Shahim, A., Batenburg, R. Een governance, risicomanagement en compliance (GRC) volwassenheidsmodel voor de Nederlandse ziekenhuizen. Maandblad voor Accountancy en Bedrijfseconomie: 2013, 87(11), 473-482

Een governance, risicomanagement en compliance (GRC) volwassenheidsmodel voor de Nederlandse ziekenhuizen.

ABBAS SHAHIM EN RONALD BATENBURG

Samenvatting in dit artikel presenteren wij de eerste aanzet tot een maturity mo- Del (hierna; 'volwassenheidsmodel') om de volwassenheid van nederlandse zieken- huizen op het terrein van governance, risicomanagement en compliance (verder: GRC) vast te stellen, te monitoren en te verbeteren. Een literatuurstudie over de gezondheidszorg en een uitgebreide vergelijking van bestaande volwassenheidsmodellen hebben gediend als input voor de eerste versie van het model. Het model is vervolgens getest door middel van interviews met senior managers van grote zie- kenhuizen en in twee versies bijgewerkt en verfijnd. Het model bestaat uit 14 ver- schillende dimensies die zijn gebaseerd op de hoofdelementen van GRC in de dagelijkse praktijk van ziekenhuizen en vijf volwassenheidsniveaus.

Relevantie voor de praktijk: De waarde van het model ligt in de ondersteuning van een praktische aanpak die ziekenhuizen alsmede andere organisaties kunnen hanteren om hun huidige GRC-volwassenheid te bepalen en deze te verbeteren.

1 INLEIDING

Verscheidene ontwikkelingen in de gezondheidszorg hebben ervoor gezorgd dat ziekenhuizen de behoefte hebben aan een aanpak die bekend staat als governance, risicomanagement en compliance (GRC). GRC is als concept interessant voor ziekenhuizen om rekening te houden met de toenemende mate waarin zij gemonitord worden door de maatschappij, de overheid, toezichthoudende organen en verzekeraars. Gedurende de afgelopen jaren hebben overheden om uiteenlopende redenen veel nieuw beleid en nieuwe regelgeving geïntroduceerd in de gezondheidszorg.
Ziekenhuizen staan constant onder druk om zeker te stellen dat de beschikbare middelen op een efficiënte, effectieve en verifieerbare wijze worden gebruikt. Bestuurders dienen duidelijk te maken dat adequaat risicomanagement wordt uitgeoefend door verantwoord om te gaan met de geïdentificeerde risico's.

Formeel gezien zijn zij verplicht om alle relevante aspecten van hun functioneren te rapporteren aan inspectieorganen en overheidsinstanties. Bovendien verwacht de samenleving van ziekenhuizen dat zij zich verantwoordelijk en transparant opstellen. Het is bijvoorbeeld in het geval van een bacterie-uitbraak essentieel dat direct passende maatregelen worden getroffen en, om dergelijke situaties te voorkomen, aan te tonen dat deze in gebruik zijnde maatregelen effectief werken.
Hoewel GRC een veel gehoord concept is bij multinationals, banken, verzekeraars en beursgenoteerde bedrijven, is nog weinig empirisch onderzoek gedaan naar de adoptie ervan in organisaties. Dat geldt nog sterker voor ziekenhuizen. Dit is opvallend, gezien hun maatschappelijke functie en rekening houdend met het feit dat deze instellingen worden geconfronteerd met een toenemende druk vanuit wet- en regelgeving – bijvoorbeeld met betrekking tot privacy. Daarom is de behoefte des te groter geworden om naast de methoden voor de implementatie van GRC ook (op empirisch onderzoek gebaseerde) modellen te ontwikkelen die ziekenhuizen kunnen ondersteunen bij het streven naar het beoogde GRC- volwassenheidsniveau. Deze modellen zijn daarmee niet uitsluitend relevant voor deze instellingen, maar ook voor andere organisaties die in sterk gereguleerde markten opereren waarin onder meer risicomanagement en toezicht van essentieel belang zijn. In dit artikel presenteren we de eerste versie van een GRC-volwassenheidsmodel dat is toegesneden op de situatie van ziekenhuizen in Nederland. Hieronder wordt beschreven hoe het model is ontwikkeld, getest en toegepast op een aantal zieken- huizen. In de conclusie reflecteren we op onze werkwijze en geven we aan hoe het model breder gebruikt zou kunnen worden als onderzoeksinstrument.

