MASTER'S THESIS

Een maturity model voor de domeinen governance, riskmanagement en compliance als onderdeel van data governance

Kroos-Kerpershoek, P. (Petra)

Award date:
2020

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain.
• You may freely distribute the URL identifying the publication in the public portal.

Take down policy
If you believe that this document breaches copyright please contact us at:

pure-support@ou.nl

providing details and we will investigate your claim.

Downloaded from https://research.ou.nl/ on date: 16. May. 2025

Open Universiteit
www.ou.nl

Een maturity model voor de domeinen governance, riskmanagement en compliance als onderdeel van data governance

A maturity model for the governance, risk management and compliance domains as part of data governance

Opleiding:	Open Universiteit, faculteit Management, Science & Technology
	Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeeropdracht Business Process Management and IT
Student:	Petra Kroos-Kerpershoek
Identiteitsnummer:	
Datum:	27 december 2020
Afstudeerbegeleider	Drs. Ing. Jan Merkus
Meelezer	Prof. Dr. Ir. Remco Helms en Prof. Dr. Rob Kusters
Derde beoordelaar	geen
Versie nummer:	1
Status:	definitief

Abstract

De omvang van data neemt steeds meer toe binnen organisaties. Het is van belang dat data betrouwbaar, juist en volledig is om hiermee de kwaliteit van data te kunnen waarborgen. Data governance (DG) helpt de organisatie om de waarde van data te waarborgen en om de datakwaliteit te verbeteren en te onderhouden. Governance, riskmanagement en compliance (GRC) zijn belangrijk om de prestaties te verbeteren en de risico's van binnen en buiten de organisatie te beheersen. In de literatuur is echter nog weinig onderzoek gedaan naar GRC-activiteiten in relatie tot DG. Dit onderzoek heeft als doel een meetinstrument te ontwikkelen om de organisatievolwassenheid in de praktijk bij een organisatie te kunnen meten. Na literatuuronderzoek is het Data Governance Governance Riskmanagement en Compliance Maturity Model (DGGRCMM) ontstaan. Dit model is met een empirisch onderzoek in de praktijk getoetst door middel van semigestructureerde interviews met vier experts die ruim 15 jaar werkervaring, kennis en expertise hebben op het gebied van GRC. Uit de resultaten bleek, dat het DGGRCMM een gevalideerd meetinstrument is om de organisatievolwassenheid van DG te kunnen beoordelen binnen een organisatie. Dit onderzoek geeft inzicht in de belangrijkheid van de GRC-activiteiten binnen DG en kan worden gebruikt voor vervolgonderzoek.

Sleutelbegrippen

Data governance, governance risk management and compliance, GRC, maturity model

Samenvatting

Relevantie
Data speelt een steeds grotere rol binnen organisaties. Data met grotere volumes wordt verzameld, vastgelegd en beschikbaar gesteld in systemen om doelstellingen te kunnen behalen. Het is hierbij van belang dat data betrouwbaar, juist en volledig is om hiermee de kwaliteit van data te kunnen waarborgen. Data governance (DG) helpt de organisatie om de waarde van data te waarborgen en om datakwaliteit te verbeteren en te onderhouden. Governance, riskmanagement en compliance (GRC)-activiteiten zijn binnen organisaties belangrijk om de prestaties te verbeteren en de organisatie van binnen en van buiten te beschermen tegen risico's. DG helpt de organisaties met het structureren en documenteren van datakwaliteit. Een volwassenheidsmodel, dat bestaat uit een reeks van volwassenheidniveaus, dimensies en bijbehorende criteria van processen, is een goed hulpmiddel om de organisatievolwassenheid te kunnen beoordelen, zodat de organisatie kan groeien in haar volwassenheid.
Dit onderzoek is bedoeld om een bijdrage te leveren aan de wetenschap en nieuwe kennis op te doen over GRC in relatie tot DG. Er is een Data Governance Governance Riskmanagement en Compliance Maturity Model (DGGRCMM) opgesteld om de organisatievolwassenheid binnen de organisatie te kunnen meten.

Doelstelling
Dit onderzoek is bedoeld om op basis van de literatuur een volwassenheidsmodel te ontwikkelen om de organisatievolwassenheid binnen een organisatie te kunnen meten op het gebied van GRC in relatie tot DG. Het doel hierbij is om het ontwikkelde DGGRCMM te toetsen in de praktijk en meer kennis op te doen voor de wetenschap.

Probleemstelling
Het is niet makkelijk om de huidige situatie van een organisatie vast te stellen, omdat men moet weten wat er gemeten moet worden en bij welk volwassenheidsniveau dat hoort. De hoofdvraag van dit onderzoek luidt:

'**Hoe kan de organisatievolwassenheid van de GRC-dimensies van DG worden gemeten?**'

Het DGGRCMM is een goed hulpmiddel om de organisatievolwassenheid te kunnen meten. Het DGGRCMM is aan de hand van de literatuur ontwikkeld. Er is in de literatuur gezocht naar kwalificaties en criteria die betrekking hebben op GRC. Nadat het DGGRCMM ontwikkeld was, is het model in de praktijk getoetst door semigestructureerde interviews af te nemen. Vier experts hebben tijdens de interviews de dimensies en kwalificaties herkend en bevestigt met praktijkvoorbeelden. Na aanpassing van de criteria zijn deze ook valide bevonden door de experts. De organisatievolwassenheid kan volledig worden gemeten door het in de praktijk toetsen van het DGGRCMM op relevante dimensies, kwalificaties, levels en criteria.

Aanpak
Om de hoofdvraag te kunnen beantwoorden, is eerst antwoord gegeven op twee deelvragen. Er is literatuuronderzoek gedaan naar de definities van DG, GRC en maturity model. Vervolgens heeft er een empirisch onderzoek plaatsgevonden waarbij de bevindingen uit de literatuur zijn getoetst in de praktijk. De literatuurstudie en het empirisch onderzoek tezamen leiden tot het antwoord op de hoofdvraag.

Resultaten
Alle dimensies van het DGGRCMM zijn door de experts bevestigd met praktijkvoorbeelden. Volgens meerdere experts ontbrak de kwalificatie integriteit in het DGGRCMM. Ook gaven de experts aan dat structuur onder governance thuishoort en niet onder GRC. De criteria zijn concreter gemaakt, waardoor het model beter toetsbaar werd. Het DGGRCMM is hiermee relevant, betrouwbaar en een valide meetinstrument om de GRC-dimensies binnen DG te kunnen meten.

Conclusies
Het DGGCRMM is goed te gebruiken als meetinstrument om de organisatievolwassenheid van DG te kunnen meten. Na aanpassingen van de criteria is dit model als valide en compleet bevonden om te kunnen groeien in DG, mits het volwassenheidsniveau van de organisatie laag is.
De kennis voor de wetenschap is verrijkt met een nieuwe kwalificatie, namelijk integriteit.

Aanbevelingen voor verder onderzoek
Er heeft nog weinig wetenschappelijk onderzoek plaatsgevonden van GRC in relatie tot DG. Dit onderzoek toont aan, dat GRC binnen DG een belangrijk onderdeel is om te kunnen groeien binnen DG. Verder onderzoek is nodig om meer kennis hierover te vergaren. Aanbevolen wordt om ditzelfde onderzoek ook uit te voeren bij andere kleine organisaties, maar ook bij grote organisaties. Mogelijk leidt dit tot aanvullingen en/of verbeteringen in het model.
Nader onderzoek is nodig om te kunnen uitwijzen of integriteit moet worden opgenomen als kwalificatie in het model. Nader onderzoek is ook nodig om uit te wijzen of de structuur alleen onder governance thuishoort of ook onder riskmanagement en compliance. Mogelijk leidt het aanvullen of het wijzigen van de criteria nog tot verbeteringen in het model.

Summary

Relevance
Data plays an increasingly important role within organizations. Data with larger volumes is collected, recorded and made available in systems to achieve objectives. It is important that data is reliable, correct and complete to guarantee the quality of data. Data governance (DG) helps the organization to guarantee the value of data and to improve and maintain data quality. Governance, risk management and compliance (GRC) activities are important within organizations to improve performance and to protect the organization inside and out against risk. DG helps organizations to structure and document data quality. A maturity model, which consists of a series of maturity levels, dimensions and associated criteria of processes, is a good tool for assessing organizational maturity so that the organization can grow in its maturity.
This research is intended to contribute to science and to gain new knowledge about GRC in relation to DG. A Data Governance Governance Risk Management and Compliance Maturity Model (DGGRCMM) has been drawn up to measure organizational maturity within the organization.

Goal
This research is intended to develop a maturity model based on the literature to measure the organizational maturity within an organization around GRC in relation to DG. The aim is to test the developed DGGRCMM in practice and to gain more knowledge for science.

Issue
It is not easy to determine the current situation of an organization, because one must know what needs to be measured and what maturity level it belongs to. An organizational maturity model is a good tool for this. The main question of this research is:

"How can the organizational maturity of DG GRC dimensions be measured?"

The DGGRCMM is a good tool for measuring organizational maturity. The DGGRCMM has been developed based on the literature. The literature was searched for qualifications and criteria related to GRC. After the DGGRCMM was developed, the model was tested in practice by conducting interviews. During the interviews, four experts recognized the dimensions and qualifications and confirmed them with practical examples. The DGGRCMM can be fully tested on relevant dimensions, qualifications, levels and criteria.

Approach
To be able to answer the main question, answers were first given to two sub-questions. Literature research was first conducted into the definitions of DG, GRC and maturity model. Subsequently, empirical research was conducted in which the findings from the literature were tested in practice. The literature study and the empirical research together led to the answer to the main question.

Results
All dimensions of the DGGRCMM have been confirmed by the experts with practical examples. According to several experts, the qualification integrity was lacking in the DGGRCMM. The experts also indicated that structure belongs under governance and not under GRC. The criteria have been made more concrete, making the model more verifiable. The DGGRCMM is therefore relevant, reliable and a valid measuring instrument for measuring the GRC dimensions within DG.

Conclusions

The DGGCRMM can be used well as a measuring instrument to measure the organizational maturity of DG. After adjustments to the criteria, this model has been found to be valid and complete for growth in DG, provided that the maturity level of the organization is low.
Knowledge for science has been enriched with a new qualification, namely integrity.

Recommendations for further research

Little scientific research has been conducted on GRC in relation to DG. This research shows that GRC within DG is an important part of growth within DG. Further research is needed to gain more knowledge about this. It is recommended that the same research be carried out in other small organizations as well as in large organizations. This may lead to additions and / or improvements in the model.
Further research is needed to determine whether integrity should be included as a qualification in the model. Further research is also necessary to determine whether the structure belongs only to governance or also to risk management and compliance. Supplementing or changing the criteria may lead to improvements in the model, so that it becomes even more specific for another research organization.

Inhoudsopgave

Abstract iii
Sleutelbegrippen iii
Samenvatting iv
Summary vi
Inhoudsopgave viii
1. Introductie 1
1.1. Achtergrond 1
1.2. Gebiedsverkenning 1
1.3. Probleemstelling 2
1.4. Opdrachtformulering 2
1.5. Motivatie / relevantie 3
1.6. Aanpak in hoofdlijnen 3
2. Theoretisch kader 4
2.1. Onderzoeksaanpak 4
2.2. Uitvoering 5
2.3. Resultaten en conclusies 6
2.4. Doel van het vervolgonderzoek 13
3. Methodologie 14
3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n) 14
3.2. Technisch ontwerp: uitwerking van de methode 14
3.3. Gegevensanalyse 15
3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten 15
4. Resultaten 16
4.1. Onderzoeksorganisatie 16
4.2. Experts 17
4.3. Context onderzocht organisatie 17
4.4. Resultaten van het onderzoek op deelvraag I 18
4.5. Resultaten van het onderzoek op deelvraag II 23
5. Discussie, conclusies en aanbevelingen 24
5.1. Discussie 24
5.2. Conclusies 26
5.3. Aanbevelingen voor de praktijk 27

5.4. Aanbevelingen voor verder onderzoek 28
5.5 Reflectie 28
Referenties 30
Bijlage 1 Literatuuronderzoek 31
Bijlage 2 Ontwerp volwassenheidsmodellen 33
Bijlage 3 Totstandkoming DGGRCMM 38
Bijlage 4 Interviewprotocol 47
Bijlage 5 Verklaring van eigen werk 58
Bijlage 6 Aanpassingen in criteria in DGGRCMM 59

1. Introductie

1.1. Achtergrond

Data speelt een grote rol binnen organisaties. Data met grotere volumes wordt verzameld, vastgelegd en beschikbaar gesteld in systemen om doelstellingen te kunnen behalen. Het is hierbij van belang dat data betrouwbaar, juist en volledig is om hiermee de kwaliteit van data te kunnen waarborgen (Otto, 2011). Data governance (DG) helpt om de waarde van data te waarborgen en om datakwaliteit te verbeteren en te onderhouden (Otto, 2011). Governance, riskmanagement en compliance (GRC) spelen hierbij een belangrijke rol (Khatri & Brown, 2010). GRC-activiteiten zijn belangrijk in organisaties om hun prestaties te verbeteren en om organisaties van binnen en van buiten te beschermen (Vicente & da Silva, 2011). Om dit doel te bereiken moeten organisaties de GRC-activiteiten verschuiven naar bedrijfseenheden om dezelfde activiteiten te verbeteren (Vicente & da Silva, 2011). Het is voor organisaties van belang om DG te beheersen.
In de literatuur is nog weinig onderzoek gedaan naar DG. Organisaties hebben vaak de middelen niet om de status van DG te beoordelen. Daarom is het nodig om aanvullend een kwalitatief of kwantitatief onderzoek te doen (Otto, 2011). Er is onderzoek nodig naar het selecteren van het juiste DG model, dat per organisatie verschillend kan zijn (Kooper, Maes, & Lindgreen E.E.O., 2011). Ook de eisen aan DG veranderen snel, omdat organisaties ook aan veranderingen onderhevig zijn. Daarom is het nodig om de volwassenheid binnen de organisatie te beschrijven en te beoordelen (Otto, 2011).

1.2. Gebiedsverkenning

DG wordt gezien als een veelbelovende aanpak om de kwaliteit van gegevens binnen de organisatie te verbeteren en te behouden (Khatri & Brown, 2010). Volgens Merkus, Helms & Kusters (2019) is DG nodig om een adequaat beheer van data en informatie te hebben. Om data te kunnen beheersen, moeten data en informatie betrouwbaar zijn (Merkus, Helms, & Kusters, 2019). DG helpt organisaties met het structureren en documenteren van datakwaliteit verantwoordelijkheden (Wende, 2007). Racz, Weippl & Seufert (2010) adviseren om een holistische benadering te hanteren gefocust op mensen, processen en technologie. Organisaties moeten constant hun datakwaliteit meten en kwantificeren. Dit houdt in dat gegevens moeten worden beheerst om problemen met datakwaliteit aan te pakken (Cheong & Chang, 2007). Om aan de strategische eisen te kunnen voldoen is compliance of geïntegreerd klantenmanagement vereist (Otto, 2011).

GRC is afhankelijk van een effectieve DG (Gregory, 2011). Het doel van GRC en DG is een gedeeld doel: waarde toevoegen aan een organisatie terwijl het risico wordt beperkt (Gregory, 2011). Binnen dit onderzoek wordt onderzocht hoe de volwassenheid van GRC-activiteiten gemeten kan worden, zodat de kwaliteit van data wordt gewaarborgd en de risico's binnen en buiten de organisatie worden beheerst. DG is hierbij nodig om data te structureren en documenteren. Vanuit DG worden rollen, beslissingsbevoegdheden en verantwoordelijkheden vastgelegd. DG helpt om de waarde van data te waarborgen en datakwaliteit te verbeteren.

Een volwassenheidsmodel is hierbij een goed hulpmiddel (Bruin & Rosemann, 2007). Volgens Becker, Knackstedt & Pöppelbuβ (2009) bestaat het volwassenheidsmodel uit een reeks van volwassenheidsniveaus, dimensies en bijbehorende criteria van processen. Het onderste stadium

kan worden gekenmerkt door een organisatie met weinig mogelijkheden en het hoogste stadium vertegenwoordigt een concept van totale volwassenheid (Becker, Knackstedt, & Pöppelbuβ, 2009). Een volwassenheidsmodel is een belangrijk instrument gebleken, omdat ze een betere positionering van de organisatie mogelijk maakt en helpt bij het vinden van betere oplossingen (Becker et al., 2009). Merkus (2015) heeft aan de hand van literatuur al het Data Governance Maturity Model (DGMM) ontwikkeld voor DG. Dit model bestaat uit acht dimensies, vijf volwassenheidsniveaus en bijbehorende criteria. De dimensies GRC uit het model van Merkus (2015) worden in dit onderzoek verder onderzocht.

1.3. Probleemstelling

Het beheersen van data met grote volumes speelt een steeds grotere rol binnen organisaties. De regelgeving zorgt ervoor dat DG en GRC juist geïmplementeerd en verbeterd moeten worden om de kwaliteit van data te kunnen waarborgen. Becker et al. (2009) beschreven al dat het niet makkelijk is om de huidige situatie van een organisatie ten opzichte van doelen vast te stellen, omdat men moet weten wat er gemeten moet worden en bij welk volwassenheidsniveau dit hoort. Volgens Bruin & Rosemann (2007) is een volwassenheidsmodel hierbij een goed hulpmiddel om dit te bewerkstelligen. Dit onderzoek zal leiden tot een Data Governance Governance Risk management en Compliance Maturity Model (DGGRCMM), dat een organisatie in staat stelt om GRC als onderdeel van DG tot een goed volwassenheidsniveau te brengen.

1.4. Opdrachtformulering

Doel

Het doel van dit onderzoek bestaat uit twee delen. Op basis van literatuuronderzoek zal een organisatievolwassenheidsmodel voor de GRC-dimensies van DG ontworpen worden. De validiteit en compleetheid van het model zal gewaarborgd worden door het uitvoeren van een empirisch onderzoek. Dit zal meer kennis opleveren over DG, omdat er nog weinig wetenschappelijk onderzoek heeft plaatsgevonden.

Onderzoeksvragen

Om een volwassenheidsmodel te ontwerpen voor de GRC-dimensies van DG, zal onderstaande hoofdvraag beantwoord moeten worden:

Hoe kan de organisatievolwassenheid van de GRC-dimensies van DG worden gemeten?

Om de hoofdvraag te kunnen beantwoorden, zijn deelvragen voor literatuur- en empirisch onderzoek opgesteld.
De theoretische vragen voor literatuuronderzoek zijn:

- Wat is de definitie van DG en wat is de relatie van GRC tot DG?
- Wat is een organisatievolwassenheidsmodel en welke modellen bestaan er al voor GRC-dimensies van DG?
- Wat zijn relevante dimensies, levels en criteria om de organisatievolwassenheid te meten ten aanzien van de GRC-dimensies van DG?

De deelvragen voor het empirisch onderzoek zijn:

- Hoe kan de organisatievolwassenheid in DG met de dimensies, levels en criteria uit de literatuur worden beoordeeld in de vorm van het DGGRCMM?
- Wat zijn relevante aanvullingen voor organisaties op het DGGRCMM om te kunnen groeien in DG?

1.5. Motivatie / relevantie

Wetenschappelijke relevantie

Dit onderzoek naar GRC zal een bijdrage leveren aan de wetenschap op het gebied van DG. Er is meer onderzoek nodig om een model te ontwikkelen, waarbij deze drie gebieden tezamen worden meegenomen (Racz et al., 2010). Uit literatuuronderzoek bleek, dat er wel volwassenheidsmodellen bestaan voor GRC, maar deze voldoen niet aan alle eisen (Racz et al., 2010). Een model voor de wetenschap zal nog ontwikkeld moeten worden.

Praktische relevantie

Het onderzoek is praktisch relevant, omdat het leidt tot een organisatievolwassenheidsmodel om de GRC-dimensies van DG te kunnen meten. Het volwassenheidsmodel is geschikt om DG te beheersen en de risico's te beperken. DG is nog in ontwikkeling en is voor organisaties nog niet volledig te beheersen. Dit onderzoek leidt tot een praktisch hulpmiddel om DG te meten en te groeien binnen de organisatie.

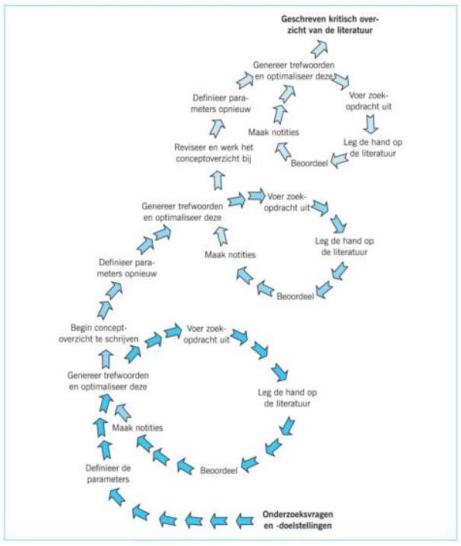
1.6. Aanpak in hoofdlijnen

Hoofdstuk 2 beschrijft het theoretisch kader voor de uitvoering van het onderzoek en het ontworpen volwassenheidsmodel. De methode van onderzoek wordt in hoofdstuk 3 geschreven. In hoofdstuk 4 worden de resultaten uit het empirische onderzoek beschreven. Naar aanleiding van de resultaten uit hoofdstuk 4, worden in hoofdstuk 5 de eindconclusies getrokken.

