeeld aan en gebruikt worden door de hele onderneming (ISACA, 2013).
<b>Risicotolerantie (Risk Tolerance)</b>	Het aanvaardbare niveau van variatie dat het management bereid is toe te staan voor een bepaald risico bij het nastreven van doelstellingen (ISACA, 2013).
<b>Risico-universum</b>	Het risico-universum behelst het totale met een onderneming samenhangende risico, met inbegrip van de onbekende risico's, dat een positieve of negatieve invloed zou kunnen hebben op het vermogen van een onderneming om haar missie (of visie) op lange termijn te verwezenlijken (ISACA, 2013).