2 VAN RISICOMANAGEMENT NAAR GRC

Over het algemeen wordt aangenomen dat de onderliggende filosofie van risicomanagement duidelijk is voor ziekenhuizen. Het belang van risicomanagement wordt erkend en men heeft passend beleid en bijbehorende plannen uitgewerkt, procedures en handboeken geïmplementeerd en activiteiten ontplooid. Voorbeelden zijn training van personeel en de ontwikkeling van handleidingen om zowel medische als niet-medische processen (zoals chirurgie en vastlegging van informatie over patiënten) die patiënten ondergaan onder controle te houden. Inspanningen zijn erop gericht de risico's die patiënten lopen binnen de ziekenhuizen zo goed mogelijk te kunnen managen zodat idealiter wordt gezorgd voor een 'incidentvrij' ziekenhuis en optimale zorg. Extern zijn drie belangrijke partijen te noemen waar ziekenhuizen op het terrein van risicomanagement mee te maken hebben. De eerste is de Inspectie voor de Gezondheidszorg (IGZ), dat deel uit- maakt van het Ministerie van Volksgezondheid, Wel- zijn en Sport (VWS), en zorgt voor handhaving van de kwaliteit van gezondheidsdiensten, preventiecontroles en medische producten. De inspectie beschikt over verschillende middelen om de naleving van wetgeving, professionele standaarden en richtlijnen te kunnen waarborgen. De tweede partij is het Nederlands Instituut voor Accreditatie in de Zorg (NIAZ) dat kwaliteitsnormen ontwikkelt. Het beoordeelt of de zorginstellingen aan de normen voldoen, verschaft zekerheid en zet aan tot verbeteringen. Ten derde kan als 'partij' het Veiligheidsmanagementsysteem (VMS Zorg, 2009) worden genoemd dat de verenigingen van ziekenhuizen (NVZ en NFU) heeft laten ontwikkelen om risico's

voor patiënten en vermijdbare schade te reduceren. Daarnaast staan een aantal basiseisen in de Norm Technische Afspraak (NTA) 8009 waaraan de zieken- huizen dienen te voldoen en die tevens voor externe audits wordt toegepast.

Het belang van GRC als een bredere aanpak dan risicomanagement is met name ontstaan door de hoge verwachtingen die de bevolking heeft ten aanzien van zorg in het algemeen en medisch-specialistische behandelingen in het bijzonder. Er wordt ervan uitgegaan dat in elk ziekenhuis zorg door specialisten wordt geleverd in een optimale omgeving zonder enig risico op fouten en met inachtneming van privacy. Een aantal ziekenhuisincidenten die expliciet in het nieuws open- baar is gemaakt laat zien dat deze perfecte wereld niet bestaat. Een bekend incident betreft een verslaafde
neuroloog die tussen 1990 en 2004 herhaaldelijk foutieve diagnoses heeft gesteld en recepten heeft vervalst bij het Medisch Spectrum Twente in Enschede (Van Aartsen, 2009). Een ander incident vond plaats in het Maasstad Ziekenhuis in Rotterdam, waar men er niet in is geslaagd om de verspreiding van de Klebsiella bacterie tijdig te voorkomen. Als gevolg hiervan zijn drie patiënten in september 2011 overleden en zijn vele andere geïnfecteerd (Van der Wal, 2012). Een derde incident dat de samenleving schokte kwam in februari 2012 aan het licht en ging over Eyeworks, een TV-producent die bij het VU Medisch Centrum (VUmc) in Amsterdam kon meekijken bij medische ingrepen op de spoedeisende hulp. De programmamakers konden luisteren naar conversaties van patiënten door gebruik te maken van 35 op afstand bestuurbare camera's (Van der Elsen, 2012). In de meeste gevallen was achteraf pas om toestemming gevraagd.