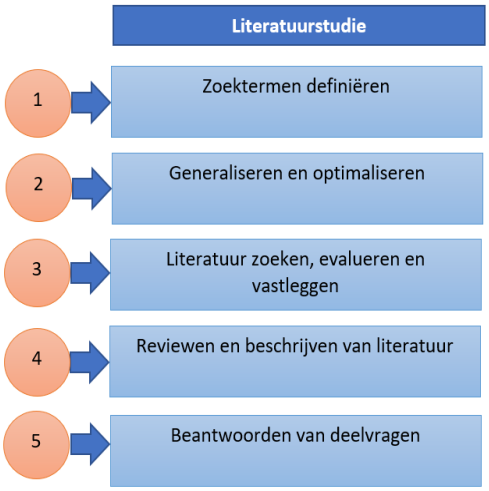
2. Theoretisch kader

2.1. Onderzoeksaanpak

Thornhill, Saunders & Lewis (2009) hebben “het proces van literatuurstudie” geschreven. Dit proces kan worden vergeleken met een opwaartse spiraal, met als hoogtepunt het voltooide product, een geschreven kritisch literatuuroverzicht van de literatuur (Thornhill, Saunders, & Lewis, 2009). Aan de hand van dit proces, is een opzet literatuurstudie gemaakt. Dit proces wordt gebruikt voor het literatuuronderzoek.



Figuur 1a: Het proces literatuurstudie overgenomen uit “Research methods for business students: Prentice Hall: London” door Thornhill, A., Saunders, M. & Lewis, P., 2009



Figuur 1b: Opzet literatuurstudie

Het doel van deze aanpak is antwoord te kunnen geven op de theoretische deelvragen om zo tot een goed organisatievolwassenheidsmodel te komen voor de GRC-dimensies van DG.
Er is online literatuur verzameld op Google Scholar en de Open Universiteit bibliotheek. Er is gezocht op de zoektermen: “data governance”, “GRC” en “maturity model”. De zoektermen worden ook in combinatie met elkaar gebruikt voor betere zoekresultaten. De filters die hierbij zijn toegepast staan in onderstaande tabel.

Tabel 1: Filters Google Scholar en Open universiteit bibliotheek

Google Scholar	Open universiteit bibliotheek
Artikelen vanaf 2010	Artikelen vanaf 2010
Sorteren op relevantie	Sorteren op relevantie
Exclusief patenten	peer reviewed
Exclusief citaten	

2.2. Uitvoering

Data governance

Er zijn artikelen bestudeert om te begrijpen wat DG is en beoordeeld op relevantie.
Na de primaire zoekactie bleek, dat na pagina twee de relevantie afnam. Daarom zijn maximaal 20 artikelen oppervlakkig doorgenomen. Hierbij zijn de volgende inclusiecriteria toegepast:

- Het artikel bevat DG en “designing”;
- Het artikel bevat de term “a conceptual framework” en DG;
- Het artikel bevat het onderwerp GRC in combinatie met DG;
- Het artikel bevat DG en is gericht op geïntegreerde GRC;
- Het artikel bevat de term “information” en DG.

Dit resulteerde in acht artikelen, die volledig bestudeerd zijn.

Tabel 2: Resultaten query's DG

Query's DG	Zoekmachine	Resultaten	Relevante artikelen
"data governance" and "designing"	Googe Scholar	118.000	3
"data governance a conceptual framework"	Open Universiteit bibliotheek	70.055	1
"data governance new concept of information"	Googe Scholar	26.000	1
"data governance and information governance merkus"	Googe Scholar	1	1
"data governance grc"	Googe Scholar	9.610	1
"data governance integrated grc"	Googe Scholar	7.120	1

GRC

Er is gezocht naar GRC in combinatie met governance, risk en compliance. Om het aantal artikelen te reduceren zijn inclusiecriteria toegepast:

- De titel bevat GRC;
- De titel bevat de termen integrated governance, risk & compliance en/of GRC;
- Artikelen die niet specifiek op GRC gericht zijn, worden als minder relevant beschouwd.

Na het reduceren van de artikelen bleven een tweetal artikelen over die relevant zijn bevonden.

Tabel 3: Resultaten query's GRC

Query's GRC		Resultaten	Relevante artikelen
"grc integrated governance risk and compliance"	Googe Scholar	4.460	2

Maturity model

Er zijn artikelen bestudeert om te begrijpen wat een maturity model is. Om de artikelen te beoordelen zijn onderstaande inclusiecriteria gehanteerd:

- Het artikel bevat maturity model;
- Het artikel bevat het onderwerp maturity model in combinatie met GRC of IT of focus area;

Een viertal artikelen zijn hierbij relevant bevonden, waarvan bij de laatste query één artikel uit jaar 2009 is opgenomen.
Bij het artikel van Merkus (2015) is de ‘snowball’ techniek toegepast. Eén relevant artikel is nog gebruikt bij dit onderzoek. Dit heeft geleid tot onderstaande resultaten.

Tabel 4: Resultaten query's Maturity model

Query's Maturity model		Resultaten	Relevante artikelen
"data governance maturity model"	Googe Scholar	47.200	1
"data governance maturity model framework"	Googe Scholar	43.300	1
"focus area maturity models"	Googe Scholar	76.800	1
"maturity model grc"	Googe Scholar	4.090	1
"maturity models for IT"	Open Universiteit bibliotheek	95.669	1

Van alle relevante artikelen is in Bijlage 1 per zoekterm een literatuurlijst opgenomen die voor het literatuuronderzoek is gebruikt.

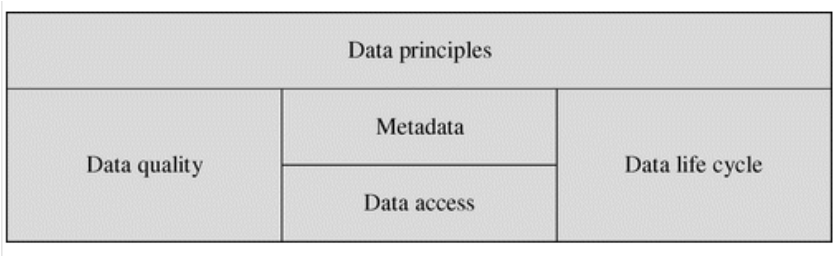
2.3. Resultaten en conclusies

2.3.1 DG & GRC in relatie tot DG

Volgens Merkus, Helms en Kusters (2019) is de definitie van DG als volgt:

Data governance is het oprichten van beheer van gegevens binnen een organisatie om kwaliteit en toegang tijdens haar levenscyclus te garanderen om verantwoording af te leggen voor haar data assets (Merkus et al., 2019).

Volgens Otto (2011) wordt DG gedefinieerd als een bedrijf breed raamwerk voor het toekennen van beslissing gerelateerde rechten en plichten om adequaat met gegevens als bedrijfsmiddel om te gaan. Volgens Khatri & Brown (2010) moeten er beslissingsdomeinen worden geïdentificeerd om de juiste verantwoordelijkheden en taken toe te wijzen.



Figuur 2: Decision domains for data governance overgenomen uit "Data governance activities: an analysis of the literature" door Alhassan, I., 2016, p. 64-75

Deze definities benadrukken, dat het toekennen van de juiste verantwoordelijkheden en taken een belangrijk aspect is binnen DG. Merkus (2015) voegt hieraan nog toe dat mensen, processen en technologieën de data assets maximaliseren.
Uit de literatuur van Alhassan, Sammon & Daly (2016) blijkt dat DG zich bezighoudt met onderstaande punten:

- Ontwerpen (DG-structuur met richtlijnen en standaarden);
- Implementeren;
- Monitoren.

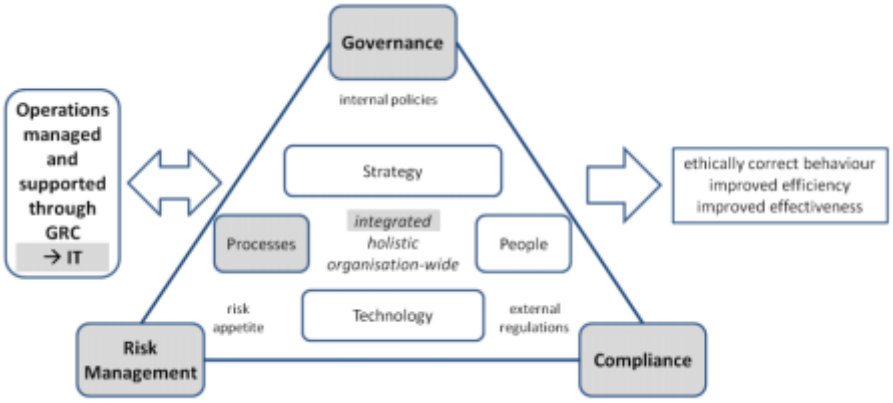
(Alhassan, Sammon, & Daly, 2016).

Zij geven een holistisch beeld van welke activiteiten belangrijk zijn binnen DG, maar laten geen model zien om DG te begrijpen, zoals in het model van Khatri & Brown (2010).

Opmerkelijk is, dat er binnen de modellen en definities geen GRC benoemd wordt als belangrijk onderdeel van DG. Merkus (2015) spreekt wel over corporate governance, riskmanagement en compliance met beslissingsdomeinen, maar dat bevat meer informatie over data zelf. Ook in de definitie van Merkus et al. (2019) wordt niet benoemd dat GRC een belangrijk onderdeel is binnen DG.

GRC

De definitie van een geïntegreerde GRC is volgens Racz et al. (2010):
GRC is een geïntegreerde, holistische benadering van organisatie brede governance, risk en compliance die ervoor zorgt dat een organisatie ethisch correct en in overeenstemming met haar risicobereidheid, intern beleid en externe regelgeving handelt door de afstemming van strategie, processen, technologie en mensen, waardoor de efficiëntie en effectiviteit worden verbeterd
(Racz et al., 2010).
Deze definitie is door Racz et al. (2010) vertaald naar een referentiekader voor GRC-onderzoek.



Figuur 3: Elements in focus in the frame of reference for GRC research overgenomen uit "Towards a process model for integrated IT governance, risk and compliance" door Racz, N. et al., 2010

Binnen dit referentiekader vormen risicobereidheid, intern beleid en externe regelgeving de regels binnen GRC (Racz et al., 2010). Door het samenvoegen van de onderwerpen, componenten en regels tot een holistische en organisatie brede manier, worden de doelstellingen via GRC bereikt binnen de organisatie (Racz et al., 2010). De regels zijn van belang bij DG. Vanuit dit referentiekader is een procesmodel gedefinieerd voor IT GRC beheer dat afgestemd is met de processen binnen de organisatie. Hierbij speelt software een belangrijke rol (Racz, Panitz, Amberg, Weippl, & Seufert, 2010).

Wat is de relatie van GRC tot DG?

Volgens Vicente & da Silva (2011) wordt governance bereikt door regels op te stellen, risico's te monitoren, controles te doen en te rapporteren. Door de juiste mensen aan te stellen in het management, kunnen bewuste risico beslissingen worden genomen om de bedrijfsdoelstellingen te behalen. Volgens Gregory (2011) wordt door het implementeren van GRC waarde toegevoegd aan de onderneming en risico's worden beperkt, waardoor op lange termijn DG verbeterd (Gregory, 2011).
Hieruit kan geconcludeerd worden dat GRC nodig is om de bedrijfsdoelstellingen te behalen. Door GRC te implementeren worden regels opgesteld, is er toezicht op de naleving ervan en worden risico's beheerst. Door het afstemmen van strategie, processen, technologie en mensen verbetert de efficiëntie en effectiviteit van datakwaliteit. De waarde van data assets wordt hiermee gewaarborgd.

Door GRC binnen de organisatie op te nemen wordt de kwaliteit van data verbeterd en de risico's worden beheerst, daardoor verbetert de effectiviteit van DG. De organisatie kan daardoor verantwoording garanderen over haar data assets.

2.3.2 Volwassenheidsmodel en bestaande modellen voor GRC

2.3.2.1 Volwassenheidsmodel

Een volwassenheidsmodel bevat een reeks niveaus die samen een geanticipeerd, gewenst of logisch pad vormen van een beginfase tot volwassenheid (Becker et al., 2009). Een volwassenheidsmodel is een belangrijk instrument gebleken, omdat ze een betere positionering van de organisatie mogelijk maakt en helpt bij het vinden van oplossingen (Becker et al., 2009). Een volwassenheidsmodel kan worden gebruikt om de huidige volwassenheid van de organisatie te meten en daarin verder te groeien (Becker et al., 2009). Alhassan, Sammon & Daly (2016) vullen dit aan en stellen dat een volwassenheidsmodel bestaat uit een raamwerk met volwassenheidlevels en dimensies, die zijn onderverdeeld in kwalificaties.

Volwassenheidsmodellen zijn een middel om stapsgewijs een volledig volwassen functie te implementeren om voortgang te kunnen boeken binnen de organisatie (van Steenbergen, Bos, Brinkkemper, van de Weerd, & Bekkers, 2010). De meeste maturity modellen die hierbij gebruikt worden zijn fixed-level modellen, ook wel looptijdmodellen genoemd. Volgens Steenbergen et al. (2010) zijn looptijdmodellen met een vast niveau, zoals het Capacity Maturity Model (CMM), te onderscheiden met een vast aantal (meestal vijf) generieke volwassenheidsniveaus, waarbij elk volwassenheidsniveau wordt geassocieerd met een aantal processen die geïmplementeerd moeten worden. Een beperking van modellen met een vast niveau is, dat ze er niet op gericht zijn om onderlinge afhankelijkheden uit te drukken in volwassenheidsniveaus, waardoor ze weinig houvast bieden in de volgorde waarin deze processen moeten worden geïmplementeerd. Vast niveau modellen worden door sommige organisaties als te groot en te zwaar ervaren om te gebruiken (van Steenbergen et al., 2010).

Andere type volwassenheidsmodellen zijn focusgebied volwassenheidsmodellen. Deze zijn gebaseerd op het concept van een aantal focusgebieden die ontwikkeld moeten worden om de volwassenheid te bereiken in een functioneel domein (van Steenbergen et al., 2010). Volgens Steenbergen et al. (2010) definieert het focusgebied volwassenheidsmodel voor elk van zijn aandachtsgebieden een reeks ontwikkelingsstappen in de vorm van progressief volwassen capaciteiten. In onderstaand figuur geven de letters A tot en met D de focusgebieden aan, bij een steeds volwassener wordende capaciteit. De werkelijke volwassenheid van de onderzoeksorganisatie kan worden aangegeven met een kleur.

Maturity Scale / Focus Area	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Development of architecture		A			B			C						
Use of architecture			A			B				C				
Alignment with business		A				B				C				
Alignment with the development process			A				B		C					
Alignment with operations					A			B			C			
Relationship to the as-is state					A				B					
Roles and responsibilities				A		B					C			
Coordination of developments							A			B				
Monitoring				A		B		C		D				
Quality management								A		B			C	
Maintenance of the architectural process							A		B		C			
Maintenance of architectural deliverables					A			B					C	
Commitment and motivation		A					B		C					
Architectural roles and training				A		B			C			D		
Use of an architectural method				A						B				C
Consultation			A		B				C					
Architectural tools							A				B			C
Budgeting and planning				A							B		C	

Figuur 4: Een focusgebied volwassenheidsmodel overgenomen uit "The Design of Focus Area Maturity Models", Berlin, Heidelberg, door Van Steenbergen et al., 2010

Het volwassenheidsmodel van het focusgebied maakt het mogelijk om meer dan vijf niveaus te onderscheiden in algemene stadia van volwassenheid, wat resulteert in kleinere stappen tussen de fasen en meer gedetailleerde richtlijnen voor het stellen van prioriteiten bij de ontwikkeling van capaciteiten (van Steenbergen et al., 2010).

Pöppelbuβ & Röglinger (2011) hebben al een raamwerk ontwikkeld met ontwerpprincipes met een stapsgewijze aanpak om een volwassenheidsmodel te ontwikkelen. Merkus (2015) heeft al het DGMM ontwikkeld met vijf volwassenheidsniveaus dat gebaseerd is op de literatuur.

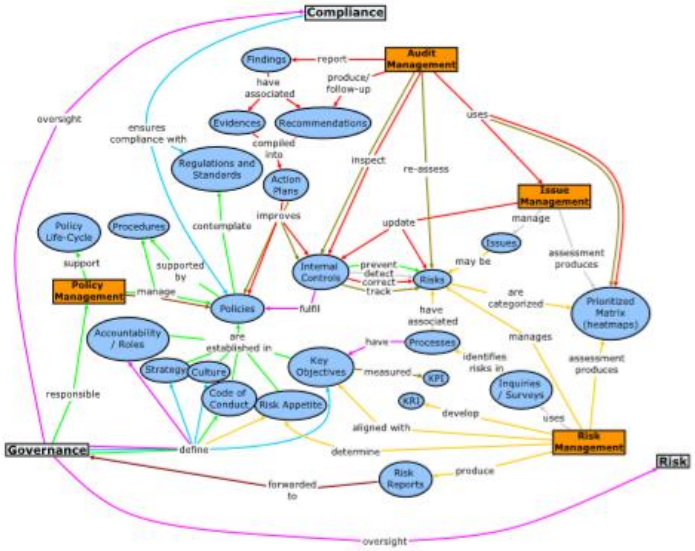
De onderzoeksorganisatie is een kleine organisatie die al bewust is van DG. Dit onderzoek vormt een aanvulling op het bestaande DGMM van Merkus (2015). Daarom is gekozen om de vijf volwassenheidsniveaus te gebruiken die Merkus (2015) ook gebruikt heeft. Om het model te ontwerpen zullen de ontwerpprincipes van Pöppelbuβ & Röglinger (2011) en Becker, Knackstedt & Pöppelbuβ (2009) gebruikt worden.
Er is diepgaand onderzoek nodig zijn om te onderzoeken hoeveel volwassenheidsniveaus er daadwerkelijk nodig zijn voor kleine organisaties. Deze aanpak vergt echter te veel tijd voor dit onderzoek.

2.3.2.2 Bestaande modellen GRC

Er is nog weinig wetenschappelijk onderzoek gedaan naar GRC binnen DG. In de literatuur zijn twee bestaande GRC-modellen gevonden. Omdat er nog te weinig onderzoek heeft plaatsgevonden, is het noodzakelijk gebleken om alleen van de twee bestaande GRC-modellen uit te gaan die in de literatuur zijn gevonden.

OCEG Capability Model

Vicente en da Silva (2011) hebben het OCEG Capability Model ontwikkeld. Dit model beschrijft hoe GRC-activiteiten geïmplementeerd en beheerd kunnen worden (Vicente & da Silva, 2011). Uit het model blijkt dat interne controles van cruciaal belang zijn op het gebied van GRC. Controles zijn nodig om de bedrijfsdoelstellingen te behalen door effectief risicobeheer. Compliance beheert controles. Om alle GRC-activiteiten op een efficiënte manier te beheren, moeten processen gepaard gaan met risico's en risico's moeten worden gekoppeld aan controles (Vicente & da Silva, 2011). Beleid wordt in het model opgenomen, omdat het de cultuur en verantwoording verwoord op het niveau van bestuur, risico en naleving. Dit heeft impact op de gehele organisatie.



Figuur 5a: OCEG Capacity Model overgenomen uit "A conceptual model for integrated governance, risk and compliance", door Vicente, P. & da Silva, M., 2011

GRC maturity model

Voor ziekenhuizen hebben Batenburg, Neppelenbroek & Shahim (2014) een GRC maturity model ontwikkeld (zie Bijlage 2). In dit model is te zien dat controles erg belangrijk zijn. Uit dit onderzoek blijken het in kaart brengen van risico's en het monitoren/rapporteren daarvan een belangrijke rol te spelen (Batenburg, Neppelenbroek, & Shahim, 2014). Bij compliance spelen bewustzijn, indicatoren en structuur een belangrijke rol. De verantwoordelijkheden worden in de structuur weergegeven.

Figuur 5b: GRC maturity model for hospitals overgenomen uit "A maturity model for governance, risk management and compliance in hospitals" door Batenburg, R., Neppelenbroek, M. & Shahim, A., 2014

Een opvallend punt is dat het model van Vicente & da Silva (2011) monitoren, dashboards en rapporteren buiten het model laten, omdat het te complex is. Batenburg, Neppelenbroek & Shahim (2014) nemen deze punten wel op in het GRC maturity model for hospitals, omdat dit essentiële onderdelen zijn in het model. Door het monitoren, analyseren en rapporteren van risico's, kunnen de risico's efficiënt beheerst en gecontroleerd worden. Hierdoor kunnen de doelstellingen van een organisatie worden behaald (Vicente & da Silva, 2011). Dit sluit aan bij de definitie van Racz et al. (2010) die stelt dat risicobereidheid, intern beleid en externe regelgeving de regels vormen van GRC. Volgens Racz et al. (2010) zijn GRC-activiteiten belangrijk om organisaties van binnen en van buiten te beschermen.

Uit beide modellen kan geconcludeerd worden, dat door het goed implementeren van GRC de bedrijfsdoelstellingen kunnen worden behaald. Door de regels van GRC te implementeren worden organisaties beschermt tegen risico's van buitenaf, wordt de waarde van data gewaarborgd en wordt datakwaliteit beheerst. De controle op de GRC-activiteiten speelt hierbij een belangrijke rol om de bedrijfsdoelstellingen te kunnen halen.