Medische fouten worden in toenemende mate onacceptabel gevonden in de moderne maatschappijen. Niet alleen vanuit ethisch oogpunt, maar de laatste tijd ook door een stijgende trend in het aantal en het bedrag van schades die zijn betaald aan ex-patiënten. In de afgelopen jaren is veel onderzoek verricht naar de invloed, de ernst en de oorzaken van verschillende soorten incidenten in ziekenhuizen om de effectiviteit van verschillende toegepaste methoden te evalueren, risicomanagementpraktijken te verbeteren en het behaalde niveau van compliance met wet- en regelgeving, procedures en richtlijnen in kaart te brengen (Dückers et al., 2009; Van der Hoeff & Van der Schaaf, 1995). Onderzoeken gericht op risicomanagement staan in nauw verband met de toepassing van wetten en relevante standaarden en indicatoren, zoals de Nederlandse Zorgwetgeving en de Joint Commission International (JCI). Dit laatste is een initiatief bedoeld als antwoord op de groeiende vraag naar standaard-gebaseerde evaluatie in de gezondheidszorg waardoor zorginstellingen in staat zijn om adequaat en integraal te sturen. Het perspectief sluit aan bij GRC als geïntegreerd concept en de premisse dat dit (op een samen- hangende wijze) onderdeel zou moeten uitmaken van het 'DNA' van ziekenhuizen. Wij beweren hiermee echter niet dat op deze wijze een geheel waterdicht systeem wordt gerealiseerd.

3 EEN OVERZICHT VAN DE GRC-LITERATUUR

Bij de bestudering van de literatuur op het gebied van GRC valt op dat het meest voorkomende thema integratie is. Dit komt terug in aspecten als samenwerking, delen van informatie en een holistische benadering van GRC. Een geïntegreerde aanpak van GRC als concept betekent dat een consistent overzicht bestaat waarmee de efficiëntie van processen kan worden verbeterd en risico's beheerst worden (OCEG, 2009; Mitchell, 2007; RIMS, 2006; Rasmussen, 2008). Een holistische benadering wordt gekarakteriseerd door communicatie en delen van informatie, ondersteund door verschillende IT-oplossingen en -omgevingen. De drie onderdelen van GRC afzonderlijk worden in de literatuur als volgt omschreven:

- *Governance* gaat over hoe het management dient te zijn vormgegeven en wat de bijbehorende rollen en verantwoordelijkheden zijn. Governance houdt ook in dat op de hoogste leidinggevende niveaus gewaarborgd is dat de juiste procedures ter plaatse zijn en worden gecommuniceerd. Deze regels en procedures dienen extern te worden gecontroleerd zodat niet alleen het topmanagement continue kan vaststellen dat zij worden gevolgd. Met name de rol van de Raad van Toezicht is met de komst van de Zorgbrede Governance Code en de Governance Commissie Gezondheidszorg belangrijker geworden en scherper gedefinieerd (Brancheorganisaties Zorg (BoZ), 2005, 2010; Commissie Health Care Governance, 1999; OCEG, 2009).

- *Riscomanagement* is gericht op het mitigeren en minimaliseren van de impact van risico's c.q. kansen. Belangrijk is hoe deze risico's worden geïdentificeerd, geanalyseerd, geëvalueerd en afgedekt, met andere woorden worden gemanaged. Verscheidene aspecten van risicomanagement kunnen worden gebruikt voor het meten van de volwassenheid van een organisatie in dit opzicht. Daarbij kan onderscheid gemaakt worden tussen de scope en de structuur van risicomanagement, de frequentie van risicoanalyse, de mate van bewustzijn over risicomanagement en de mate waarin risico-indicatoren worden gebruikt (Carroll, 2003; RIMS, 2006, OCEG, 2009; Van Ros- malen, Kastelein & Prinsenberg, 2010).