2.3.3 DGGRCMM

Dimensies

Voor dit onderzoek zijn twee relevante volwassenheidsmodellen beschikbaar vanuit de literatuur, zoals beschreven is in paragraaf 2.3.2.2. Uit deze modellen zijn de dimensies tot stand gekomen door sleutelwoorden uit de definities van GRC te halen van Vicente & da Silva (2011) en de dimensies die benoemd zijn in beide modellen. De gevonden dimensies zijn in een tabel gezet. Daarna zijn de dimensies die een soortgelijke betekenis hadden bij elkaar gezet onder één naam. Als input voor het DGGRCMM zijn de dimensies van het GRC maturity model for hospitals van Batenburg, Neppelenbroek & Shahim (2014) gebruikt:

Tabel 5: Dimensies GRC maturity model for hospitals

Governance	Risk management	Compliance
Governance structure	Frequency of risk analysis	Compliance mapping
Wistleblower process	Risk management awareness	Information security
Information sharing	Scope of risk management	Compliance controls
Patient co-determination	Risk indicators	
Complaint handling		
Incident reporting		
Patient safety incidents		

Ook zijn de dimensies in het OCEG capability model van Vicente & da Silva (2011) gebruikt:

Tabel 6: Dimensies OCEG capability model

Governance	Risk management	Compliance
Verantwoordelijkheden	Identificeren risico's	Externe regels
Rollen	Evalueren	Interne controles
Procedures	Analyseren	Audit management
Cultuur	Monitoren	
Structuur	Verbeteren	
	Rapporteren	

In Tabel 7 is de onderbouwing weergegeven van de gevonden dimensies.

Tabel 7: DGGRCMM-dimensies

Domeinen	Dimensies	Onderbouwing dimensies
Governance	Gezag en verantwoordelijkheden	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "authority" en "accountability" expliciet benoemd. Vicente & da Silva (2011) bevestigen "accountability".
	Structuur en beleid	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "structure" en incident reporting" expliciet benoemd. Vicente & da Silva (2011) vullen dit aan met "policy".
	Rapporteren	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "incident reporting" expliciet benoemd. Vicente, Racz & da Silva (2011) benoemen dit ook.
Risk management	Monitoring	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "monitoring" expliciet benoemd. Vicente & da Silva (2011) benoemen tevens expliciet "risk reports".
	Beheersen risico's	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "risk structure en scope" benoemd. Vicente & da Silva (2011) vult dit aan met "risks prevent, detect, correct, track".
Compliance	Naleving beleid	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "structure" en "controls" expliciet benoemd. Vicente & da Silva (2011) benoemen "internal controls" en bevestigen dit ook in de definitie.
	Bewustzijn	Uit onderzoek van Batenburg, Neppelenbroek & Shahim (2014) staat "awareness" benoemd.

Alle gevonden dimensies staan in Bijlage 3 met beredenering en afkomstige literatuurbron.

Relevante kwalificaties en levels

Om de validiteit van het onderzoek te waarborgen, is gebruik gemaakt van de eerder getoetste volwassenheidsniveaus (levels) van Merkus (2015) die al getoetst zijn in het Data Governance Maturity Model (DGMM). Het concept DGGRCMM kan gezien worden als een uitbreiding en specificering op het DGMM (Merkus, 2015).
Uit het DGMM zijn onderstaande volwassenheidsniveaus ontstaan:

Tabel 8: Levels DGGRCMM

No process	Beginning process	Established process	Managed process	Optimizing process

Volgens de literatuur van Pöppelbuß & Röglinger (2011) worden de kwalificaties stapsgewijs bepaald (zie Bijlage 2). De bronnen per kwalificatie staan in Bijlage 3. Nadat de kwalificaties, behorende bij de levels in kaart zijn gebracht, wordt bepaald welke kwalificatie in het DGGRCMM wordt behouden en welke niet. De reden waarom kwalificaties niet behouden worden, is dat zij of niet opgenomen worden of worden samengevoegd. Deze kwalificaties worden aangegeven met de tekst "niet in DGGRCMM" en de reden waarom.

Op basis van de ontwerpprincipes van Pöppelbuß & Röglinger (2011) zijn onderstaande stappen doorlopen:

1. Het verzamelen van mogelijke volwassenheidsdimensies uit de literatuur (ontwerpprincipe 1.2a, (Pöppelbuß & Röglinger, 2011)).
2. Het zoeken naar volwassenheidslevels in de literatuur (ontwerpprincipe 1.2b, (Pöppelbuß & Röglinger, 2011)). Vervolgens wordt met stap R2 van het stappenplan van Becker et al. (2009) de indeling gemaakt in maturity levels op basis van overeenkomsten of soortgelijke betekenis voor het stap voor stap ontwikkelen van het model.
3. Het verzamelen van alle kwalificaties die behoren bij de volwassenheidsdimensies die gevonden zijn in stap 1 (ontwerpprincipe 1.2c, (Pöppelbuß & Röglinger, 2011)).

4. Het beschrijven van de beoordeling van de verzamelde criteria uit de literatuur. Met stap R3 van het stappenplan worden de criteria beoordeeld en gevalideerd door de onderzoeksorganisatie.
5. De verzamelde kwalificaties en criteria worden gereduceerd tot een volwassenheidsmodel dat als meetinstrument gebruikt kan worden bij de onderzoeksorganisatie. Met stap R7 van het stappenplan wordt het DGGRCMM gepresenteerd in Figuur 6: Concept DGGRCMM V1.0.

DGGRCMM V0.1						
Dimensies	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process
Governance	Gezag en Verantwoordelijkheden					
	Structuur en Beleid					
	Rapporteren					
Riskmanagement	Monitoring					
	Beheersen risico's					
Compliance	Naleving beleid					
	Bewustzijn					

Figuur 6: Concept DGGRCMM V1.0

Vanwege de beperkte tijd van dit onderzoek, zijn niet alle stappen van de ontwerpprincipes van Pöppelbuβ & Röglinger (2011) uitgewerkt.

2.4. Doel van het vervolgonderzoek

Op basis van de conclusies uit het theoretisch kader zijn de antwoorden op de deelvragen geformuleerd. Dit heeft geleid tot een goed onderbouwde opzet van het DGGRCMM. Het doel van het vervolgonderzoek is om de kwaliteit van het DGGRCMM kwalitatief hoogwaardig te laten worden om zo de validiteit en betrouwbaarheid van het onderzoek te vergroten. Dit zal bereikt worden door een methodologisch onderzoek uit te voeren, waarna ook antwoord gegeven kan worden op de hoofdvraag van dit onderzoek.

3. Methodologie

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Dit empirisch onderzoek is een kwalitatief verkennend onderzoek met als doel antwoord te kunnen geven op de empirisch deelvragen. De onderzoeksmethode die wordt toegepast is de deductieve methode, omdat de theorie uit de literatuur wordt getoetst in de praktijk bij één onderzoeksorganisatie (Thornhill et al., 2009). Er zal een kwalitatief onderzoek gedaan worden, omdat dan zoveel mogelijk kennis wordt vergaard.

Om de deelvragen te kunnen beantwoorden en doelstellingen te bereiken zal een enkelvoudige casestudie met een holistische benadering worden uitgevoerd om de kwalitatieve data te verzamelen. Een casestudie is hiervoor een geschikte methode, omdat deze aansluit bij de deductieve methode. Volgens Yin (2009) wordt een casestudie ook gebruikt om de 'wat', 'waarom' en 'hoe' vragen te kunnen beantwoorden. Dit is nodig om de DG van de onderzoeksorganisatie te onderzoeken. Casestudies hebben als voordeel dat er een beeld gevormd wordt van de huidige situatie en op meerdere manieren kan worden uitgevoerd. Een nadeel is dat door de beperkte tijd die beschikbaar is, het niet mogelijk is om meerdere organisaties te onderzoeken. Hierdoor wordt generaliseerbaarheid van de resultaten beperkt.

3.2. Technisch ontwerp: uitwerking van de methode

Om de validiteit van het onderzoek te vergroten worden interviews afgenomen bij vier experts binnen dezelfde organisatie. Deze experts hebben vele jaren ervaring op het gebied van GRC en DG. Ook hebben zij de kennis en expertise om het DGGRCMM goed te kunnen beoordelen en aan te vullen. Er worden semigestructureerde interviews afgenomen. Hierbij worden open vragen gesteld, waarop de geïnterviewde expert gelijk kan reageren. Ook kunnen er onderwerpen aangesneden worden, die leiden tot discussie. Deelname aan het onderzoek is vrijwillig. Iedere expert zal vooraf aan het onderzoek geïnformeerd worden over het doel van het onderzoek, rechten op privacy en op het annuleren van deelname. Het interview zal opgenomen worden (met toestemming), zodat geen gegevens gemist kunnen worden. Ook zullen de namen van de organisatie en experts worden geanonimiseerd om de privacy te waarborgen. De experts zullen een samenvatting ontvangen om deze te beoordelen met de vraag of zij willen tekenen voor akkoord. De interviews zullen per expert afgenomen worden in een aparte, rustige omgeving en zullen niet langer duren dan 90 minuten.

Het interview betreft een beoordeling van het DGGRCMM. De experts zullen gevraagd worden om de eigen organisatie te beoordelen aan de hand van het DGGRCMM. Per kwalificatie per criteria worden onderstaande vragen gesteld:

1. Zijn de gebruikte kwalificaties en criteria duidelijk, juist en volledig? Zijn er nog aanvullingen nodig?
2. Hoort deze dimensie thuis in het DGGRCMM? Waarom?
3. Zijn de kwalificaties in staat om de dimensie te meten in het DGGRCMM? Waarom?
4. Geven de kwalificaties van DG een volledig beeld van alle aspecten van het onderwerp? Waarom?
5. Zorgen de kwalificaties in het DGGRCMM ervoor om te kunnen groeien binnen de organisatie? Waarom?

Iedere gestelde vraag is een open vraag, zodat de expert een duidelijke uitleg kan geven en dieper op het onderwerp in kan gaan. Na elke vraag zullen er aanvullende vragen gesteld worden om zo een goed beeld van de organisatie te krijgen. Na de interviews worden de experts gevraagd het

DGGRCMM van de gehele organisatie met een online vragenlijst te beoordelen. De vragenlijst bestaat uit gesloten vragen en hebben alleen betrekking op de organisatievolwassenheidsniveaus. Er zal ook ruimte zijn voor een toelichting op de score. De validiteit van het DGGRCMM wordt hiermee vergroot.

3.3. Gegevensanalyse

Om te meten of het DGGRCMM wel of niet valide is worden onderstaande interviewvragen gesteld.

Interviewvragen:

1. Zijn de kwalificaties en criteria duidelijk, juist en volledig zijn voor de experts? Mogelijke aanvullingen worden hierin meegenomen.
2. Zijn er kwalificaties die niet thuishoren in het DGGRCMM? Zo ja, dan worden deze toegevoegd als verbeterpunt. Indien dit niet mogelijk blijkt te zijn, zal dit als punt worden beschouwd voor vervolgonderzoek.
3. Ontbreken er nog kwalificaties in het DGGRCMM? Zo ja, dan worden deze toegevoegd als verbeterpunt. Indien dit niet mogelijk blijkt te zijn, zal dit als punt worden beschouwd voor vervolgonderzoek.
4. Zijn de kwalificaties nuttig en relevant? Zo niet, dan worden deze toegevoegd als verbeterpunt. Indien dit niet mogelijk blijkt te zijn, zal dit als punt worden beschouwd voor vervolgonderzoek.
5. Zorgen de kwalificaties ervoor om te kunnen groeien in DG binnen de organisatie? Indien dit niet mogelijk blijkt te zijn, zal dit als punt worden beschouwd voor vervolgonderzoek.

Het voordeel van open interviewvragen is dat de expert gelijk kan reageren op een gestelde vraag, maar ook dieper in kan gaan op het onderwerp door het geven van praktijkvoorbeelden. Een nadeel is, dat de wijze van data verzamelen afhankelijk is van de kennis, ervaring en expertise van de onderzoeker zelf.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Binnen dit onderzoek worden de resultaten op een verantwoorde wijze opgezet, rekening houdend met validiteit, compleetheid, en ethische aspecten.

Betrouwbaarheid

Het onderzoek zal uitgevoerd worden bij één organisatie. Door het interviewen van vier experts, zal de betrouwbaarheid van de verzamelde gegevens worden vergroot. Tegelijkertijd is dit een nadeel, omdat maar een klein deel van de organisatie hierbij betrokken is. De interviews worden afgenomen door één persoon. Ieder interview wordt op dezelfde wijze uitgevoerd. Hierdoor kunnen overeenkomstige antwoorden in de interviews goed met elkaar vergeleken worden. De beoordelaarsbetrouwbaarheid wordt hierdoor vergroot. De betrouwbaarheid zal verder toenemen als een andere onderzoeker dit onderzoek nogmaals doet. Door de resultaten uit interviews samen te vatten en te laten accorderen door de experts, wordt de kans op waarnemersbias geminimaliseerd. In dit onderzoek is de waarnemersbias verkleind door de uitspraken van de experts letterlijk weer te geven in de uitwerking van het interview en tijdens de interviews een neutrale houding te hebben.

Begrips-/constructvaliditeit

Om de begripsvaliditeit te vergroten worden de getranscribeerde interviews van de experts uitgewerkt en ter akkoord getekend door de expert om interpretatieverschillen tegen te gaan. Om de inhoudsvaliditeit te waarborgen is tijdens de interviews gevraagd of de kwalificaties en criteria in het DGGRCMM volledig, juist en duidelijk zijn.

Interne en externe validiteit

De interne validiteit wordt vergroot, doordat er definities van de dimensies zijn opgesteld uit de literatuur en deze verder uitgewerkt zijn in het onderzoek. Er is gezocht naar verbanden tussen de opzet en uitvoering van het onderzoek en de hieraan verbonden resultaten en conclusies. Aan de hand hiervan is het DGGRCMM opgesteld. Om sociaal gewenste antwoorden te verkleinen is vooraf kenbaar gemaakt om de organisatie- en persoonsgegevens te anonimiseren, wat ten goede komt aan de interne validiteit. Een beperking is echter de kennis en het inzicht van de onderzoeker zelf. Om respondentbias tegen te gaan is gekozen om alleen verdiepende vragen te stellen naar aanleiding van uitspraken van de geïnterviewde expert en niet te refereren naar andere experts. Om de externe validiteit te verhogen is gezocht naar experts die inhoudelijk kennis hebben en werkzaam zijn op het gebied van DG met name gericht op GRC. De kans bestaat dat de expert niet genoeg kennis heeft over het onderwerp. Daarom is tijdens het interview gevraagd om dit kenbaar te maken. Een nadeel is dat het onderzoek slechts bij één organisatie wordt uitgevoerd. De generaliseerbaarheid zou vergroot worden als het onderzoek bij meerdere organisaties zou plaatsvinden.

Ethische aspecten

In dit onderzoek is de verzamelde data geanonimiseerd en zijn er geen persoons- of organisatiegegevens opgenomen. Om ervoor te zorgen dat de experts weten wat ze kunnen verwachten is een Interviewprotocol opgesteld. Hierin staan de ethische aspecten als privacy, vrijwilligheid en anonimiteit vermeld. In het Interviewprotocol is ook het Toestemmingsformulier opgenomen, dat zowel door de geïnterviewde als de onderzoeker getekend wordt. Het interviewprotocol is toegevoegd als Bijlage 4.

4. Resultaten

4.1. Onderzoeksorganisatie

Het onderzoek heeft plaatsgevonden bij een kleine Nederlandse zorgverzekeraar. In jaar 2017 heeft De Nederlandse Bank (DNB) richtlijnen en verwachtingen voor de beheersing van datakwaliteit opgesteld. De onderzochte organisatie is vanaf dat moment al bezig om DG te implementeren binnen de organisatie. De onderzoeksorganisatie moest door deze richtlijnen een datakwaliteitsbeleid opstellen met daarin de structuur, het beleid, de verantwoordelijkheden, bedrijfsprocessen, interne controles en de vastlegging daarvan. In jaar 2018 is door een extern bedrijf een onderzoek uitgevoerd naar de status van de organisatie op het gebied van DG. Uit het onderzoek bleek dat de vastlegging van processen niet gedaan werd binnen de organisatie. Na dit onderzoek is een datakwaliteitsbeleid opgesteld met daarin beschreven welke richtlijnen er zijn op het gebied van datakwaliteit, hoe risico's beoordeeld worden en welke controles hierop plaatsvinden. Daarnaast is een governance raamwerk opgesteld en een ICT-landschap vastgelegd.

4.2. Experts

Er zijn vier experts geïnterviewd. Drie experts zijn werkzaam in de dimensies GRC en zijn apart van elkaar geïnterviewd. De vierde expert is expert op het gebied van interne audit, het toetsen van de regels en risicobeheersing.

De eerste expert voert alle werkzaamheden uit die te maken hebben met het opstellen van de jaarrekening, waarbij rekening moet worden gehouden met de regels van Solvency II en de vereisten van DNB.
De tweede expert is compliance officer die verantwoordelijk is voor het compliance beleid. De expert zorgt ervoor dat de organisatie haar compliance- en integriteitsrisico's kent en adviseert in beheersmaatregelen.
De derde expert is riskmanager. De riskmanager brengt alle risico's binnen de organisatie in kaart, analyseert en beoordeelt deze, stelt beheersmaatregelen op en toetst deze. De risico's worden gerapporteerd aan het bestuur.
De vierde expert is manager van de afdeling interne-audit en toetst de effectiviteit van de processen van risicomanagement, beheersing en governance.

Alle vier de experts kunnen een goed oordeel geven op het DGGRCMM, omdat zij allen kennis en expertise hebben op het gebied van GRC, waardoor het mogelijk is om praktijkvoorbeelden te achterhalen. Daarnaast wordt DG toegepast binnen de organisatie. Hierdoor is het mogelijk om het DGGRCMM goed te kunnen beoordelen.

4.3. Context onderzocht organisatie

Voor het onderzoek is het van belang dat de experts ook daadwerkelijk de juiste kennis en expertise hebben op het gebied van DG. Om dit aan te tonen, zijn opvallende citaten met betrekking tot DG vastgelegd. De citaten geven weer hoe DG in de praktijk wordt toegepast.

Citaat 1: "In het governance beleid staat specifiek opgenomen hoe de structuur is, hoe de rapportagelijnen liggen en wie de verantwoordelijkheden binnen de organisatie, dat is je basis."

Citaat 2: "Vastleggen van uitkomsten van processen is niet een sterk punt bij de organisatie."

Citaat 3: "De organisatie moet een governance structuur en beleid hebben."

Citaat 4: "De riskmanager zal verantwoording moeten afleggen aan het bestuur."

Citaat 5: "Als je risico's niet monitort, dan weet je niet wat je risico's zijn."

Citaat 6: "Als er een risico geïdentificeerd is, dan wordt erop gehandeld, dit is vastgelegd in stukken over datakwaliteit waaraan voldaan moet worden."

Citaat 7: "De organisatie moet voldoen aan regels en voorwaarden, er wordt uitgevoerd wat de overheid oplegt."

Citaat 8: "Het gaat om het bewust zijn van regels binnen de organisatie."

Uit de citaten blijkt dat de onderzoeksorganisatie bewust is van DG en het toepassen daarvan. Ook blijkt hieruit dat de experts voldoende kennis en expertise hebben om het DGGRCMM goed te kunnen beoordelen.

4.4. Resultaten van het onderzoek op deelvraag I

Om deelvraag één te kunnen beantwoorden is onderzocht hoe het DGGRCMM getoetst kan worden als meetinstrument voor het beoordelen van de organisatievolwassenheid in DG. Per dimensie zijn de resultaten weergegeven plus de beoordeling van de organisatievolwassenheid bij de onderzoeksorganisatie.

4.4.1 Gezag en verantwoordelijkheden

Dimensie van Governance	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Gezag en verantwoordelijkheden	Gezag				1	3	
	Verantwoordelijkheden				4		

Figuur 7: Resultaten dimensie Gezag en verantwoordelijkheden

Governance wordt gezien als een belangrijk onderdeel in de beheersing waar gezag en verantwoordelijkheden onder vallen. In het governancebeleid zijn alle regels vastgelegd, waaronder gezag en verantwoordelijkheden. Hierin is specifiek opgenomen hoe de structuur en de rapportagelijnen liggen en wie welke verantwoordelijkheden hebben. Gezag bleek voor alle experts moeilijk te meten. De experts ervaarden macht in de criteria als erg negatief. De beslissingen worden bij de onderzoeksorganisatie genomen op basis van adviezen van de $1^e/2^e$ lijn. Het bestuur is eindverantwoordelijk en neemt de definitieve beslissingen. De kwalificatie werd wel relevant bevonden.

Verantwoordelijkheden zijn in de structuur van de functie vastgelegd. Iedere werknemer is verantwoordelijk voor bepaalde onderdelen en dat is vastgelegd in charters. Hierover wordt gerapporteerd en getoetst. Het vastleggen van processen wordt niet consequent gedaan.

De experts gaven aan dat gezag en verantwoordelijkheden dicht elkaar liggen. Het hangt af van de organisatie en de grootte van de organisatie.

4.4.2 Structuur en beleid

Dimensie van Governance	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Structuur en beleid	Structuur			2	2		
	Regels/procedures				2	2	
	Controle professionals			3	1		

Figuur 8: Resultaten dimensie Structuur en beleid

De organisatiestructuur, regels en het beleid zijn vastgelegd. De organisatie moet voldoen aan de eisen van het raamwerk van DNB en daarover rapporteren. “Zonder structuur en beleid is er geen governance”, citeerde expert 2.