- *Compliance* is de term die aangeeft of een organisatie in overeenstemming met wetten, regels, protocollen, standaarden en specificaties wordt bestuurd en functioneert. Dit kan op verschillende manieren worden bereikt, waaronder de inrichting van specifieke beheersmaatregelen om te monitoren of een organisatie *compliant* is. Een relevant aspect voor volwassenheidsmeting is *compliance mapping*, hetgeen is gericht op het stroomlijnen van externe en interne standaarden, het voorkomen van tegenstrijdigheden en het detecteren van overbodigheden (OCEG, 2009; Tarantino, 2008).

In de literatuur wordt GRC als een integraal concept op diverse manieren gedefinieerd. Eén van de meest gebruikte definities is die van Racz et al. (2010): GRC is een geïntegreerde en holistische benadering ten behoeve van organisatie-brede governance, risk en compliance. GRC waarborgt dat organisaties ethisch en volgens hun risicoprofiel intern beleid voeren dat enerzijds aan externe wetgeving

voldoet, en anderzijds zorgt voor afstemming tussen strategie, processen, technologie en mensen waardoor efficiency en effectiviteit worden verbeterd.

In de weinige literatuur over GRC in ziekenhuizen ligt de focus op hoe het ziekenhuis wordt bestuurd. Ver- schillende publicaties schenken voornamelijk aandacht aan de managementtransparantie, samenwerking tussen managementlagen en de scheiding van taken en verantwoordelijkheden (Ministerie van VWS, 2006; Brancheorganisaties Zorg (BoZ), 2005; Commissie Health Care Governance, 1999). Daarnaast is het management van patiëntveiligheid van cruciaal belang voor ziekenhuizen. Dit vormt een zeer specifiek risico in vergelijking met reguliere organisaties. Dit komt te- rug in de missies van ziekenhuizen waarin de veiligheid van patiënten centraal staat en adequaat manage- ment erop gericht is om de kwaliteit van zorg te verbeteren (Carroll, 2003; NPSA, 2006). Naast patiëntenzorg-gerelateerde risico's spelen ook werknemer- gerelateerde risico's en eigendomsrisico's een rol. Historisch gezien is risicomanagement gericht op financiële risico's en risico's van het niet compliant zijn, maar idealiter hoort de scope van risicomanagement alle typen risico's af te dekken middels een integrale benadering (Brancheorganisaties Zorg (BoZ), 2010; Carroll, 2003; Van Rosmalen et al., 2010). Binnen het GRC-concept vervult compliance een dominante positie in ziekenhuizen, gezien hun verplichten- de aard. Er zijn diverse wetten, richtlijnen, reguleringen en standaarden waaraan een ziekenhuis zich dient te houden. De wijze waarop dit wordt uitgevoerd en bestuurd is onderdeel van compliance management en compliance mapping (Beuving & Van der Wal, 2008; NEN, 2005; NVZ, 2010; OCEG, 2009; Vrije Universiteit Amsterdam, 2010).

4 ONTWIKKELING VAN HET GRC-VOLWASSENHEIDS- MODEL

Voortbouwend op het bovenstaande is een ontwerpgerichte en gefaseerde aanpak gehanteerd om een specifiek GRC-volwassenheidsmodel voor ziekenhuizen te ontwikkelen (Hevner et al., 2004). Binnen deze aanpak is een aantal stappen doorlopen die zijn gebaseerd op standaardmethoden die in de design science gebruikt worden om volwassenheidsmodellen te ontwikkelen (De Bruin et al., 2005; Knackstedt et al., 2011; Maier et al., 2009; Pöppelbuß & Röglinger, 2011).