Regels/procedures zijn in de structuur opgenomen voor de hele organisatie. Hierin is een governance raamwerk, een ICT-landschap en een datakwaliteitsbeleid opgenomen. Uit het datakwaliteitsproject zijn Key Risk Controls (KRC’s) opgesteld om de risico’s te beheersen. Hierop zijn processen aangepast.

Er is binnen de organisatie geen DG-expert aanwezig. De experts vinden dat ook niet noodzakelijk. Er zijn wel sleutelfuncties ingericht. Bij een grote organisatie zou wel een DG-expert aanwezig kunnen zijn.

Voor de eindbeoordeling wordt elk stuk ter sprake gebracht in een directieoverleg. De directie geeft aan of deze goedgekeurd wordt. Voor de controle op professionals worden externen ingehuurd

zoals de accountant. De externe controles zijn altijd gepland. Het oordeel is wel afhankelijk per organisatie. Binnen deze organisatie geeft de professional een eigen oordeel op de KRC. Af en toe wordt daarin een steekproef genomen en wordt er gevraagd om “evidence”. De experts gaven aan dat de criteria niet helemaal te volgen zijn. Een externe audit is niet beter dan een interne audit. Eén expert gaf aan dat de criteria gewijzigd moeten worden van ad hoc audit naar jaarlijkse toetsing met interne en/of externe audit.

4.4.3 Rapporteren

Dimensie van Governance	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Rapporteren	Resultaten rapporteren				3	1	
	Rapporteren incidenten				1	2	1

Figuur 9: Resultaten dimensie Rapporteren

Resultatenanalyse werd door één expert niet duidelijk bevonden. De criteria waren niet duidelijk en ook de kwalificatie was niet te plaatsen. Resultaten rapporteren werd wel relevant bevonden. De kwalificatie is daarom aangepast. De andere expert gaf aan dat de riskmanager verantwoording moet afleggen aan Raad van Bestuur en Raad van Commissarissen. Er zijn indicatoren vastgesteld om resultaten te kunnen analyseren zoals Key Performance Indicatoren (KPI’s) en Key Risk Controls (KRC’s). “Zonder rapportage is er geen inzicht” gaf expert 3 aan.

Voor het rapporteren van incidenten is een incidentenregister aanwezig. Dit is een vereiste van DNB. Expert 3 gaf aan dat bij deze organisatie zo weinig incidenten zijn, dat er bijna geen meting kan plaatsvinden. De incidenten worden maandelijks in het managementoverleg besproken. Er is een procedure aanwezig bij een datalek.
Expert 4 gaf aan dat rapporteren eigenlijk onder het beleid van governance thuishoort. “In het beleid staat de opzet van de organisatie waarover gerapporteerd moet worden zoals rapporteren en incidenten.” Met rapporteren wordt verantwoording afgelegd vanuit de organisatie. Bij governance worden alle regels opgesteld. Als het puur over het rapporteren van rapporten gaat, dus de rapporten die gezien worden binnen de organisatie, dan hoort deze wel onder governance thuis.

4.4.4 Monitoring

Dimensie van Risk-management	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Monitoring	Structuur			1	1	2	
	Indicatoren en monitoring			2		2	

Figuur 10: Resultaten dimensie Monitoring

Per afdeling is er door de riskmanager een raamwerk opgezet waarin de risico’s staan die de afdeling loopt. Ook wordt dit gerapporteerd. Er worden indicatoren gebruikt zoals KPI’s en KRC’s om de risico’s te monitoren. Dit wordt vastgelegd in Word en Excel. Er wordt ook aan de betreffende stakeholders gerapporteerd. “Zonder monitoring is er geen inzicht in de beheersing”, gaven meerdere experts aan. Indicatoren zijn zeer nauw verbonden met de structuur, ze zijn onderdeel van de structuur. Meerdere experts gaven aan dat een dashboard om te monitoren meer is weggelegd voor grotere organisaties. Voor kleinere organisaties zijn andere indicatoren ook goed, als het ervoor zorgt dat het proces en de risico’s beheerst zijn.

4.4.5 Beheersen risico's

Dimensie van Risk-management	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Beheersen risico's	Risicoanalyse				2	2	
	Beheersing risico's				2	2	

Figuur 11: Resultaten dimensie Beheersen risico's

Jaarlijks vindt een strategische risicoanalyse plaats. Er wordt een risicoanalyse uitgevoerd bij het nemen van een belangrijke beslissing binnen de organisatie. De risico's worden gerapporteerd aan het bestuur. Per afdeling zijn risicoanalyses gemaakt en gerapporteerd.
Als een risico wordt geïdentificeerd, dan wordt er ook naar gehandeld. Dit is vastgelegd in het stuk datakwaliteit. Er is documentatie aanwezig om aan het raamwerk te kunnen voldoen.
Als er geen structuur is, kan er niet gemonitord worden. "Een eenvoudige structuur kan al voldoende zijn" gaf expert 3 aan. Bij het ontwikkelen van nieuwe systemen wordt ook AVG meegenomen. De AVG is vastgelegd onder governance. Dit moet goed bekend zijn binnen de organisatie. Expert 3 gaf aan dat de stap tussen "sommige typen risico's worden gemonitord" naar "risico's worden gemonitord" te groot is. Hier zou een tussenstap moeten komen met "de hoofdrisico's worden gemonitord en beheerst".

4.4.6 Naleving beleid

Dimensie van Compliance	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Naleving beleid	Structuur					3	1
	Regels naleven				1	3	
	Controles			2		2	

Figuur 12: Resultaten dimensie Naleving beleid

De organisatie moet voldoen aan wet- en regelgeving. Dit is in het beleid vastgelegd. Er moet onder andere voldaan worden aan de kwalificaties van Wet op Financieel Toezicht (WFT) en Burgerlijk Wetboek voor de rapportages.
Eén expert gaf aan dat in de criteria soortgelijke processen binnen de structuur niet te standaardiseren zijn. Compliance gaat over de regels van processen uitvoeren, niet de processen standaardiseren. Regels naleven en controles zijn wel relevant bevonden. De structuur is hierbij niet relevant volgens één expert. Expert 4 gaf aan bij regels naleven, dat regels naleven eigenlijk gelijk is aan structuur. Naleven regels weghalen of samenvoegen met structuur. Door het uitvoeren van controles kan er bepaald worden waar de organisatie staat in verband met het naleven van regels.

De organisatie moet voldoen aan regels en voorwaarden die de overheid opgelegd. Dit wordt opgenomen in de ontwikkeling van de systemen en de inrichting van processen.
Er worden controles uitgevoerd op de naleving van het beleid. Voor de toetsing van het beleid is intern een screeningsbeleid opgesteld waar audits op uitgevoerd worden.
Expert 3 gaf aan dat de criteria vanaf established process niet passen binnen de organisatie. Er is een geautomatiseerd compliance systeem om te voldoen aan de berekeningswijze van de verantwoording. Het is een beheersing tool om ervoor te zorgen dat het risico op non-compliance nul is. Expert 4 gaf aan dat veel processen al geautomatiseerd zijn zoals controles op declaraties.
Eén expert gaf aan dat de regelgeving per organisatie anders kan zijn. Deze organisatie houdt zich aan de financiële verantwoording. Het medisch dossier van een ziekenhuis zal aan andere eisen moeten voldoen. De interne regelgeving is belangrijk, maar dat maakt het ook ingewikkeld.

4.4.7 Bewustzijn

Dimensie van Compliance	Kwalificaties	No process	Beginning process	Established process	Managed process	Optiming process	Geen Keuze
Bewustzijn	Bewust zijn van compliance			1		3	

Figuur 13: Resultaten dimensie Bewustzijn

Bewustzijn van de regels is voor een organisatie een randvoorwaarde. Bewustzijn gaat volgens de experts om betrouwbaarheid en integriteit. Het uitvoeren van controles op de declaratie is geautomatiseerd. Het toetsen aan wet- en regelgeving gebeurt door externe partijen zoals het Nederlands Zorginstituut (ZINL) en de Nederlandse Zorgautoriteit (NZA). Er wordt een controle gedaan op de rapportage om te zien of er voldaan wordt aan de wet- en regelgeving. Wordt er niet aan voldaan, dan wordt er door NZA, ZINL of DNB een boete gegeven of een aantekening gemaakt.

Er zijn sleutelfuncties ingericht om het naleven van de regels te toetsen. Voor de interne regels is de integriteit een heel belangrijk onderdeel. Dit wordt volgens één of meerdere experts gemist in de kwalificaties. Andere experts geven aan, dat dit valt onder de naleving van het beleid en zien deze niet als een nieuwe kwalificatie. Ook vonden de experts de criteria te breed.

Eén expert gaf aan dat er voor de gehele organisatie controles zijn in de processen. Het is van belang binnen iedere organisatie dat men bewust is van compliance en de regels naleeft. Door interviews af te nemen wordt gecontroleerd of regels worden nageleefd. Dit wordt vastgelegd.

Naast het interview was er een vragenlijst uitgezet onder de geïnterviewde experts om de gehele organisatie nogmaals te beoordelen met de kennis die zij hebben opgedaan tijdens het interview (zie Bijlage 4). De resultaten zijn hieronder vermeld.

Domeinen	Dimensies	Kwalificaties	Expert 1	Expert 2	Expert 3	Expert 4
Governance	Gezag en verantwoordelijkheden	Gezag	Level 5	Level 5	Level 5	Level 5
		Verantwoordelijkheden	Level 5	Level 4	Level 5	Level 4
	Structuur en beleid	Structuur	Level 5	Level 1	Level 4	Level 1
		Regels\procedures	Level 5	Level 5	Level 4	Level 5
		Controle professionals	Level 5	Level 3	Level 4	Level 5
	Rapporteren	Resultaten rapporteren	Level 5	Level 4	Level 5	Level 4
		Rapporteren incidenten	Level 5	Level 4	Level 4	Level 5
Risk Management	Monitoring	Structuur	Level 5	Level 5	Level 4	Level 5
		Indicatoren en monitoring	Level 5	Level 5	Level 3	Level 5
	Beheersen risico's	Risicoanalyse	Level 4	Level 4	Level 2	Level 5
		Beheersing risico's	Level 5	Level 5	Level 4	Level 5
Compliance	Naleving beleid	Structuur	Level 5	Level 5	NR	Level 5
		Regels naleven	Level 5	Level 4	Level 4	Level 5
		Controles	Level 2	Level 5	Level 5	Level 3
	Bewustzijn	Bewust zijn van compliance	Level 5	Level 5	Level 3	Level 4

Legenda	
	Level 5
	Level 4
	Level 3
	Level 2
	Level 1
	Niet relevant (NR)

Figuur 14: Resultaten vragenlijst

Expert 1 en 4 beoordelen de onderzoeksorganisatie grotendeels op niveau 5. Controles worden door expert 1 op niveau 2 beoordeeld, omdat de controles niet allemaal geautomatiseerd plaatsvinden. Structuur wordt op niveau 1 beoordeeld door expert 1 en 4, omdat er geen specifieke DG-expert als functie aanwezig is. Er is wel een DG-datakwaliteitsbeleid opgezet door verschillende experts binnen de organisatie. Expert 2 en 3 beoordelen de organisatie grotendeels op volwassenheidsniveau 3, 4 en 5. Dit komt mede, doordat ze meer inhoudelijke kennis en werkervaring hebben op het gebied van GRC.

Bevestiging kwalificaties en score per kwalificatie

De analyse van de interviews in combinatie met de volwassenheidsscore van de organisatie hebben geleid tot onderstaande bevindingen voor het DGGRCMM.

Alle dimensies en kwalificaties zijn bevestigd met praktijkvoorbeelden door één of meerdere experts. Enkele kwalificaties werden als 'neutraal' ingevuld, maar geen van de kwalificaties werd als niet relevant beoordeeld. In onderstaande tabel is de bevestiging weergegeven per kwalificatie.

Dimensies van GRC	Kwalificaties	Expert 1	Expert 2	Expert 3	Expert 4
Gezag en verantwoordelijkheden	Gezag	v	v*	v	v
	Verantwoordelijkheden	v	v	v	v*
Structuur en beleid	Structuur	v	v*	v*	v
	Regels/procedure	v	v	v	v
	Controle professionals	v	v*	v	v
Rapporteren	Resultaten rapporteren	v	v*	v	v
	Rapporteren incidenten	v	v	v	v
Monitoring	Structuur	v	v	v	v
	Indicatoren en monitoring	v	v	v	v
Beheersen risico's	Risicoanalyse	v	v	v	v
	Beheersing risico's	v	v	v	v
Naleving beleid	Structuur	v	v	v	v
	Regels naleven	v	v	v	v
	Controles	v	v	v	v
Bewustzijn	Bewust zijn van compliance	v	v	v	v
		v	v*	v	v

v = bevestiging
v* = meer uitleg nodig
grijs = geen expertise

Figuur 15: Bevestiging kwalificaties

Tijdens de interviews is het DGGRCMM getoetst op organisatievolwassenheid. Dit werd gedaan door per kwalificatie een score te geven om te zien hoe de organisatievolwassenheid van de onderzoeksorganisatie op dit moment is. Het totaal van de scores per kwalificatie per volwassenheidsniveau wordt in onderstaande tabel getoond.

Dimensies van GRC	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process	Geen Keuze
Gezag en Verantwoordelijkheden	Gezag				1	3	
	Verantwoordelijkheden				4		
Structuur en Beleid	Structuur			2	2		
	Regels\procedures				2	2	
	Controle professionals			3	1		
Rapporteren	Resultaten rapporteren				3	1	
	Rapporteren incidenten				1	2	1
Monitoring	Structuur			1	1	2	
	Indicatoren en monitoring			2		2	
Beheersen risico's	Risico-analyse				2	2	
	Beheersing risico's				2	2	
Naleving beleid	Structuur					3	1
	Regels naleven				1	3	
	Controles			2		2	
Bewustzijn	Bewust zijn van compliance			1		3	

Figuur 16: Uitkomsten DGGRCMM

Het resultaat is dat de organisatie het meest scoort op volwassenheidsniveau 4 en 5. Met uitzondering op controle professionals. Hierbij werd volwassenheidsniveau 3 gescoord.

4.5. Resultaten van het onderzoek op deelvraag II

Om deelvraag twee te kunnen beantwoorden is gezocht naar aanvullingen op het DGGRMM om te kunnen groeien in DG. Door één expert wordt aanbevolen om de onderstaande kwalificatie toe te voegen in het DGGRCMM.

Nieuwe kwalificatie:

- Integriteit – De interne regels binnen de organisatie worden gezien als een belangrijk onderdeel binnen compliance.

Deze kwalificatie staat niet in de literatuur genoemd, maar is ontstaan in de praktijk. Deze kwalificatie kan op inductieve wijze worden bevestigd in een vervolgonderzoek.

Criteria aangepast

- De criteria zijn concreter beschreven om te kunnen groeien in DG. Dit leidt tot DGGRCMM V0.2 (zie Bijlage 6).

Centraliseren van kwalificatie structuur:

- Structuur wordt gezien als belangrijk onderdeel dat valt onder governance.

De kwalificatie structuur staat in de literatuur genoemd onder GRC. In de praktijk is ontstaan, dat de structuur alleen onder governance thuishoort. Of structuur alleen onder governance hoort, kan op inductieve wijze worden bevestigd in een vervolgonderzoek.

5. Discussie, conclusies en aanbevelingen

5.1. Discussie

Hieronder is de discussie van het literatuur- en empirisch onderzoek beschreven.

5.1.1 Literatuuronderzoek

Naar aanleiding van het literatuuronderzoek uit hoofdstuk 2, worden in dit hoofdstuk de resultaten weergegeven. Onderstaande resultaten worden nader toegelicht:

1. Kwalificatie structuur valt onder governance.
2. Dashboard is niet rendabel bij een kleine organisatie.
3. Er is geen DG-expert aanwezig.
4. Extra uitleg nodig bij criteria.
5. Integriteit nieuw onderdeel in DGGRCMM?

1.
Kwalificatie structuur staat onder GRC, zoals ook te zien is in het GRC-model van Batenburg, Neppelenbroek en Shahim (2014). Volgens de experts zou de structuur alleen onder governance moeten staan, omdat onder governance de structuur wordt bepaald en daar moet eenieder zich aan houden. Dit is ook terug te zien in het GRC-model van Vicente & da Silva (2011). Dit geeft als inzicht dat de literatuur van Vicente & da Silva (2011) overeenkomt met de praktijk. Het verschil is, dat het onderzoek door Batenburg, Neppelenbroek & Shahim (2014) is uitgevoerd bij een ziekenhuis, dat vele malen groter is dan de onderzoeksorganisatie. Bij grotere organisaties zoals een ziekenhuis zijn er meer mensen, afdelingen en regels, waardoor het inzichtelijker is om voor GRC apart de structuur te bepalen. Verder onderzoek hiernaar is noodzakelijk om erachter te komen of de structuur bij een kleine organisatie alleen onder governance valt of toch onder GRC.

2.
In de literatuur is in het model van Vicente & da Silva (2014) monitoren, dashboards en rapporteren buiten het model gelaten omdat dit te complex is. Batenburg, Neppelenbroek & Shahim (2014) nemen deze punten wel op in het GRC maturity model for hospitals, omdat dit essentiële onderdelen zijn in het model. Opvallend was dat de onderzoeksorganisatie geen gebruik van dashboards maakt omdat het niet rendabel is, maar het wel noodzakelijk vond dat de gegevens getoond moeten worden in een andere vorm dan een dashboard, zoals in Key Performance Indicators (KPI's) en Key Risk Controls (KRC's), zodat de betrouwbare data aan het bestuur periodiek gerapporteerd kan worden.
Voor kleine organisaties is het van belang dat het proces en de risico's beheerst zijn en de data betrouwbaar is. Grote organisaties moeten voldoen aan meer eisen en regels die getoond moeten worden aan meerdere afdelingen en managers. Een dashboard zou daarbij een goed hulpmiddel zijn. Dit geeft als inzicht dat het niet altijd noodzakelijk is om een dashboard te hebben binnen een kleine organisatie, maar dat een andere indicator zoals een KPI of KRC, ook ingezet kan worden om processen te tonen en de risico's te beheersen. Op deze wijze is de organisatie ook in staat om betrouwbare data te tonen.

3.
Bij de onderzoeksorganisatie is geen DG-expert aanwezig. De vraag is of dit wel nodig is bij een kleine organisatie. In de onderzoeksorganisatie zijn sleutelfuncties ingericht van mensen die de

benodigde kennis en expertise hebben. Die kennis tezamen zorgt ervoor dat de DG goed geïmplementeerd en uitgevoerd kan worden. Bij grotere organisaties is het wellicht wel nodig, omdat het volume aan data dan vele malen groter is dan bij een kleinere organisatie. De risico's zijn dan ook veel groter. Het belangrijkste inzicht hierbij is dat er geen DG-expert aanwezig hoeft te zijn in kleinere organisaties. Er moet wel een goed DG-beleid opgesteld zijn door experts binnen de organisatie om de risico's te kunnen beheersen. Het is goed om hier vervolgonderzoek naar te doen.

4.

Bij meerdere criteria was meer uitleg nodig, omdat de criteria als abstract werden bevonden. Bij enkele experts was de kennis ook niet toereikend om aan te kunnen geven of de kwalificatie te meten was met bijbehorende criteria. Er werd aangeraden om de criteria concreter te maken. Zou dit niet voor elke organisatie gelden in een andere branche? Niet alle elementen in het model zijn van toepassing op de kleine onderzoeksorganisatie. Bij grotere organisaties zouden deze elementen wel allemaal van toepassing kunnen zijn. Het is goed om hier vervolgonderzoek naar te doen.

5.

Integriteit zou volgens één of meerdere experts toegevoegd moeten worden als kwalificatie aan het model. De integriteit is belangrijk binnen de organisatie, want het bepaalt de normen en waarden die binnen een organisatie aanwezig zijn. Bovendien is het een proces van voortdurende bewustwording binnen organisaties. Maar horen deze thuis als een nieuwe kwalificatie in het model of valt dit onder het compliance beleid? Integriteit van data is onderdeel van de strategie. DG moet begrepen worden binnen de organisatie en daar moet naar gehandeld worden. Het is belangrijk dat data op de juiste manier vastgelegd wordt, zodat het betrouwbaar is. Integriteit speelt daarbij zeker een bepaalde rol. Integriteit is belangrijk binnen de onderzoeksorganisatie om het vertrouwen van de klant te winnen. De onderzoeksorganisatie is gebaad bij binding met de klant en het positief verspreiden van de goede reputatie. Maar ook intern is integriteit belangrijk voor de medewerkerstevredenheid en de bedrijfscultuur. Integer handelen zorgt voor een betere service naar de klant toe. Vervolgonderzoek zal nodig zijn om te onderzoeken of integriteit ook bij andere (soortgelijke) organisaties een belangrijke rol speelt en of deze als nieuwe kwalificatie opgenomen zou moeten worden in het DGGRCMM.

5.1.2 Empirisch onderzoek

Het DGGRCMM is getoetst bij één onderzoeksorganisatie. De experts gaven aan dat het DGGRCMM geschikt is om te groeien in DG, maar dan wel beginnend met een lage score. Bij hogere scores is de organisatie al bewust van DG. Het model zou aangepast moeten worden naar een specifiek onderwerp waarvan de organisatievolwassenheid laag is beoordeeld.