Het te ontwikkelen GRC-volwassenheidsmodel heeft twee hoofddoelen: (1) het bepalen van de GRC-volwassenheid van ziekenhuizen en bewustzijn over de ontwikkeling hiervan te creëren, en (2) de GRC-volwassen- heid van ziekenhuizen te verhogen door deze te vergelijken met andere ziekenhuizen en organisaties (Maier et al., 2009).
De doelgroep voor het toepassen van het GRC-volwassenheidsmodel wordt gevormd door security officers, risicomanagers, compliance officers, auditors en directeuren van ziekenhuizen. Van hen wordt verwacht dat zij een overzicht hebben van GRC in de praktijk. Daarbij moet bedacht worden dat er meestal meer dan één functionaris nodig is om de volwassenheid te meten en te testen op validiteit, betrouwbaarheid en toepasbaarheid.

4.1 Stap 1: een overzicht van bestaande volwassenheids- modellen

Een vergelijking van bestaande (GRC-)volwassenheids- modellen is de eerste stap om te bepalen welke componenten van deze modellen kunnen worden gebruikt voor een GRC-volwassenheidsmodel voor ziekenhuizen. Daartoe is een uitgebreide vergelijkingsstudie uitgevoerd om de verschillen en overeenkomsten tussen bestaande volwassenheidsmodellen te inventariseren, en de structuren, inhoud of dimensies uit deze modellen te analyseren. In totaal zijn 15 modellen geselecteerd en vergeleken op een vijftal criteria. Tabel 1 geeft hiervan een overzicht.

[TABLE 1]

De vijf criteria die zijn gebruikt om de volwassenheids- modellen te rangschikken, en te vergelijken op wat het beste past bij het doel om een GRC-model voor zieken- huizen te ontwikkelen, zijn:
1. Het criterium ‘Niveaus’; demonstreert of een model een relevant aantal volwassenheidsniveaus heeft. Normaal gesproken ligt het aantal niveaus tussen de vier en zes (Maier et al., 2009). Een model met slechts 1 niveau werd niet gezien als een volwassenheidsmodel.
2. Het criterium ‘Dimensies’ laat zien of een model ver- schillende dimensies gebruikt. Dimensies zijn verzamelingen van interessegebieden, die soms ook *key* of *processsareas* (gebieden) worden genoemd. Een dimensie kan verder worden gespecificeerd op activiteit, gemeenschappelijke kenmerken en maatregelen per volwassenheidsniveau. Deze dimensies kunnen eendimensionaal, multidimensionaal of hiërarchisch zijn. Het voordeel van multidimensionale (hiërarchische) structuren is de mogelijkheid om aparte volwassenheidsmetingen te doen en een uitgebreid overzicht van het interessegebied te dekken (De Bruin et al., 2005; Lahrmann & Marx, 2010).
3. De ‘Aard’ van een volwassenheidsmodel kan descriptief (D) of prescriptief (P) zijn. Bij een descriptief mo- del zijn criteria voor ieder volwassenheidsniveau vastgesteld, bij een prescriptief model worden daar- bij ook maatregelen en suggesties beschreven voor verbeteracties, vaak op basis van *best practices* (De Bruin et al., 2005; Knackstedt et al., 2011; Pöppel- buß & Röglinger, 2011). Een prescriptief volwassenheidsmodel levert uitgebreidere informatie en heeft daarmee toegevoegde waarde voor een GRC-volwassenheidsmodel.
4. Het criterium ‘G R C Z’ geeft aan of de modellen aan- dacht besteden aan de vier elementen Governance, Risicomanagement, Compliance en, specifiek voor deze studie, Ziekenhuizen/Zorg. Ingeschat is in welk mate de inhoud van het volwassenheidsmodel gespecificeerd is voor deze vier elementen.
5. Het criterium ‘IT focus’ geeft weer of het model ook technologische specificaties kent. IT is belangrijk voor de integratie van Governance, Risicomanage- ment en Compliance en kan worden gezien als een *enabler*. Volwassenheidsmodellen met een IT-focus zijn relevanter als voorbeeld voor een GRC-volwassenheidsmodel voor ziekenhuizen.

Alle bovenstaande modellen en criteria overwegend en rekening houdend met verwijzingen in de literatuur, is het OCEG Corporate Governance model het meest geschikt om het beoogde GRC-volwassenheidsmodel verder op te baseren.

4.2 Stap 2: opbouw van het GRC-volwassenheidsmodel

De twee basisonderdelen van het te ontwikkelen GRC- volwassenheidsmodel zijn enerzijds de volwassenheids- dimensies en anderzijds de volwassenheidsniveaus.

De volwassenheidsdimensies van het GRC-volwassenheidsmodel zijn geformuleerd op basis van literatuurstudie en de hiervoor genoemde volwassenheidsmodellen, met name het OCEG Corporate Governance model.
Gekomen is tot een lijst van 14 dimensies die geclassificeerd zijn naar de drie GRC-elementen governance, risicomanagement en compliance, en wel als volgt:

Met betrekking tot Governance:

• governance structuur;
• klokkenluiders-proces;
• informatie delen;
• klachtafhandeling;
• incidentenrapportage;
• incidenten rondom veiligheid van patiënten.

Met betrekking tot Risicomanagement:

• frequentie van risicoanalyse;
• risicomanagement awareness;
• scope van risicomanagement;
• structuur van risicomanagement;
• risico-indicatoren.

Met betrekking tot Compliance:

• compliance mapping;
• informatiebeveiliging;
• compliance controls.

Aangenomen wordt dat deze dimensies essentiële onderdelen van de concepten Governance, Risicomanagement en Compliance dekken – zonder daarbij te beweren dat hiermee alle aspecten van deze dimensies volledig in het model geïncorporeerd zijn. Vervolgens zijn er twee benaderingen mogelijk om de volwassenheidsniveaus per dimensie te bepalen. Ten eerste een *fixed-level*-benadering waarbij een vast aantal volwassenheidsniveaus voor iedere volwassenheiddimensie bepaald wordt. En ten tweede een *focus-area*-benadering, waarbij een variabel aantal volwassenheidsniveaus voor iedere dimensie gedefinieerd wordt. De fixed levelbenadering past goed bij vergelijkingen en inschattingen, terwijl de focus-area-benadering past bij kleine verbeteringen (Van Steenbergen et al., 2010). De fixed-level-benadering wordt het meest gebruikt in volwassenheidsmodellen (De Bruin et al., 2005; Maier et al., 2009), hoewel het ook wordt bekritiseerd om het gevaar van ‘over-simplificatie’. Voor ons GRC-volwassenheidsmodel is een algemene *fixed-*

level als uitgangs- punt gebruikt, waarbij vijf volwassenheidsniveaus worden onderscheiden. Om oversimplificatie te voorkomen is wel de heuristiek gehanteerd dat in het geval een dimensie minder of meer volwassenheidsniveaus vergt het vaste aantal van vijf volwassenheidsniveaus wordt herzien voor die dimensie. Met deze hybride benadering worden de voordelen van de focus-area-benadering gebruikt om de fixed-level-benadering aan te vullen.
Aan de volwassenheidsniveaus zijn specifieke 'labels' toegekend welke zo 'intuïtief ' mogelijk geformuleerd zijn en een 'logische progressie' weergeven (Maier et al., 2009). Voor het GRC-volwassenheidsmodel zijn de indicaties van de vijf standaardniveaus gelabeld volgens het OCEG Corporate Governance model, namelijk:

1. formeren,
2. ontwikkelen,
3. normaliseren,
4. vaststellen,
5. optimaliseren.