Uit de interviews is één nieuwe aanvulling op het model gekomen, namelijk integriteit. Integriteit zou als nieuwe kwalificatie opgenomen kunnen worden in het model. Verder onderzoek zal nodig zijn om uit te zoeken of integriteit valt onder het compliance beleid of als nieuwe kwalificatie in het DGGRCMM.

Ook gaven één of meerdere experts aan dat de criteria erg abstract waren beschreven, waardoor het makkelijk was om de organisatie goed te scoren. Zij gaven aan deze concreter te maken en specifiek te maken voor organisaties uit verschillende branches. Ook bleek dat niet alle criteria toepasbaar waren binnen de onderzoeksorganisatie of ontbraken er criteria. De criteria die zijn

hierop aangepast voor de onderzoeksorganisatie. Verder onderzoek zou uit moeten wijzen of deze aanpassingen ook van belang zijn bij andere kleine organisaties, maar ook bij grote organisaties.

Eén expert gaf aan dat structuur en naleving beleid eigenlijk hetzelfde is. Andere experts gaven aan dat structuur eigenlijk alleen onder governance wordt bepaald. Dat is de basis waaraan eenieder zich moet houden. Naleving beleid is wel relevant onder compliance, dat is ook terug te zien in de literatuur. Verder onderzoek in de praktijk zal nodig zijn bij zowel kleine als grote organisaties om te bepalen of structuur alleen onder governance thuishoort of bij GRC apart.

Het DGGRCMM was goed te toetsen bij de onderzoeksorganisatie. De organisatie is bewust van DG en datakwaliteit en het toepassen daarvan. Dit kwam mede, doordat er al een onderzoek had plaatsgevonden in jaar 2018. De onderzoeksorganisatie moet zich houden aan bepaalde wet- en regelgeving, wat voor iedere organisatie weer anders kan zijn. Doordat de criteria nu zijn aangepast is het model meer toepasbaar geworden in de praktijk. In de praktijk zal uit moeten wijzen of het model ook toepasbaar is bij andere kleine organisaties en grote organisaties.

5.2. Conclusies

Naar aanleiding van de onderzoeksbevindingen in hoofdstuk 4, worden in dit hoofdstuk de conclusies getrokken.

De hoofdvraag van dit onderzoek luidt: '**Hoe kan de organisatievolwassenheid van de GRC-dimensies binnen DG worden gemeten?'**.
Om de hoofdvraag te kunnen beantwoorden, moet eerst antwoord gegeven kunnen worden op onderstaande deelvragen:

1. Hoe kan de organisatievolwassenheid in DG met de dimensies, levels en criteria uit de literatuur worden beoordeeld en in de vorm van het DGGRCMM?
2. Wat zijn relevante aanvullingen voor organisaties op het DGGRCMM om te kunnen groeien in DG?

Deelvraag 1: 'Hoe kan de organisatievolwassenheid in DG met de dimensies, levels en criteria uit de literatuur worden beoordeeld en in de vorm van het DGGRCMM?'
Voor het beantwoorden van deelvraag 1, worden op basis van de onderzoeksbevindingen uit hoofdstuk 4 onderstaande deelconclusies getrokken:

- Op basis van literatuuronderzoek zijn alle definities met betrekking tot DG, GRC en Maturity model herkend en bevestigd door de experts.
- Volgens de principes van Pöppelbuβ & Röglinger (2011) is het DGGRCMM opgesteld om de organisatievolwassenheid te beoordelen om te kunnen groeien in DG.
- Door het DGGRCMM in de praktijk te toetsen konden alle dimensies, kwalificaties en levels herkend en bevestigd worden door de experts met praktijkvoorbeelden.
- Bij tien van de vijftien criteria zijn aanpassingen gedaan in het DGGRCMM, waardoor de experts in staat waren om de organisatievolwassenheid aan de hand van de volwassenheidsniveaus te beoordelen.

Deelvraag 2: 'Wat zijn relevante aanvullingen voor organisaties op het DGGRCMM om te kunnen groeien in DG?'
Voor het beantwoorden van deelvraag 2, worden op basis van de onderzoeksbevindingen uit hoofdstuk 4 onderstaande deelconclusies getrokken:

- Het toevoegen van integriteit aan het DGGRCMM. Door één of meerdere experts werd bevestigd, dat integriteit een belangrijk gemist onderdeel is in het DGGRCMM.
- Als de organisatie een hoge score heeft als volwassenheidniveau, dan zou volgens de experts het model specifiek op een bepaald onderwerp gericht moeten zijn. Het DGGRCMM zou hierdoor beter beoordeeld kunnen worden door een organisatie. Bij een lage score is het DGGRMM geschikt bevonden, nadat de verbeterpunten in de criteria waren aangepast.
- Bij de kwalificatie structuur werd aangegeven door de experts dat de structuur onder governance wordt bepaald en niet onder riskmanagement of compliance. Vervolgonderzoek bij andere kleine en grotere organisaties zal uit moeten wijzen of de structuur onder GRC moet vallen of alleen onder governance.

Er kan nu antwoord gegeven worden op de hoofdvraag van dit onderzoek:

'**Hoe kan de organisatievolwassenheid van de GRC-dimensies binnen DG worden gemeten?'**

De organisatievolwassenheid van de GRC-dimensies binnen DG kan gemeten worden door semigestructureerde interviews in de praktijk af te nemen, nadat het DGGRCMM is ontwikkeld op basis van de wetenschappelijke literatuur. Bij de interviews wordt van elke kwalificatie gevraagd of deze te meten is in de praktijk en of deze kwalificatie thuishoort in het DGGRCMM. De criteria per kwalificatie worden beoordeeld door de experts en er wordt een score gegeven om de organisatie te beoordelen op volwassenheid. Door de waaromvraag te stellen, worden voorbeelden gegeven om het antwoord te bevestigen. Hierdoor kan het DGGRCMM volledig worden getoetst op relevante dimensies, kwalificaties, levels en criteria. Hiermee kan de organisatievolwassenheid volledig worden gemeten. Het DGGRCMM is hiermee relevant, betrouwbaar en is een valide meetinstrument om de GRC-dimensies binnen DG te kunnen meten.

5.3. Aanbevelingen voor de praktijk

Organisaties die nog niet geheel bewust zijn van DG, kunnen het DGGRCMM goed gebruiken om te kunnen groeien in DG. De organisatie krijgt met dit model handvaten om belangrijke dimensies en kwalificaties te implementeren binnen de organisaties. Wettelijke eisen zorgen ervoor dat er een goed DG-beleid moet worden opgezet. Er zal geïnventariseerd moeten worden of er een DG-beleid is waarin de GRC is vastgelegd. GRC opnemen in het DG-beleid kan meerwaarde bieden voor DG door het bepalen van de structuur en het beleid binnen governance, risico's in kaart brengen en beheersen en controles doen op de naleving van de regels die bij governance zijn opgesteld. De betrouwbaarheid van data wordt hiermee vergroot en de datakwaliteit gewaarborgd. Een belangrijk punt hierbij is de vastlegging van structuur en beleid onder governance. Dat vormt de basis om risico's te kunnen beheersen en wet- en regelgeving te kunnen naleven.

5.4. Aanbevelingen voor verder onderzoek

Uit literatuuronderzoek is gebleken dat er nog weinig wetenschappelijk onderzoek heeft plaatsgevonden naar GRC binnen DG. Dit onderzoek heeft aangetoond dat GRC binnen DG een belangrijk onderdeel is om te kunnen groeien in DG. Verder onderzoek is nodig om nog meer te kunnen groeien in DG. De aanbevelingen die de experts hebben gegeven komen in aanmerking voor verder onderzoek. De onderzoeksorganisatie is klein. Een aanbeveling is om hetzelfde onderzoek ook uit te voeren bij andere kleine organisaties en bij grotere organisaties. Mogelijk leidt dit tot aanvullingen of verbeteringen in het DGGRCMM.

Een volgende onderzoeker die het DGGRCMM beoordeelt, zal kunnen aangeven of integriteit in het model opgenomen moet worden als kwalificatie. Nader onderzoek zou ook kunnen uitwijzen of de structuur binnen GRC alleen onder governance opgenomen dient te worden of toch bij GRC. En als de structuur apart wordt opgenomen, valt naleven regels dan niet onder de structuur? De regels zijn immers opgesteld onder de structuur. Dit is in dit onderzoek niet verder onderzocht.

Mogelijk leidt het aanvullen of het wijzigen van criteria tot verbeteringen in het model, zodat deze nog specifieker wordt voor een andere onderzoeksorganisatie.

5.5 Reflectie

Reflecterend op de methode van dit onderzoek en de betrouwbaarheid van de resultaten kunnen onderstaande punten worden benoemd:

Literatuuronderzoek:

- Er was weinig literatuur beschikbaar op het gebied van GRC maturity modellen.
- De kwalificaties en criteria zijn gebaseerd op twee artikelen uit de literatuur. Het nam veel tijd in beslag om kwalificaties en criteria te vinden in de literatuur.
+ Om literatuur te zoeken is gebruik gemaakt van de zoekmachines Google Scholar en de Open Universiteit bibliotheek. De zoeksystemen bleken erg gebruiksvriendelijk en het zoeken naar waardevolle artikelen werd hierbij eenvoudiger.
+ Door de stappen in literatuurstudie te volgen, werd er structuur aangebracht in het onderzoek.
+ De theorie uit de literatuur sloot goed aan op het onderzoek.

Empirisch onderzoek:

- Het onderzoek heeft plaatsgevonden bij één onderzoeksorganisatie vanwege de beperkte tijd die beschikbaar was. De generaliseerbaarheid van de resultaten werd hierdoor beperkt.
- Het onderzoek is uitgevoerd door één onderzoeker, wat onderzoekersbias tot gevolg kan hebben. Door de interviews op te nemen en letterlijk te transcriberen, komt de informatie letterlijk uit de bron. De eigen interpretatie van de onderzoeksgegevens blijft hierdoor buiten bereik. Onderzoekersbias wordt hierdoor verkleind.
- Er is één onderzoeksmethode gebruikt om gegevens te verzamelen, namelijk een casestudie. Door triangulatie toe te passen zou de betrouwbaarheid kunnen worden vergroot. De betrouwbaarheid is iets vergroot door een vragenlijst uit te sturen aan de experts om de organisatie nogmaals te beoordelen met de kennis die zij hebben opgedaan tijdens het interview.

+ De waarnemersbias is verkleind door de interviews te transcriberen en voor akkoord te laten tekenen door de experts. De uitspraken zijn hierbij letterlijk weergegeven in de uitwerking. Hiermee is ook de begripsvaliditeit gewaarborgd.
+ De inhoudsvaliditeit is gewaarborgd door tijdens het interview te vragen of de kwalificaties volledig, juist en duidelijk zijn. De antwoorden werden bevestigd met praktijkvoorbeelden.
+ Door het anonimiseren van de interviewresultaten, hadden de experts geen beperkingen om bepaalde zaken achter te houden, dat ten koste zou gaan voor het onderzoek.
+ De onderzoeksorganisatie was al bewust van DG, waardoor de begrippen en definities niet uitgelegd hoefden te worden. Door de kennis en expertise van de experts, konden makkelijk praktijkvoorbeelden worden gegeven om de scores van de volwassenheidsniveaus te onderbouwen.
+ Het onderzoek heeft nieuwe wetenschappelijke kennis opgeleverd over GRC binnen DG
+ Het DGGRCMM is een goed meetinstrument gebleken om de volwassenheid van DG binnen een organisatie in de praktijk te meten.

Uit bovenstaande punten kan geconcludeerd worden, dat het DGGRCMM een goed meetinstrument is gebleken om de volwassenheid van DG in de praktijk te beoordelen. Nieuwe kennis is opgedaan om verder onderzocht te worden. Door het onderzoek ook bij ander organisaties uit te voeren om de resultaten te bevestigen, zal de generaliseerbaarheid van het onderzoek worden vergroot.

Referenties

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems, 25*(sup1), 64-75.

Batenburg, R., Neppelenbroek, M., & Shahim, A. (2014). A maturity model for governance, risk management and compliance in hospitals. *J Hosp Adm, 3*, 43-52.

Becker, J., Knackstedt, R., & Pöppelbuβ, J. (2009). Developing Maturity Models for IT management - A Procedure Model and its Application. *BISE-Research Paper, 1*, 213-222. Retrieved from https://doi-org.exprozy.elib11ub.unimaas.nl/10.1007/s12599-009-0044-5

Bruin, T., & Rosemann, M. (2007). Using the Delphi technique to identify BPM capability areas. *Australian conference on information systems (ACIS), 18*.

Cheong, L. K., & Chang, V. (2007). The need for data governance: a case study. *ACIS 2007 Proceedings*, 100.

Gregory, A. (2011). Data governance - Protecting and unleashing the value of your customer data assets. *Journal of Direct, Data and Digital Marketing Practice, 12*, 230-248.

Khatri, & Brown. (2010). Designing Data Governance Communications of the ACM. *1*, 148-152.

Kooper, M., Maes, R., & Lindgreen E.E.O., R. (2011). On the governance of information: introducing a new concept of governance to support the management of information. *International Journal of Information Management, 31*, 195-200.

Merkus. (2015). *Data Governance Maturity Model.* Open Universiteit Nederland,

Merkus, Helms, R., & Kusters, R. (2019). Data governance and information governance: Set of definitions in relation to data and information as part of DIKW. *ICEIS2019*, 143-154.

Otto, B. (2011). *A morphology of the organisation of data governance.* Paper presented at the ECIS.

Pöppelbuß, J., & Röglinger, M. (2011). *What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management.* Paper presented at the Ecis.

Racz, N., Panitz, J. C., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (GRC) status quo and software use: results from a survey among large enterprises. *ACIS 2010 Proceedings, Paper, 21*.

Racz, N., Weippl, E., & Seufert, A. (2010). *A process model for integrated IT governance, risk, and compliance management.* Paper presented at the Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010).

Thornhill, A., Saunders, M., & Lewis, P. (2009). *Research methods for business students*: Prentice Hall: London.

van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., & Bekkers, W. (2010). *The Design of Focus Area Maturity Models*, Berlin, Heidelberg.

Vicente, P., & da Silva, M. M. (2011). *A conceptual model for integrated governance, risk and compliance.* Paper presented at the International Conference on Advanced Information Systems Engineering.

Wende, K. (2007). A model for data governance-Organising accountabilities for data quality management. *ACIS 2007 Proceedings*, 80.

Bijlage 1 Literatuuronderzoek

Tabel 1.1: Literatuuronderzoek zoekterm data governance

Zoekterm met data governance	Artikel
Data governance and designing	Otto, B. (2011). A morphology of the organisation of data governance. ECIS.
	Khatri, V. and Brown, C.V. (2010). "Designing Data Governance Communications of the ACM." **(53)1**: 148-152.
	Al-Ruithe, M., et al. (2016). "A Conceptual Framework for Designing Data Governance for Cloud Computing (MobiSPC 2016)." Conference Paper: 160-167.
Data governance a conceptual framework	Abraham, R., et al. (2019). "Data governance: A conceptual framework, structured review and research agenda." International Journal of Information Management **29**.
Data governance new concept of information	Kooper, M., et al. (2011). "On the governance of information: introducing a new concept of governance to support the management of information." International Journal of Information Management (31): 195-200.
Data governance and information governance Merkus	Merkus, J., Helms, R., & Kusters, R. (2019). Data governance and information governance: Set of definitions in relation to data and information as part of DIKW. *ICEIS2019*, 143-154.
Data governance grc	Gregory, A. (2011). Data governance - Protecting and unleashing the value of your customer data assets. *Journal of Direct, Data and Digital Marketing Practice, 12*, 230-248.
Data governance integrated grc	Racz, N., Panitz, J. C., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (GRC) status quo and software use: results from a survey among large enterprises. *ACIS 2010 Proceedings, Paper, 21*.

Tabel 1.2: Literatuuronderzoek zoekterm grc

Zoekterm met grc	Artikel
Grc governance risk and compliance	Vicente, P., & da Silva, M. M. (2011). *A conceptual model for integrated governance, risk and compliance.* Paper presented at the International Conference on Advanced Information Systems Engineering.
	Racz, N., et al. (2010). A process model for integrated IT governance, risk, and compliance management. Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), Citeseer.

Tabel 1.3: Literatuuronderzoek zoekterm maturity model

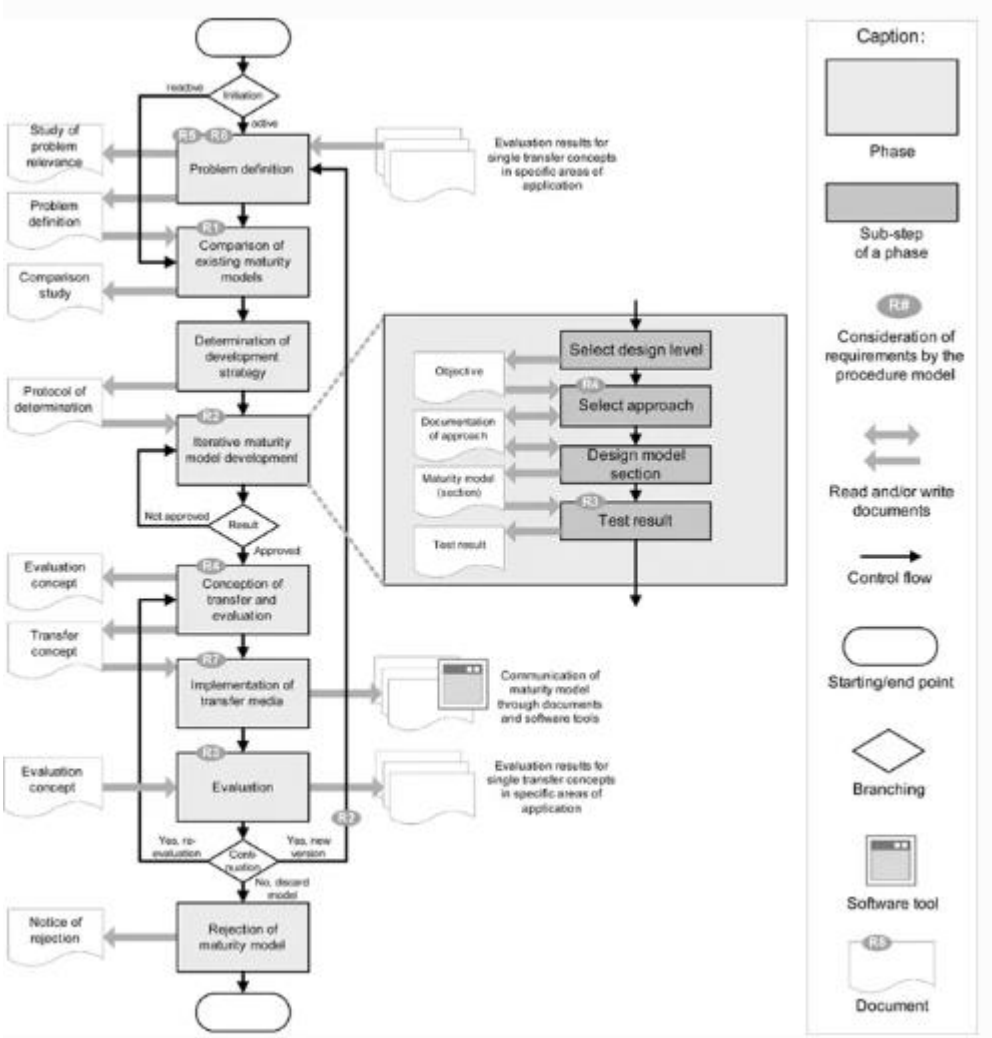
Zoekterm met maturity model	Artikel
Data governance maturity model	Merkus. (2015). *Data Governance Maturity Model.* Open Universiteit Nederland.
	Pöppelbuß, J., & Röglinger, M. (2011). *What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management.* Paper presented at the Ecis.
Maturity model grc	Batenburg, R., Neppelenbroek, M., & Shahim, A. (2014). A maturity model for governance, risk management and compliance in hospitals. *J Hosp Adm, 3*, 43-52.
Maturity models for it	Becker, J., et al. (2009). "Developing Maturity Models for IT Management - A Procedure Model and its Application." BISE - Research Paper **1**: 213-222
Focus area maturity models	van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., & Bekkers, W. (2010). *The Design of Focus Area Maturity Models*, Berlin, Heidelberg.

Tabel 1.4: Literatuuronderzoek onderzoeksmethoden

Onderzoeksmethoden	Artikel
Research methods	Thornhill, A., Saunders, M., & Lewis, P. (2009). *Research methods for business students*: Prentice Hall: London.

Bijlage 2 Ontwerp volwassenheidsmodellen

Becker et al. (2009) beschreef een procedure van een volwassenheidsmodel dat een reeks niveaus bevat die samen een geanticipeerd, gewenst of logisch pad vormen van een beginfase tot volwassenheid.



Figuur 2.1: Procedure model for developing models overgenomen uit "Developing Maturity models for IT Management - A Procedure Model and its Application" door Becker, J., Knackstedt, R. & Pöppelbuß, J., 2009, BISE - Research paper, 1, 213-222

Op basis van dit model zijn onderstaande stappen gehanteerd voor dit onderzoek:

1. Het zoeken naar de definities van DG en GRC
2. Het zoeken naar de definitie van een volwassenheidsmodel en zoeken welke modellen al bestaan
3. Het vinden van volwassenheidsniveaus die horen bij de definitie DG
4. Het zoeken naar dimensies op basis van bestaande GRC-modellen
5. Het verzamelen van criteria uit de literatuur
6. Het evalueren en analyseren van de criteria, zodat er een valide DGGRCMM ontstaat

De betekenis van de afkortingen in het model zijn gebruikt staan hieronder:

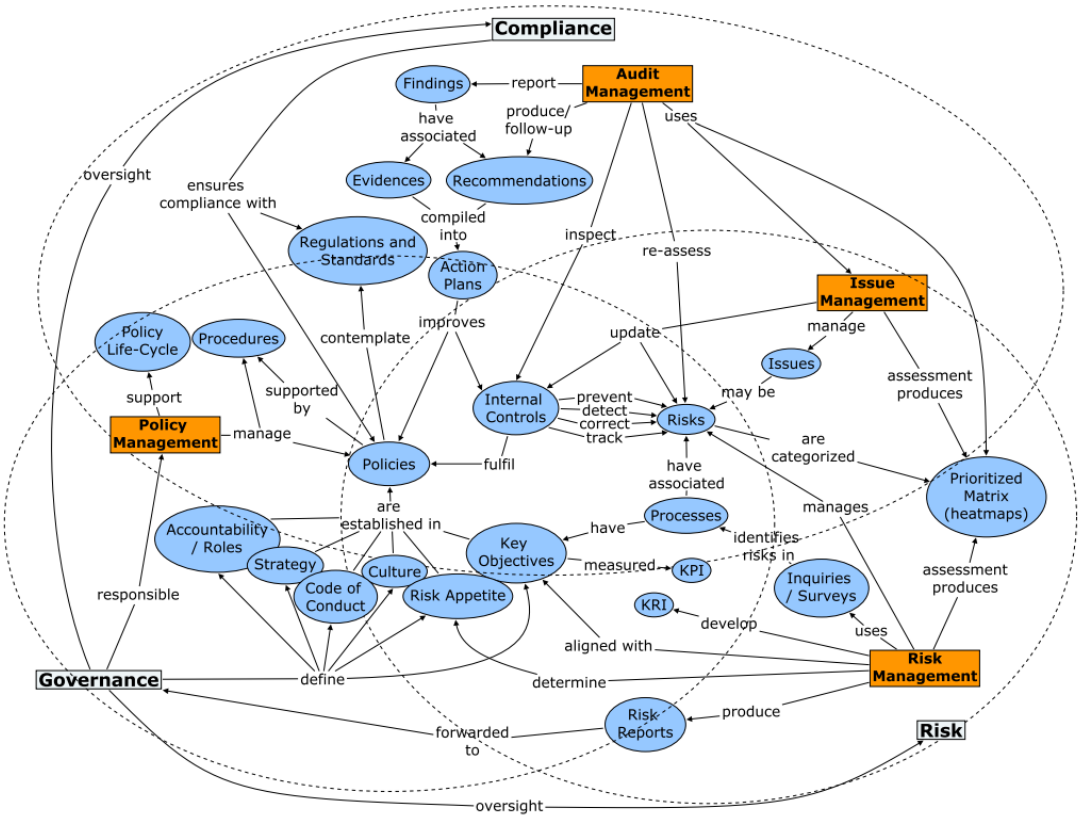
R1	Vergelijking met andere bestaande modellen.
R2	Stap voor stap een model ontwikkelen door levels, dimensies en kwalificaties te bepalen.
R3	Kwaliteit en effectiviteit van criteria moeten geëvalueerd worden en valide zijn.
R4	Het maturity modellen bevat verschillende onderzoeksmethoden: literatuurstudie/interviews.
R5	De relevantie van het probleem moet door de onderzoeker getoond worden.
R6	De definitie van het probleem moet beschreven zijn.
R7	Presentatie resultaat maturity model.

Een volwassenheidsmodel bestaat uit een raamwerk met volwassenheidlevels en dimensies, die zijn onderverdeeld in kwalificaties (Pöppelbuß & Röglinger, 2011). Het raamwerk betreft een algemeen ontwerp voor maturity modellen (Pöppelbuß & Röglinger, 2011).

Group		Design Principles
(1) BASIC	1.1	**Basic information** a) Application domain and prerequisites for applicability b) Purpose of use c) Target group d) Class of entities under investigation e) Differentiation from related maturity models f) Design process and extent of empirical validation
	1.2	**Definition of central constructs related to maturity and maturation** a) Maturity and dimensions of maturity b) Maturity levels and maturation paths c) Available levels of granularity of maturation d) Underpinning theoretical foundations with respect to evolution and change
	1.3	**Definition of central constructs related to the application domain**
	1.4	**Target group-oriented documentation**
(2) DESCRIPTIVE	2.1	**Intersubjectively verifiable criteria for each maturity level and level of granularity**
	2.2	**Target group-oriented assessment methodology** a) Procedure model b) Advice on the assessment of criteria c) Advice on the adaptation and configuration of criteria d) Expert knowledge from previous application
(3) PRESCRIPTIVE	3.1	**Improvement measures for each maturity level and level of granularity**
	3.2	**Decision calculus for selecting improvement measures** a) Explication of relevant objectives b) Explication of relevant factors of influence c) Distinction between an external reporting and an internal improvement perspective
	3.3	**Target group-oriented decision methodology** a) Procedure model b) Advice on the assessment of variables c) Advice on the concretization and adaption of the improvement measures d) Advice on the adaptation and configuration of the decision calculus e) Expert knowledge from previous application

Figuur 2.2: A framework of general design principles for maturity models overgenomen uit "What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management" door Pöppelbuß, J. Röglinger, M., 2011, Paper presented ad Ecis.

Vicente & da Silva (2011) hebben een geïntegreerd GRC conceptueel model ontwikkeld.



Figuur 2.3: Integrated GRC Conceptual Model overgenomen uit "A conceptual model for integrated governance, risk and compliance", door Vicente, P. & da Silva, M., 2011, Paper presented at the International Conference on Advanced Information Systems Engineering

Batenburg, Neppelenbroek & Shahim hebben het GRC maturity model ontwikkeld voor ziekenhuizen:

	Maturity model version 2	Level 1 Forming	Level 2 Developing	Level 3 Normalized	Level 4 Established	Level 5 Optimized
1	Governance: authority	Ad-hoc authority, actually professionals have the power.	Board is responsible without any power.	Board is responsible and has the power.	Board is responsible and has the power & prof. do not oppose.	Board & professionals share the power in a balanced way.
2	Governance: structure	There is no P&C (Planning & Control) in place.	P&C is ill structured and not documented.	P&C is structured and known by professionals.	P&C is implemented, most professionals contribute.	All professionals contribute proactively to an integrated P&C.
3	Governance: accountability	Professionals are not accountable to management.	Professionals view accountability as a bureaucratic process.	Each professional is accountable to management.	Each professional embraces his accountability.	Each professional is intrinsically motivated to be accountable.
4	Governance: control of professionals	No audit is performed on the professionals.	An internal audit is conducted based on quality indicators.	An external audit is conducted based on quality indicators.	An unexpected external audit is conducted.	There is a good balance between trust and control.
5	Governance: incident reporting	Incidents are reported on an ad-hoc basis.	A paper form is used to report incidents.	There is an easy (electronic) way to report incidents.	Professionals feel safe to report an incident.	Professionals trust the quality of the process of reporting incidents.
6	Risk management: authority	There is no CRO (Chief Risk Officer).	A CRO is appointed by the board.	The CRO reports directly to the board.	The CRO has authority to enact changes.	The board & CRO communicate ERM's importance.
7	Risk management: structure	No risk management framework is in place.		A risk management framework is used.		A risk management framework is fully impemented.
8	Risk management: analysis	No risk analysis is performed.	A decentralized risk analysis is performed.	A centralized risk analysis is performed.	Strategic risk analysis is performed.	Risk analysis is integrated in planning new developments
9	Risk management: scope	Risks are managed in a fragmented way.		Some types of risks are managed jointly.		Risks are managed in an integrated way.
10	Risk management: indicators	There are no risk indicators in place.	Indicators are used for internal regulations & policies.	Indicators are used for internal & external regulations & policies.	A risk management dashboard is used to monitor risks.	A system is in place to alert stakeholders about risks.
11	Compliance: authority	There is no CCO (Chief Compliance Officer).	A CCO is appointed by the board.	The CCO reports directly to the board.	The CCO has authority to enact changes.	The board & CRO & CCO work closely together.
12	Compliance: structure	No attempt to standardize similar processes.	Little attempt to standardize similar processes.	Similar processes are standardized across parts of the hospital.	Similar processes are evaluated across the hospital.	Similar processes are standardized across the hospital.
13	Compliance: controls	Rely on manual compliance processes & controls.	Manual & automated compliance processes & controls.	Tactical automated compliance processes & controls.	Strategic automated compliance processes & controls.	Flexible strategic automated compl. processes & controls.
14	Compliance: awareness	Hospital is indifferent to compliance .	Hospital is concerned about fixing noncompliance.	Hospital continuously monitors for compliance.	Hospital plans controls to sustain compliance.	Hospital incorporates compliance controls.

Figuur 2.4: The GRC maturity model for hospitals uit "A maturity model for governance, risk management and compliance hospitals" door Batenburg, R., Neppelenbroek, M., Shahim, A., 2014, J Hosp Adm, 3. 43-52

Bijlage 3 Totstandkoming DGGRCMM

Inleiding

In deze bijlage wordt de totstandkoming van het DGGRCMM beschreven. Het DGGRCMM bestaat uit onderstaande onderdelen:

- De dimensies die behoren bij de domeinen van GRC
- De levels om het DGGRCMM te beoordelen
- De kwalificaties die gevonden zijn bij de dimensies
- Levels bij de dimensies en kwalificaties bepalen
- Filteren van de kwalificaties
- Het conceptmodel

Hieronder wordt de uitwerking per onderdeel beschreven.

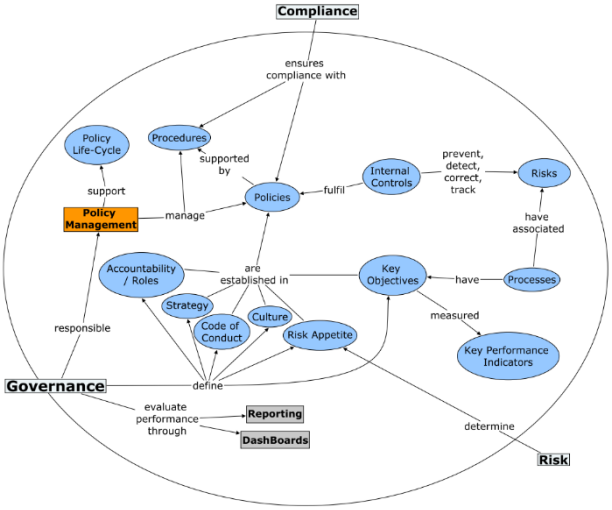
De dimensies die behoren bij de domeinen van GRC

De dimensies zijn tot stand gekomen door sleutelwoorden uit de definities van governance, riskmanagement en compliance en genoemde dimensies uit het literatuurartikel Conceptual Model for Governance. De bron van Vicente & da Silva (2011) is hiervoor toegepast. Ook is gekeken naar het bestaande GRC maturity model van Batenburg, Neppelenbroek & Shahim (2016).

De definities en figuren uit bron Vicente & da Silva (2011) staan hieronder vermeld.

Governance

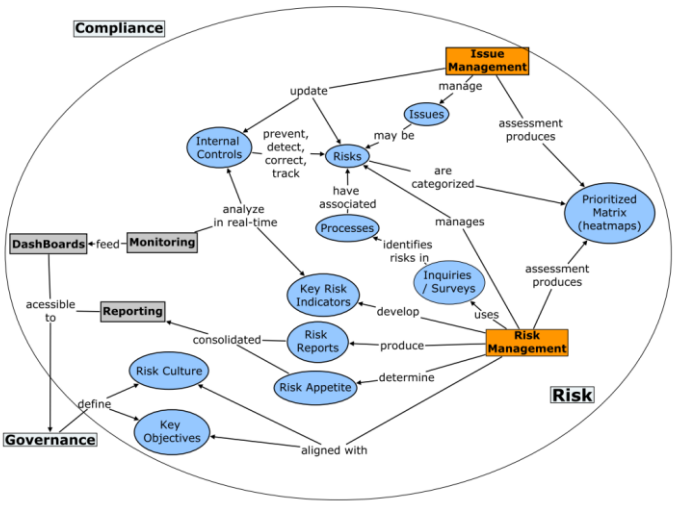
Het OCEG model stelt dat governance de cultuur, waarden, missie, structuur, beleidslagen, processen en maatregelen is waarmee organisaties bestuurd en gecontroleerd worden (Vicente & da Silva, 2011). Governance is verantwoordelijk voor het toezicht op risico's en naleving en voor het evalueren van prestaties ten opzichte van bedrijfsdoelstellingen (Vicente & da Silva, 2011).



Figuur 3.1: Conceptual Model for Governance overgenomen uit "A conceptual model for integrated governance, risk and compliance" door Vicente, P. & da Silva, M., 2011, Paper presented at the International Conference on Advanced Information Systems Engineering

Riskmanagement

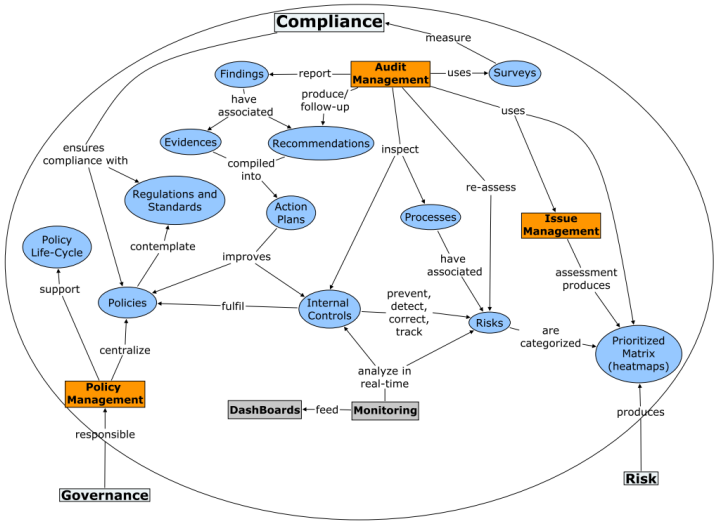
Volgens OCEG is risicobeheer “de systematische toepassing van processen en structuur die een organisatie in staat stellen risico’s te identificeren, evalueren, analyseren, optimaliseren, bewaken, verbeteren of overdragen, terwijl risico’s en risicobesluiten aan belanghebbenden worden meegedeeld (Vicente & da Silva, 2011). Een sterke risico managementstructuur kan zorgen voor een betere besluitvorming en strategiebepaling (Vicente & da Silva, 2011). Monitoring speelt een cruciale rol bij risk management, want het biedt de mogelijkheid om effectief en efficiënt potentiële risico’s en problemen te identificeren (Vicente & da Silva, 2011).



Figuur 3.2: Conceptual Model for Governance overgenomen uit "A conceptual model for integrated governance, risk and compliance" door Vicente, P. & da Silva, M., 2011, Paper presented at the International Conference on Advanced Information Systems Engineering

Compliance

Compliance moet ervoor zorgen dat de organisatie al haar verplichtingen nakomt en dus binnen de vastgestelde grenzen opereert (Vicente & da Silva, 2011). Volgens OCEG is “naleving” de handeling van het naleven van en het vermogen om naleving aan te tonen van verplichte vereisten die zijn vastgelegd in wet- en regelgeving, evenals alle vereisten die voortvloeien uit contractuele verplichtingen en intern beleid.



Figuur 3.3: Conceptual Model for Governance overgenomen uit "A conceptual model for integrated governance, risk and compliance" door Vicente, P. & da Silva, M., 2011, Paper presented at the International Conference on Advanced Information Systems Engineering

Het GRC maturity model van Batenburg, Neppelenbroek & Shahim staat al als figuur weergegeven in Bijlage 2.

In beide modellen en in de definities is gezocht naar dimensies. Hierbij is als uitgangspunt het GRC maturity model van Batenburg, Neppelenbroek & Shahim (2016) genomen, omdat dit het enige al bestaande GRC maturity model is in de literatuur. De dimensies die zijn gevonden uit beide bronnen, zijn in onderstaande tabel gezet:

Tabel 3.1: Gevonden dimensies uit bestaande modellen

Domeinen	Dimensies	Batenburg, Neppelenbroek & Shahim	Vicente & da Silva
Governance	**Gezag**	**X**	
	Besturing/beleid		**X**
	Verantwoordelijkheden	**X**	**X**
	Structuur	**X**	
	Strategie		X
	Cultuur		X
	Rapporteren		**X**
	Rapporteren incidenten	**X**	
	Missie		X
	Waarden		X
	Gedrag		X
	Procedures		X
	Controle professionals	X	
Riskmanagement	Structuur	X	X
	Beheersen risico's	**X**	**X**
	Analyseren	X	
	Indicators/monitoring	**X**	**X**

	Rapporteren		X
	Evalueren		X
Compliance	Gezag	X	
	Structuur	**X**	
	Controles	X	
	Interne controles		X
	Bewustzijn	**X**	
	Monitoring compliance		**X**
	Dashboards		X
	Naleven regels/beleid		**X**

Dimensies die in beide bronnen voorkwamen zijn gelijk beschouwd als valide (deze staan dik gedrukt in tabel 3.1). Van de 'overige' gevonden dimensies is geanalyseerd of er overeenkomsten waren en zijn samengevoegd tot een begrip in het overzicht van de definitieve dimensies die in onderstaande tabel zijn weergegeven. Achter elke dimensie is een omschrijving gezet met daarin de omschrijving van waarom deze dimensies bij de bijbehorende domeinen horen.

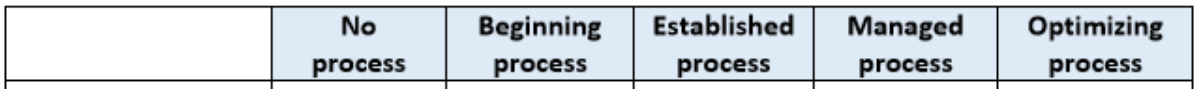
Tabel 3.2: Dimensies DGGRCMM

Domein	Dimensies	Omschrijving uit bron Vicente & da Silva (2011)
Governance	Gezag en verantwoordelijkheden	Governance is verantwoordelijk voor risico en compliance toezicht. Governance moet macht verdelen om inzicht en intelligentie te geven, zodat de juiste mensen in het management bewuste risico beslissingen te kunnen nemen om de bedrijfsdoelstellingen te halen.
	Structuur en beleid	Door mensen aan te stellen met kennis en over structuur en beleid, zullen de doelstellingen worden gehaald. Compliance zorgt voor de naleving ervan.
	Rapporteren	Door het rapporteren en analyseren van incidenten zorgt voor een effectief en efficiënt toezicht op de uitvoering van alle GRC-activiteiten
Riskmanagement	Monitoring	Door het monitoren van risico's kunnen risico's in kaart gebracht worden en aangegeven worden wat de status en impact is van de risico's. Het geeft vertrouwen in de organisatie en is goed voor het maken van governance- en bedrijfsbeslissingen. Door continue te monitoren en te controleren, wordt dat als bewijs gebruikt voor compliance.
	Beheersen risico's	Door het opsporen en beperken van risico's, wordt het gevaar van bedrijfsdoelstellingen behalen verminderd. Door regels op te stellen vanuit governance kan dit worden bereikt.
Compliance	Naleving beleid	Door interne controles te doen en het beleid te reviewen en te rapporteren zal het beleid verbeterd worden. Door het beleid te reviewen wordt de compliance verbeterd ten

		aanzien van externe voorschriften en standaarden die invloed hebben op het beleid.
	Bewustzijn	Door het bewustzijn in de organisatie te vergroten, door het geven van trainingen en self-assessments, is de organisatie bewust van compliance problemen.

De levels om het DGGRCMM te beoordelen

In het al bestaande data governance maturity model (DGMM) van Merkus (2015) staan de levels die gebruikt zijn voor zijn onderzoek.



Figuur 3.4: Levels DGMM

Hierbij is onderscheid gemaakt tussen een weinig (beginning process) of vergevorderde maturity level. De mate van gevorderdheid (established process) bepaalt hoe de gemiddelde maturity level is binnen een organisatie.
Deze levels worden op dezelfde wijze toegepast en getoetst om het DGGRCMM te beoordelen.
In tabel 3.3 staan de al bestaande levels uit het onderzoek van Merkus (2015) met daarbij de omschrijving per level.

Tabel 3.3: Levels met omschrijving uit DGMM

Level	Omschrijving
No process	Geen volwassenheid, ad hoc, weinig bewust
Beginning process	Weinig volwassenheid, bewust, in ontwikkeling
Established process	Mate gevorderd volwassenheid, ontwikkeld, proactief
Managed process	Volwassenheid bereikt, gevorderd, gemanaged, meer bewust
Optimizing process	Ultieme mate van volwassenheid, geoptimaliseerd, integratie, continue verbetering

De kwalificaties die gevonden zijn bij de dimensies

De dimensies die zijn gevonden bij de domeinen staan weergegeven in tabel 3.1. Alle dimensies zijn gevonden in de literatuur. De kwalificaties die bij de dimensies zijn gevonden, zijn uit dezelfde bronnen gehaald als de dimensies. De kwalificaties die bij de dimensies zijn gevonden, worden weergegeven in onderstaande tabel.