Hiermee is een theoretisch begin- en eindpunt van de volwassenheidsniveaus bepaald, maar deze dienen statisch noch deterministisch te worden toegepast. Per volwassenheidsdimensie kan het optimale niveau op verschillende manieren worden gedefinieerd. Dit zal in de volgende paragraaf worden verduidelijkt.

4.3 Stap 3: het GRC-volwassenheidsmodel 1.0 en 2.0

Als de 14 volwassenheidsdimensies en de vijf volwassenheidsniveaus gecombineerd worden, omvat het resulterende volwassenheidsmodel ('versie 1.0') (15x5=) 75 cellen. Voor nagenoeg elke cel van het model is ver- volgens een item geformuleerd op basis van de GRC- literatuur. Alle 14 dimensies kennen dus (meestal) 5 items, één voor elk volwassenheidsniveau, waarvoor de respondent op een 5-puntsschaal kon aangeven in hoeverre dit item van toepassing was op zijn zieken- huis. Deze eerste versie van het model is vervolgens in de praktijk getest door het aan vijf senior managers van ziekenhuizen voor te leggen. De managers zijn actief in governance, risicomanagement of compliance voor hun ziekenhuis. Het aantal 'test-experts' is beperkt, maar voor een eerste test voldoende omdat ze wel in verschillende ziekenhuizen (academisch, perifeer) werkzaam zijn. De interviews leverden drie algemene aandachtspunten op: (1) dat er soms een 'gat' is tussen de theoretische begrippen en de praktijk, (2) dat er een zekere onbalans is tussen de dimensies, en (3) dat de dimensies nog meer gestructureerd zouden kunnen worden, op een gelaagde wijze. Naast deze feed- back ter verbetering van het model maakten de interviews ook duidelijk dat GRC-beleid binnen ziekenhuizen nog niet goed genoeg geregeld is, maar dat er wel wordt gewerkt aan ontwikkeling en (verde- re) implementatie. Na ieder interview werd het volwassenheidsmodel bijgewerkt en geleidelijk verfijnd. Het model wat te zien is in tabel 2 vormt de 2.0 versie van het GRC-volwassenheidsmodel voor ziekenhuizen.

5 TOEPASSING VAN HET GRC-VOLWASSENHEIDSMODEL OP EEN VIERTAL ZIEKENHUIZEN

Zoals hiervoor beschreven, is met het GRC-volwassenheidsmodel 2.0 een vragenlijst opgesteld, waarbij voor elk van de (gevulde) cellen één 5-punts-item als meetinstrument geformuleerd is. Hiermee kan het GRC-volwassenheidsniveau van ziekenhuizen op alle dimensies en niveaus vastgesteld worden. Dit ontwikkelproces is gebaseerd op de benadering van Pederiva (2003).

[TABLE 2]

Deze vragenlijst is vervolgens daadwerkelijk in de praktijk toegepast door middel van gestructureerde interviews met senior managers van vier grote ziekenhuizen. Het betrof hier andere senior managers dan zij die tijdens de test- fase zijn ondervraagd. Het doel van de interviews was tweeledig. Ten eerste was het de bedoeling om te controleren of de vragenlijst geschikt is om het GRC-volwassenheidsniveau te bepalen, of deze begrijpelijk is, en onafhankelijk kan worden ingevuld. Ten tweede zijn de interviews gebruikt om de opgegeven scores van de vier ziekenhuizen te bespreken en te analyseren.