Tabel 3.4: Kwalificaties bij dimensies GRC

Dimensies	Kwalificaties	Bron
Gezag en verantwoordelijkheden	Gezag	Batenburg, Neppelenbroek & Shahim (2016)
Gezag en verantwoordelijkheden	Verantwoordelijkheden	Batenburg, Neppelenbroek & Shahim (2016)
Gezag en verantwoordelijkheden	Gedrag	Vicente & da Silva (2011)
Structuur en beleid	Besturing	Vicente & da Silva (2011)
Structuur en beleid	Beleid	Vicente & da Silva (2011)
Structuur en beleid	Structuur	Batenburg, Neppelenbroek & Shahim (2016)
Structuur en beleid	Cultuur	Vicente & da Silva (2011)

Structuur en beleid	Missie	Vicente & da Silva (2011)
Structuur en beleid	Waarden	Vicente & da Silva (2011)
Structuur en beleid	Procedures	Vicente & da Silva (2011)
Structuur en beleid	Controle professionals	Batenburg, Neppelenbroek & Shahim (2016)
Rapporteren	Rapporteren	Batenburg, Neppelenbroek & Shahim (2016)
Rapporteren	Rapporteren incidenten	Vicente & da Silva (2011)
Rapporteren	Analyse	Vincente & da Silva (2011)
Monitoring	Indicators	Batenburg, Neppelenbroek & Shahim (2016)
Monitoring	Monitoring	Vicente & da Silva (2011)
Monitoring	Rapporteren	Vicente & da Silva (2011)
Monitoring	Structuur	Vicente & da Silva (2011) en Batenburg, Neppelenbroek & Shahim (2016)
Beheersen risico's	Structuur	Batenburg, Neppelenbroek & Shahim (2016)
Beheersen risico's	Beheersen risico's	Batenburg, Neppelenbroek & Shahim (2016)
Beheersen risico's	Analyseren	Batenburg, Neppelenbroek & Shahim (2016)
Beheersen risico's	Evalueren	Vicente & da Silva (2011)
Naleving beleid	Gezag	Batenburg, Neppelenbroek & Shahim (2016)
Naleving beleid	Structuur	Batenburg, Neppelenbroek & Shahim (2016)
Naleving beleid	Controles	Batenburg, Neppelenbroek & Shahim (2016)
Naleving beleid	Interne controles	Vicente & da Silva (2011)
Bewustzijn	Bewustzijn	Batenburg, Neppelenbroek & Shahim (2016)
Naleving beleid	Monitoring compliance	Vicente & da Silva (2011)
Naleving beleid	Dashboards	Vicente & da Silva (2011)
Naleving beleid	Naleven regels/beleid	Vicente & da Silva (2011)

Levels bij de dimensies en kwalificaties bepalen

Per kwalificatie zijn de levels opgenomen zoals in het DGMM van Merkus (2015) is weergegeven. Per kwalificatie is per level bepaalt welke eisen er aan dat level worden gesteld.

DGGRCMM V0.1

Domeinen	Dimensies	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process
Governance	Gezag en Verantwoordelijkheden	Gezag	Ad-hoc gezag, eigenlijk hebben professionals macht	Bestuur is verantwoordelijk zonder macht	Bestuur is verantwoordelijk en heeft macht	Bestuur is verantwoordelijk en heeft macht & professionals verzetten zich niet	Bestuur en professionals delen macht op gebalanceerde wijze
		Verantwoording	Professionals zijn geen verantwoording verschuldigd aan het management	Professionals zien verantwoordelijkheid als bureaucratisch proces	Elke professional legt verantwoording af aan management	Elke professional omarmt zijn verantwoordelijkheid	Elke professional is intensief gemotiveerd om verantwoording te hebben
		Gedrag	no process	beginning process	established process	managed process	optimizing process
	Structuur en Beleid	Structuur	Er is geen DG expert aanwezig	DG expert wordt voorgesteld aan het bestuur	DG expert rapporteert direct aan het bestuur	DG expert heeft verantwoordelijkheid om veranderingen door te voeren	DG expert en het bestuur hebben volledige verantwoordelijkheid om veranderingen door te voeren
		Regels\procedures	Er zijn geen regels aanwezig m.b.t het DG beleid	De regels voor het DG beleid zijn slecht gestructureerd & niet gedocumenteerd	De regels voor het DG beleid zijn gestructureerd en bekend bij professionals	De regels voor het DG beleid zijn geïmplementeerd, de meeste professionals werken ermee	Alle professionals houden zich aan geïntegreerde regels
		Controle professionals	Er wordt geen audit uitgevoerd bij de professionals	Er wordt een interne audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een externe audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een onverwachte externe audit uitgevoerd	Er is een goede balans tussen vertrouwen en controle
		Besturing	no process	beginning process	established process	managed process	optimizing process
		Cultuur	no process	beginning process	established process	managed process	optimizing process
		Missie	no process	beginning process	established process	managed process	optimizing process
		Waarden	no process	beginning process	established process	managed process	optimizing process
	Rapporteren	Resultaten-analyse	Er is geen proces resultaten-analyse aanwezig	Er wordt een papieren formulier gebruikt om resultaten te analyseren	Er is een makkelijke manier om resultaten te analyseren aanwezig	Professionals voelen zich veilig om resultaten te analyseren	Professionals vertrouwen de kwaliteit van het proces van resultaten analyseren
		Rapporteren incidenten	Incidenten worden op ad-hoc basis gerapporteerd	Er wordt een papieren formulier gebruikt om incidenten te rapporteren	Er is een makkelijke (elektronische) manier om incidenten te rapporteren	Professionals voelen zich veilig om incidenten te rapporteren	Professionals vertrouwen de kwaliteit van het proces van incidenten rapporteren
		Rapporteren	Er wordt op ad-hoc basis gerapporteerd	Er wordt een papieren formulier gebruikt om te rapporteren	Er is een makkelijke (elektronische) manier om te rapporteren	Professionals voelen zich veilig om te rapporteren	Professionals vertrouwen de kwaliteit van het proces van rapporteren

Riskmanagement	Monitoring	Structuur	Er is geen RM raamwerk aanwezig		Er wordt een RM raamwerk gebruikt		Een RM raamwerk is volledig geimplementeerd
		Indicators	Er zijn geen risico indicatoren aanwezig	Indicatoren worden gebruikt voor interne regelgeving en beleid	Indicatoren worden gebruikt voor interne en extern regelgeveing en beleid	Een RM dashboard is in gebruik om risico's te monitoren	Er is een systeem aanwezig om stakeholders te informeren over risico's
		Monitoring	Er is geen monitoring aanwezig	Er wordt weinig gemonitoord voor interne regelgeving en beleid	Er wordt gemonitoord voor interne regelgeving en beleid	Een RM dashboard is in gebruik om risico's te monitoren	Er is een systeem aanwezig om stakeholders te informeren over risico's
		Rapporteren	Er wordt op ad-hoc basis gerapporteerd	Er wordt een papieren formulier gebruikt om te rapporteren	Er is een makkelijke (elektronische) manier om te rapporteren	Professionals voelen zich veilig om te rapporteren	Professionals vertrouwen de kwaliteit van het proces van rapporteren
	Beheersen risico's	Risico-analyse	Er wordt geen risico-analyse uitgevoerd.	Er is een gedecentraliseerde risico analyse uitgevoerd	Er is een gecentraliseerd risico analyse uitgevoerd	Er is een strategische risico analyse uitgevoerd	Risico-analyse is geimplementeerd in de planning van nieuwe ontwikkelingen
		Beheersing risico's	Risico's worden deels beheerst		Sommige typen risico's worden gezamenlijk beheerst		Risico's worden beheerst op geintegreerde wijze
		Evalueren	Eer wordt geen risico-evaluatie uitgevoerd.	Er is een gedecentraliseerde risico evaluatie uitgevoerd	Er is een gecentraliseerd risico evaluatie uitgevoerd	Er is een strategische risico evaluatie uitgevoerd	Risico-evaluatie is geimplementeerd in de planning van nieuwe ontwikkelingen
Compliance	Naleving beleid	Structuur	Er wordt geen poging gedaan om dezelfde processen te standaardiseren	Er wordt een kleine poging gedaan om dezelfde processen te standaardiseren	Dezelfde processen zijn gestandaardiseerd over delen van de organisatie	Dezelfde processen zijn geëvalueerd over delen van de organisatie	Dezelfde processen zijn gestandaardiseerd binnen de organisatie
		Regels naleven	Er wordt geen poging gedaan om de regels op te stellen en na te leven	Er wordt een kleine poging gedaan om regels op te stellen en na te leven	Er is een makkelijke manier om regels op papier te zetten en na te leven	Professionals voelen zich veilig om de regels op te stellen en na te leven	Profesionals hebben vertrouwen in de kwaliteit van het proces regels opstellen en naleven
		Controles	Er is vertrouwen in een handleiding compliance processen & controles	Handleidng & geautomatiseerde compliance processen & controles	Tactisch geautomatiseerde compliance processen & controles	Strategisch geautomatiseerde compliance processen & controles	Flexibele strategisch geautomatiseerd compliance processen & controles
		Gezag	Ad-hoc gezag, eigenlijk hebben professionals macht	Bestuur is verantwoordelijk zonder macht	Bestuur is verantwoordelijk en heeft macht	Bestuur is verantwoordelijk en heeft macht & professionals verzetten zich niet	Bestuur en professionals delen macht op gebalanceerde wijze
		Beleid	Er wordt geen poging gedaan om de regels op te stellen en na te leven	Er wordt een kleine poging gedaan om regels op te stellen en na te leven	Er is een makkelijke manier om regels op papier te zetten en na te leven	Professionals voelen zich veilig om de regels op te stellen en na te leven	Profesionals hebben vertrouwen in de kwaliteit van het proces regels opstellen en naleven
		Monitoring	Er is geen monitoring aanwezig	Er wordt weinig gemonitoord voor interne regelgeving en beleid	Er wordt gemonitoord voor interne regelgeving en beleid	Een dashboard is in gebruik om beleid te monitoren	Er is een systeem aanwezig om stakeholders te informeren
		Dashboards	Er is geen monitoring aanwezig	Er wordt weinig gemonitoord voor interne regelgeving en beleid	Er wordt gemonitoord voor interne regelgeving en beleid	Een dashboard is in gebruik om beleid te monitoren	Er is een systeem aanwezig om stakeholders te informeren
	Bewustzijn	Bewust zijn van compliance	De organisatie is onverschillig tegenover compliance	De organisatie maakt zich zorgen over het vaststellen van non-compliance	De organisatie monitoort continue op compliance	De organisatie plant controles in om compliance te ondersteunen	De organisatie neemt compliance controles op in de organisatie

Figuur 3.5: Levels en kwalificaties in DGGRCMM

Filteren van de kwalificaties

Bij het filteren van de kwalificaties is per kwalificatie een analyse gedaan. Er is bepaald of de kwalificatie in het DGGRCMM wordt opgenomen of niet. Als de kwalificatie niet wordt opgenomen in het DGGRCMM, is er een onderbouwing neergezet waarom deze niet in het model wordt opgenomen.

Tabel 3.5: Filteren kwalificaties

Dimensies	Kwalificaties	Analyse wel of niet in het DGGRCMM
Gezag en verantwoordelijkheden	Gezag	Wel in DGGRCMM
Gezag en verantwoordelijkheden	Verantwoordelijkheden	Wel in DGGRCMM
Gezag en verantwoordelijkheden	Gedrag	Niet in DGGRCMM– valt onder richtlijnen
Structuur en beleid	Besturing	Niet in DGGRCMM – samengevoegd met gezag
Structuur en beleid	Beleid	Wel in DGGRCMM
Structuur en beleid	Structuur	Wel in DGGRCMM
Structuur en beleid	Cultuur	Niet in DGGRCMM – valt onder structuur
Structuur en beleid	Missie	Niet in DGGRCMM– valt onder richtlijnen
Structuur en beleid	Waarden	Niet in DGGRCMM– valt onder richtlijnen
Structuur en beleid	Procedures	Wel in DGGRCMM– valt onder regels in structuur en beleid

Structuur en beleid	Controle professionals	Wel in DGGRCMM – verplaatst naar naleving en beleid
Rapporteren	Rapporteren	Wel in DGGRCMM
Rapporteren	Rapporteren incidenten	Wel in DGGRCMM – valt onder rapporteren
Rapporteren	Analyse	Wel in DGGRCMM
Monitoring	Indicators	Wel in DGGRCMM – kan gezien worden als middelen om te monitoren
Monitoring	Monitoring	Wel in DGGRCMM
Monitoring	Rapporteren	Niet in DGGRCMM – kan gezien worden als monitoring/indicators om te rapporteren
Monitoring	Structuur	Wel in DGGRCMM
Beheersen risico's	Structuur	Wel in DGGRCMM – samengevoegd met structuur onder monitoring
Beheersen risico's	Beheersen risico's	Wel in DGGRCMM
Beheersen risico's	Analyseren	Wel in DGGRCMM
Beheersen risico's	Evalueren	Niet in DGGRCMM – valt onder analyseren
Naleving beleid	Gezag	Wel in DGGRCMM – verplaatst naar Gezag en verantwoordelijkheden
Naleving beleid	Structuur	Wel in DGGRCMM
Naleving beleid	Controles	Wel in DGGRCMM
Naleving beleid	Interne controles	Niet in DGGRCMM – samengevoegd met controles
Bewustzijn	Bewustzijn	Wel in DGGRCMM
Naleving beleid	Monitoring compliance	Wel in DGGRCMM – verplaatst naar monitoring
Naleving beleid	Dashboards	Wel in DGGRCMM – valt onder indicators en monitoring – verplaatst naar monitoring
Naleving beleid	Naleven regels/beleid	Wel in DGGRCMM

Dit heeft als resultaat het DGGRCMM V1.0 opgeleverd:

DGGRCMM V0.1							
Domeinen	Dimensies	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process
Governance	Gezag en Verantwoordelijkheid	Gezag	Ad-hoc gezag, eigenlijk hebben professionals macht	Bestuur is verantwoordelijk zonder macht	Bestuur is verantwoordelijk en heeft macht	Bestuur is verantwoordelijk en heeft macht & professionals verzetten zich niet	Bestuur en professionals delen macht op gebalanceerde wijze
		Verantwoordelijkheden	Professionals zijn geen verantwoording verschuldigd aan het management	Professionals zien verantwoordelijkheid als bureaucratisch proces	Elke professional legt verantwoording af aan management	Elke professional omarmt zijn verantwoordelijkheid	Elke professional is intensief gemotiveerd om verantwoording te hebben
	Structuur en Beleid	Structuur	Er is geen DG expert aanwezig	DG expert wordt voorgesteld aan het bestuur	DG expert rapporteert direct aan het bestuur	DG expert heeft verantwoordelijkheid om veranderingen door te voeren	DG expert en het bestuur hebben volledige verantwoordelijkheid om veranderingen door te voeren
		Regels\procedures	Er zijn geen regels aanwezig m.b.t het DG beleid	De regels voor het DG beleid zijn slecht gestructureerd & niet gedocumenteerd	De regels voor het DG beleid zijn gestructureerd en bekend bij professionals	De regels voor het DG beleid zijn geimplementeerd, de meeste professionals werken ermee	Alle professionals houden zich aan geintegreerde regels
		Controle professionals	Er wordt geen audit uitgevoerd bij de professionals	Er wordt een interne audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een externe audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een onverwachte externe audit uitgevoerd	Er is een goede balans tussen vertrouwen en controle
	Rapporteren	Resultaten analyse	Er is geen proces resultaten-analyse/rapporteren aanwezig	Er wordt een papieren formulier gebruikt om resultaten te analyseren/rapporteren	Er is een makkelijke manier om resultaten te analyseren/rapporteren aanwezig	Professionals voelen zich veilig om resultaten te analyseren/rapporteren	Professionals vertrouwen de kwaliteit van het proces van resultaten analyseren/rapporteren
		Rapporteren incidenten	Incidenten worden op ad-hoc basis gerapporteerd	Er wordt een papieren formulier gebruikt om incidenten te rapporteren	Er is een makkelijke (elektronische) manier om incidenten te rapporteren	Professionals voelen zich veilig om incidenten te rapporteren	Professionals vertrouwen de kwaliteit van het proces van incidenten rapporteren
Riskmanagement	Monitoring	Structuur	Er is geen RM raamwerk aanwezig		Er wordt een RM raamwerk gebruikt		Een RM raamwerk is volledig geimplementeerd
		Indicatoren en monitoring	Er zijn geen risico indicatoren aanwezig	Indicatoren worden gebruikt voor interne regelgeving en beleid	Indicatoren worden gebruikt voor interne en extern regelgeveing en beleid	Een RM dashboard is in gebruik om risico's te monitoren	Er is een systeem aanwezig om stakeholders te informeren over risico's
	Beheersen risico's	Risico-analyse	Er wordt geen risico-analyse uitgevoerd.	Er is een gedecentraliseerde risico analyse uitgevoerd	Er is een gecentraliseerd risico analyse uitgevoerd	Er is een strategische risico analyse uitgevoerd	Risico-analyse is geimplementeerd in de planning van nieuwe ontwikkelingen
		Beheersing risico's	Risico's worden deels beheerst		Sommige typen risico's worden gezamenlijk beheerst		Risico's worden beheerst op geintegreerde wijze
Compliance	Naleving beleid	Structuur	Er wordt geen poging gedaan om dezelfde processen te standaardiseren	Er wordt een kleine poging gedaan om dezelfde processen te standaardiseren	Dezelfde processen zijn gestandaardiseerd over delen van de organisatie	Dezelfde processen zijn geëvalueerd over delen van de organisatie	Dezelfde processen zijn gestandaardiseerd binnen de organisatie
		Regels naleven	Er wordt geen poging gedaan om de regels op te stellen en na te leven	Er wordt een kleine poging gedaan om regels op te stellen en na te leven	Er is een makkelijke manier om regels op papier te zetten en na te leven	Professionals voelen zich veilig om de regels op te stellen en na te leven	Profesionals hebben vertrouwen in de kwaliteit van het proces regels opstellen en naleven
		Controles	Er is vertrouwen in een handleiding compliance processen & controles	Handleidng & geautomatiseerde compliance processen & controles	Tactisch geautomatiseerde compliance processen & controles	Strategisch geautomatiseerde compliance processen & controles	Flexibele strategisch geautomatiseerd compliance processen & controles
	Bewustzijn	Bewust zijn van compliance	De organisatie is onverschillig tegenover compliance	De organisatie maakt zich zorgen over het vaststellen van non-compliance	De organisatie monitoort continue op compliance	De organisatie plant controles in om compliance te ondersteunen	De organisatie neemt compliance controles op in de organisatie

Figuur 3.6: DGGRCMM V0.1

Bijlage 4 Interviewprotocol

In deze bijlage wordt het interviewprotocol beschreven. Het interviewprotocol bestaat uit onderstaande onderdelen:

- Interview
- Informatieblad
- Toestemmingsformulier
- Interviewformulier
- Survey

Interview

Voorbereiding op het interview

- De onderzoeker nodigt iedere expert uit voor een interview
- Iedere expert ontvangt per email een informatieblad waarin hij/zij wordt geïnformeerd over de inhoud van het onderzoek
- Iedere expert ontvangt een toestemmingsformulier, die getekend moet worden voordat het interview begint
- De onderzoeker geeft aan dat de gegevens van de expert en de organisatie anoniem blijven

Vooraf aan het interview

- De onderzoeker is op tijd aanwezig en goed voorbereid
- De onderzoeker stelt zich voor en bedankt de expert voor haar medewerking aan het onderzoek
- De onderzoeker licht het informatieblad toe
- De onderzoeker neemt het getekende toestemmingsformulier in ontvangst
- De onderzoeker vraagt of het interview mag worden opgenomen
- De onderzoeker deelt de expert mede dat hij/zij binnen een week een samenvatting van het interview ontvangt met de vraag om deze te controleren en feedback hierop wil geven

Interview

- De opname wordt gestart
- Het informatieblad zal de rode draad zijn tijdens het interview
- De onderzoeker vraagt aan de expert om een score te geven aan de hand van het DGGRCMM, gebaseerd op de eigen organisatie
- Elke kwalificatie en criteria komen aan bod
- Bij elke kwalificatie en criteria wordt gevraagd om voorbeelden of argumenten te geven, waarbij duidelijk aangegeven wordt welk level goed is binnen de organisatie en welke niet

Afsluiting

- De opname wordt gestopt
- De expert wordt bedankt voor het afnemen van het interview
- De onderzoeker benadrukt nogmaals dat de expert binnen een week een samenvatting ontvangt met de vraag om deze te controleren en feedback hierop wil geven
- De expert ontvangt na het interview ook een online vragenlijst, waarin nogmaals gevraagd wordt om de organisatie te beoordelen aan de hand van het DGGRCMM, nu er meer kennis vergaard is om de eigen organisatie te beoordelen

Duur van interview

De duur van het interview zal liggen tussen de 60 en 90 minuten. Dit is voldoende tijd om het model volledig door te nemen en er wordt niet te veel tijd van de expert gevraagd. Mocht er meer tijd nodig zijn, dan wordt de expert gevraagd om meer tijd of de vragen per mail te beantwoorden.

Expert

Voor het interview zijn vier experts gevraagd binnen dezelfde organisatie met kennis over governance, risk management & compliance binnen data governance. De experts zijn geselecteerd op hun kennis en expertise. Er is ook gekeken naar het aantal jaar dat zij op dit gebied werkzaam zijn, zodat zij een grote bijdrage kunnen leveren aan dit onderzoek.

Informatieblad
Governance, Risk management & Compliance model

Inleiding
Data speelt een grote rol binnen organisaties. Data met grotere volumes, wordt verzameld, vastgelegd en beschikbaar gesteld in systemen om doelstellingen te kunnen behalen. Het is hierbij van belang dat data betrouwbaar, compleet, juist en volledig is om hiermee de kwaliteit van data te kunnen verbeteren. Data governance (DG) helpt om de waarde van data te waarborgen en om datakwaliteit te verbeteren en te onderhouden. GRC-activiteiten zijn belangrijk in organisaties om hun prestaties te verbeteren en om organisaties van binnen en van buiten te beschermen.

Relevantie
De afgelopen jaren is er wetenschappelijk literatuuronderzoek gedaan naar DG, omdat het belang van DG erg belangrijk is bij het besturen van de organisatie. Door het groot aantal volume aan data is datakwaliteit nog belangrijker geworden. Om datakwaliteit te beheersen is DG nodig om goed om te kunnen gaan met data. Hiermee verandert de organisatievolwassenheid. GRC maakt onderdeel uit van DG. Als GRC en DG worden samengevoegd, wordt waarde aan de organisatievolwassenheid toegevoegd en de risico's voor de organisaties worden gereduceerd.

Uitleg model
Uit wetenschappelijk literatuuronderzoek zijn onderstaande definities gehaald:
Data governance: Data governance is het oprichten van beheer van gegevens in een organisatie om kwaliteit en toegang tijdens haar levenscyclus te garanderen om verantwoording af te leggen voor haar data assets.

GRC: GRC is een geïntegreerde, holistische benadering van organisatie brede governance, risico en compliance die ervoor zorgt dat een organisatie ethisch correct en in overeenstemming met haar risicobereidheid, intern beleid en externe regelgeving handelt door de afstemming van strategie, processen, technologie en mensen, waardoor de efficiëntie en effectiviteit worden verbeterd.

Maturity model: Een volwassenheidsmodel bevat een reeks niveaus die samen een geanticipeerd, gewenst of logisch pad vormen van een beginfase tot volwassenheid. Een volwassenheidsmodel bestaat uit een raamwerk met volwassenheidslevels en -dimensies, die onderverdeeld zijn in kwalificaties.

DGGRCMM
Op basis van wetenschappelijke literatuur is onderstaand DGGRCMM V0.1 ontwikkeld.

DGGRCMM V0.1						
Dimensies	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process
Governance	Gezag en Verantwoordelijkheden					
	Structuur en Beleid					
	Rapporteren					
Riskmanagement	Monitoring					
	Beheersen risico's					
Compliance	Naleving beleid					
	Bewustzijn					

Figuur 4.1: DGGRCMM V0.1

Toestemmingsformulier

Onderzoek (DGGRCMM) : Data Governance: Governance, Risk management & Compliance model
Onderzoeker : Petra Kroos-Kerpershoek
Opleiding : Business Process Management & IT, Open Universiteit Nederland

		Zet a.u.b. uw paraaf in het vakje Ja	Nee
1.	Ik bevestig hierbij, dat ik het informatieblad voor het onderzoek heb gelezen, begrepen en de gelegenheid heb gehad om vragen te stellen.	☐	☐
2.	Ik begrijp dat mijn deelname aan dit onderzoek vrijwillig is en dat ik op elk moment mijn deelname kan beëindigen, zonder hiervoor een reden op te geven.	☐	☐
3.	Ik ben mij ervan bewust, dat alles in het werk gesteld zal worden om de vertrouwelijkheid van de informatie te waarborgen.	☐	☐
4.	Ik begrijp dat alle informatie die ik geef als anoniem worden verwerkt.	☐	☐
5.	Ik verklaar hierbij dat ik toestemming geef om het interview op te laten nemen.	☐	☐

<u>Expert</u>
Naam :
Datum :
Handtekening :

<u>Onderzoeker</u>
Naam :
Datum :
Handtekening :

Interviewformulier

Om de hoofdvraag te kunnen beantwoorden zijn twee empirische deelvragen opgesteld.

- Hoe kan de volwassenheid van het DGGRCMM voor DG worden gemeten?
- Wat zijn relevante aanvullingen voor het DGGRCMM ten aanzien van DG?

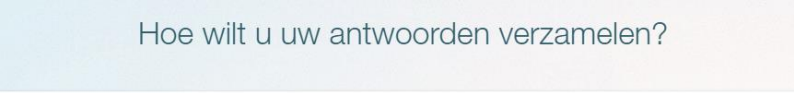
Om deze empirische deelvragen te kunnen beantwoorden, wordt aan drie experts gevraagd om het DGGRCMM V0.1 binnen de eigen organisatie te beoordelen met betrekking tot GRC als onderdeel van DG. Voor alle elementen van GRC worden onderstaande vragen gesteld.

- Hoort deze dimensie thuis in het DGGRCMM? Waarom?
- Zijn de kwalificaties in staat om de dimensie te meten in het DGGRCMM? Waarom?
- Geven de kwalificaties van DG een volledig beeld van alle aspecten van het onderwerp? Waarom?
- Zorgen de kwalificaties in het DGGRCMM ervoor om te kunnen groeien binnen de organisatie? Waarom?

Bij de alle vragen wordt de waaromvraag gesteld om zo tot voorbeelden en argumenten te komen.

Online vragenlijst

De online vragenlijst wordt gebruikt bij het onderzoek om de experts te vragen, met de opgedane kennis, de organisatie nogmaals te beoordelen. De vragenlijst wordt gebruikt als extra onderbouwing op de resultaten uit het interview. Met onderstaande link krijgen de experts toegang tot de vragenlijst.



3. Governance - Kwalificatie Structuur*

Selecteer één of meer antwoorden

- Er is geen data governance expert aanwezig
- De data governance expert wordt voorgesteld aan het bestuur
- De data governance expert rapporteert direct aan het bestuur
- De data governance expert heeft verantwoordelijkheid om veranderingen door te voeren
- De data governance expert en het bestuur hebben volledige verantwoordelijkheid om veranderingen door te voeren
- De Governance - Kwalificatie Structuur is niet relevant

Zijn de antwoorden op Governance - Kwalificatie Structuur compleet en relevant? Waarom?

4. Governance - Kwalificatie Regels*

Selecteer één of meer antwoorden

- Er zijn geen regels aanwezig met betrekking tot het data governance beleid
- De regels voor het data governance beleid zijn slecht gestructureerd & niet gedocumenteerd
- De regels voor het data governance beleid zijn gestructureerd en bekend bij professionals
- De regels voor het data governance beleid zijn geïmplementeerd en de meeste professionals werken ermee
- Alle professinals houden zich aan de geïmplementeerde regels en werken ermee
- De Governance - Kwalificatie Regels is niet relevant

Zijn de antwoorden op Governance - Kwalificatie Regels compleet en relevant? Waarom?

5. Governance - Kwalificatie Controle professionals*

Selecteer één of meer antwoorden

- Er wordt geen audit uitgevoerd bij professionals
- Er wordt een interne audit uitgevoerd op basis van kwaliteitsindicatoren
- Er wordt een externe audit uitgevoerd op basis van kwaliteitsindicatoren
- Er wordt een onverwachte externe audit uitgevoerd
- Er is een goed balans tussen vertrouwen en controle
- De Governance - Kwalificatie controle professionals is niet relevant

Zijn de antwoorden op Governance - Kwalificatie Controle professionals compleet en relevant? Waarom?

6. Governance - Kwalificatie Resultaten-analyse*

Selecteer één of meer antwoorden

- Er is geen proces resultaten-analyse aanwezig
- Er wordt een papieren formulier gebruikt om resultaten te analyseren
- Er is een makkelijke manier om resultaten te analyseren aanwezig
- Professionals voelen zich veilig om resultaten te analyseren
- Professionals vertrouwen de kwaliteit van het proces van resultaten analyseren
- De Governance - Kwalificatie Resultaten-analyse is niet relevant

Zijn de antwoorden op Governance - Kwalificatie Resultaten-analyse compleet en relevant? Waarom?

7. Governance - Kwalificatie Rapporteren incidenten*

Selecteer één of meer antwoorden

- Incidenten worden op ad-hoc basis gerapporteerd
- Er wordt een papieren formulier gebruikt om incidenten te rapporteren
- Er is een makkelijke (elektronische) manier om incidenten te rapporteren
- Professionals voelen zich veilig om incidenten te rapporteren
- Professionals vertrouwen de kwaliteit van het proces van incidenten rapporteren
- De Governance - Kwalificatie Rapporteren incidenten is niet relevant

Zijn de antwoorden op de Governance - Kwalificatie Rapporteren incidenten compleet en relevant? Waarom?

8. Risk management - Kwalificatie raamwerk risk management*

Selecteer één of meer antwoorden

- Er is geen risk management raamwerk aanwezig
- Er wordt een risk management raamwerk gebruikt
- Een risk management raamwerk is volledig geïmplementeerd
- De Risk management - Kwalificatie raamwerk risk management is niet relevant

Zijn de antwooorden op Risk management - Kwalificatie Raamwerk risk management compleet en relevant? Waarom?

9. Risk management - Kwalificatie Indicatoren*

- Er zijn geen risico indicatoren aanwezig
- Indicatoren worden gebruikt voor interne regelgeving en beleid
- Indicatoren worden gebruikt voor interne en externe regelgeving en beleid
- Er wordt een risk management dashboard gebruikt om risico's te monitoren
- Er is een systeem aanwezig om stakeholders te informeren over risico's
- De Risk management - Kwalificatie Indicatoren is niet relevant

Zijn de antwoorden op Risk management - Kwalificatie Indicatoren compleet en relevant? Waarom?

10. Risk management - Kwalificatie Risico-analyse*

Selecteer één of meer antwoorden

- Er wordt geen risico-analyse uitgevoerd
- Er is een gedecentraliseerde risico-analyse uitgevoerd
- Er is een gecentraliseerde risico-analyse uitgevoerd
- Er is een strategische risico-analyse uitgevoerd
- Risico-analyse is geïmplementeerd in de planning van nieuwe ontwikkelingen
- De Risk management - Kwalificatie Risico-analyse is niet relevant

Zijn de antwoorden op Risk management - Kwalificatie Risico-analyse compleet en relevant? Waarom?

11. Risk management - Kwalificatie Beheersing risico's*

Selecteer één of meer antwoorden

- Risico's worden deels beheerst
- Sommige typen risico's worden gezamenlijk beheerst
- Risico's worden beheerst op geïntegreerde wijze
- De Risk management - Kwalificatie Beheersing risico's is niet relevant

Zijn de antwoorden op Risk management - Kwalificatie Beheersing risico's compleet en relevant? Waarom?

12. Compliance - Kwalificatie structuur*

Selecteer één of meer antwoorden

- Er wordt geen poging gedaan om dezelfde processen te standaardiseren
- Er wordt een kleine poging gedaan om dezelfde processen te standaardiseren
- Dezelfde processen zijn gestandaardiseerd over delen van de organisatie
- Dezelfde processen zijn geëvalueerd over delen van de organisatie
- Dezelfde processen zijn gestandaardiseerd binnen de organisatie
- De Compliance - Kwalificatie structuur is niet relevant

Zijn de antwoorden op Compliance - Kwalificatie structuur compleet en relevant? Waarom?

13. Compliance - Kwalificatie Regels naleven*

Selecteer één of meer antwoorden

- Er wordt geen poging gedaan om regels op te stellen en na te leven
- Er wordt een kleine poging gedaan om regels op te stellen en na te leven
- Er is een makkelijke manier om regels op papier te zetten en na te leven
- Professionals voelen zich veilig om regels op te stellen en na te leven
- Professionals hebben vertrouwen in de kwaliteit van het proces regels opstellen en naleven
- De Compliance - Kwalificatie Regels naleven is niet relevant

Zijn de antwoorden op Compliance - Kwalificatie Regels naleven compleet en relevant? Waarom?

14. Compliance - Kwalificatie Controles*

Selecteer één of meer antwoorden

- Er is vertrouwen in een handleiding compliance processen & controles
- Handleiding & geautomatiseerde compliance processen & controles
- Tactisch geautomatiseerd compliance processen & controles
- Strategisch geautomatiseerde compliance processen & controles
- Flexibele strategisch geautomatiseerde compliance processen & controles
- De Compliance - Kwalificatie Controles is niet relevant

Zijn de antwoorden op Compliance - Kwalificatie Controles compleet en relevant? Waarom?

15. Compliance - Kwalificatie Bewust zijn van compliance*

Selecteer één of meer antwoorden

- De organisatie is onverschillig tegenover compliance
- De organisatie maakt zich zorgen over het vaststellen van non-compliance
- De organisatie monitoort continue op compliance
- De organisatie plant controles in om compliance te ondersteunen
- De organisatie neemt compliance controles op in de organisatie
- De Compliance - Kwalificatie Bewust zijn van compliance is niet relevant

Zijn de antwoorden op Compliance - Kwalificatie Bewust zijn van compliance compleet en relevant? Waarom?

Bijlage 5 Verklaring van eigen werk

Verklaring van eigen werk

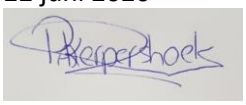
Open Universiteit
www.ou.nl

Studentnaam : Petra Kroos-Kerpershoek
Studentnummer : 852095601
Cursuscode en -naam : IM0602 Voorbereiden Afstuderen BPMIT
IM9806 Afstudeeropdracht Business Process Management and IT
Titel opdracht : Data governance maturity model met als onderdeel GRC

In het 'Examenreglementen' (Examenreglement) van alle faculteiten van de Open Universiteit, hoofdstuk 2, bevat paragraaf 3 identieke definities en een gedetailleerde uitleg van de begrippen fraude en plagiaat. Het examenreglement is alleen beschikbaar in het Nederlands en is te vinden op www.ou.nl.

Verklaring student:

Ik heb de definities van fraude en plagiaat zorgvuldig gelezen en begrepen, en verklaar hierbij dat bovengenoemde opdracht volledig mijn eigen werk is en dat ik mij niet schuldig heb gemaakt aan fraude en/of plagiaat.

Plaats : Hendrik Ido Ambacht
Datum : 22 juni 2020
Handtekening : 

Studenten bezitten het copyright op hun scriptie en hebben het recht om de publicatie ervan te voorkomen. Om er zeker van te zijn dat de Open Universiteit geen inbreuk maakt op dit recht, publiceren wij het rapport alleen als daar expliciet toestemming voor is verleend door ondertekening van dit formulier.

Ik ben het ermee eens dat mijn proefschrift op PURE kan worden gepubliceerd: pure.ou.nl.

Plaats : Hendrik Ido Ambacht
Datum : 22 juni 2020
Handtekening : 

Bijlage 6 Aanpassingen in criteria in DGGRCMM

Uit de interviews bleek dat de criteria niet concreet genoeg waren. Naar aanleiding van de te verbeteren punten van de vier experts is DGGRCMM V0.2 opgesteld.

DGGRCMM V0.2

Domeinen	Dimensies	Kwalificaties	No process	Beginning process	Established process	Managed process	Optimizing process
Governance	Gezag en Verantwoordelijkheden	Gezag	Ad-hoc leiding van directie, eigenlijk nemen de professionals de beslissingen	Directie is verantwoordelijk zonder dat zij de knoop doorhakt bij het nemen van beslissingen	Directie is verantwoordelijk en hakt de knoop door bij het nemen van beslissingen	Directie is verantwoordelijk en neemt beslissingen zonder advies van professionals	Directie is eindverantwoordelijk en neemt beslissingen op advies van professionals
		Verantwoordelijkheden	Professionals zijn geen verantwoording verschuldigd aan het management	Professionals zien verantwoording als bureaucratisch proces met veel regels en protocollen	Elke professional dient verantwoording af te leggen aan het management	Elke professional omarmt zijn/haar verantwoordelijkheid	Elke professional is wezenlijk gemotiveerd om zijn/haar verantwoordelijkheid te dragen
	Structuur en Beleid	Structuur	Er is geen datakwaliteitsraamwerk aanwezig	Het datakwaliteitsraamwerk is matig gestructureerd en niet gedocumenteerd	Het datakwaliteitsraamwerk is gestructureerd en bekend bij professionals	Het datakwaliteitsraamwerk is geïmplementeerd en de meeste professionals dragen hieraan bij	Alle professionals dragen proactief bij aan een geïntegreerd datakwaliteitsraamwerk
		Regels\procedures	Er zijn geen regels aanwezig m.b.t het DG beleid	De regels voor het DG beleid zijn slecht gestructureerd & niet gedocumenteerd	De regels voor het DG beleid zijn gestructureerd en bekend bij professionals	De regels voor het DG beleid zijn geïmplementeerd, de meeste professionals werken ermee	Alle professionals houden zich aan geïntegreerde regels
		Controle professionals	Er wordt geen audit uitgevoerd bij de professionals	Er wordt ad-hoc een interne en/of externe audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een beknopte interne en/of externe audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een uitgebreide interne en/of externe audit uitgevoerd o.b.v. kwaliteitsindicatoren	Er wordt een jaarlijks en tussentijds uitgebreide interne en/of externe audit uitgevoerd o.b.v. kwaliteitsindicatoren
	Rapporteren	Rapporteren resultaten	Er worden geen resultaten m.b.t. data gerapporteerd.	Er wordt een papieren formulier gebruikt om resultaten m.b.t.data te rapporteren/beoordelen	Er is een makkelijke manier om resultaten m.b.t. data te rapporteren/beoordelen aanwezig	Professionals voelen zich veilig om resultaten m.b.t. data te rapporteren/beoordelen	Professionals hebben vertrouwen in de kwaliteit van het proces van resultaten m.b.t. data te rapporteren/beoordelen
		Rapporteren incidenten	Incidenten worden op ad-hoc basis gerapporteerd	Er wordt een papieren formulier gebruikt om incidenten te rapporteren	Er is een makkelijke (elektronische) manier om incidenten te rapporteren	Professionals voelen zich veilig om incidenten te rapporteren	Professionals vertrouwen de kwaliteit van het proces van incidentenrapportage
Riskmanagement	Monitoring	Structuur	Er is geen RM raamwerk aanwezig		Er wordt een RM raamwerk gebruikt, maar is nog in ontwikkeling		Een RM raamwerk is volledig geïmplementeerd
		Indicatoren en monitoring	Er zijn geen risico indicatoren aanwezig voor het monitoren van data	Indicatoren worden gebruikt voor interne regelgeving en beleid	Indicatoren worden gebruikt voor interne en extern regelgeveing en beleid	Een RM indicator is in gebruik om risico's te monitoren	Er is een RM indicator in gebruik om risico's te monitoren en om stakeholders te informeren over risico's
	Beheersen risico's	Risico-analyse	Er vindt geen analyse/beoordeling plaats m.b.t. risico's op data	Er is vindt een gedecentraliseerde analyse/beoordeling plaats m.b.t. risico's op data	Er is vindt een gecentraliseerde analyse/beoordeling plaats m.b.t. risico's op data	Er vindt een strategische analyse/beoordeling plaats m.b.t. risico's op data	Risico-analyse/beoordeling is volledig geïmplementeerd in de planning van nieuwe ontwikkelingen
		Beheersing risico's	Risico's op proces en data worden beperkt beheerst	Risico's op proces en data worden deels beheerst	Risico's op proces en data worden gemonitord en deels beheerst	De hoofdrisico's op proces en data worden gemonitord en beheerst	Alle Risico's op proces en data worden gemonitord en volledig beheerst
Compliance	Naleving beleid	Structuur	Er wordt geen poging gedaan om soortgelijke processen te standaardiseren	Er wordt een kleine poging gedaan om soortgelijke processen te standaardiseren	Soortgelijke processen zijn gestandaardiseerd over delen van de organisatie	Soortgelijke processen zijn gestandaardiseerd en geëvalueerd over delen van de organisatie	Soortgelijke processen zijn gestandaardiseerd en geevalueerd binnen de gehele organisatie
		Regels naleven	Er wordt geen poging gedaan om de regels op te stellen en na te leven	Er wordt een kleine poging gedaan om regels op te stellen en na te leven	Er is een makkelijke manier om regels op papier te zetten en na te leven	Professionals voelen zich veilig om de regels op te stellen en na te leven	Profesionals hebben vertrouwen in de kwaliteit van het proces regels opstellen en leven de regels na
		Controles	De organisatie is afhankelijk van handmatige compliance processen & controlemechanismen	De organisatie heeft handmatige compliance processen & controlemechanismen	De organisatie beheerst risico's m.b.t. compliance processen (beleid) & controlemechanismen	De organisatie voert operationele en strategische analyses uit m.b.t. compliance processen en controlemechanismen	De organisatie voert flexibele operationele en strategische analyses uit op compliance processen & controlemechanismen
	Bewustzijn	Bewust zijn van compliance	De organisatie is onverschillig tegenover het naleven van wet- en regelgeving	De organisatie zet zich in voor het rechtzetten van non-compliance	De organisatie monitort continue op het naleven van wet- en regelgeving	De organisatie voert controles in om het naleven van wet- en regelgeving te handhaven	De organisatie heeft controles op wet- en regelgeving geïntegreerd in de organisatie.

Figuur 6.1 DGGRCMM V0.2