Alle geïnterviewde senior ziekenhuismanagers gaven aan de vragenlijst goed te kunnen invullen en de vragen en antwoordcategorieën te hebben begrepen. Nadat de vragenlijst was ingevuld werden de scores op het volwassenheidsmodel van hun ziekenhuis aan de geïnterviewde getoond om zo ‘fouten’ of onzekerheden in het model te kunnen duiden. Daarbij moet bedacht worden dat de scores een subjectieve inschatting van de respondent voor hun ziekenhuis blijven. Ook kon op basis van de vragenlijstscores en interviewresultaten een vergelijking worden gemaakt tussen de vier ziekenhuizen middels ‘spinnenweb’-grafieken die de balans tussen de GRC-elementen weergeven. Deze balans houdt verband met het idee van ‘integrale GRC’, namelijk dat verschillen in volwassenheid kunnen duiden op een gebrek aan samenhang tussen de (sub)dimensies van het GRC-domein. Figuur 1 geeft de volwassenheidsscores van de vier ziekenhuizen op de 14 individuele dimensies weer. De stippellijn vertegenwoordigt de gemiddelde score van de vier ziekenhuizen.

Figuur 1 laat zien dat gemiddeld de Governance-scores hoger zijn dan de Risicomanagement- en Compliance-scores. Dit gaat op voor ziekenhuizen 1-3 maar ziekenhuis 4 scoort juist hoger op Compliance dan op Governance. Dat komt omdat Ziekenhuis 4 relatief hoog scoort op de dimensie ‘Compliance: autoriteit’ en daarmee op de gemiddelde Compliance-score. Uit de interviews blijkt dat deze hoge score op ‘Compliance: autoriteit’ verklaard kan worden door een toegewijde security officer die Compliance nauw- keurig stuurt. De scores van de ziekenhuizen op het GRC-element Risicomanagement variëren vergeleken met de scores op de Governance- en Compliance-elementen. Dit komt onder andere door de relatief lage scores op de dimensies ‘Risicomanagement: autoriteit’ en ‘Risicomanagement: analyse’. De geïnterviewden erkenden de lage scores op deze dimensies en ga- ven aan dat deze in toenemende mate aandacht krijgen en dat er ruimte is voor ontwikkeling. De op-vallend hoge scores van ziekenhuis 2 op Risicomanagement en Compliance tenslotte, werden in de interviews verklaard als een gevolg van het feit dat deze twee GRC-

elementen veel aandacht hebben gekregen nadat eerder serieuze problemen (non-compliance) aan het licht kwamen.

6 CONCLUSIE

Veel organisaties worstelen met het vormgeven van hun GRC-strategie vanuit een holistisch en geïntegreerd concept. Dit geldt des te meer voor ziekenhuizen waar GRC als concept nog onvoldoende aandacht krijgt. Om hen daarbij te ondersteunen presenteren we in dit artikel een model dat ziekenhuis-managers kan helpen bij het transformeren van hun gefragmenteerde en ongecoördineerde benadering van risicomanagement. Het model is een eerste aanzet voor een managementinstrument om de GRC-volwassenheid van ziekenhuizen vast te stellen en te monitoren. De 1.0-versie van het volwassenheidsmodel is ontwikkeld op basis van GRC-literatuur en verwante volwassenheidsmodellen. Dit model is vervolgens getest en geëvalueerd door de inhoudelijke experts te interviewen, waarna een tweede versie van het model is toegepast op een viertal Nederlandse zie- kenhuizen. Dit vormde een eerste toepassingsronde die weliswaar beperkt is, maar toch liet zien dat het model in de praktijk goed te begrijpen en in te vullen is. Tevens bleek een grote behoefte te zijn aan kennis en de bepaling van GRC-volwassenheid bij managers en deskundigen. Het GRC-volwassenheidsmodel lijkt een belangrijk instrument te zijn voor gezondheidszorg en het ziekenhuismanagement.

We hebben in dit artikel laten zien dat de volwassenheid van GRC in de ziekenhuizen op een kwantitatieve wijze in kaart kan worden gebracht, door middel van een multidimensioneel, stage-based volwassenheids- model. De balans in de scores op de verschillende dimensies geeft een indicatie of GRC ook integraal wordt toegepast – hoewel de integraliteit van GRC daarmee nog niet direct is gemeten. Onze geïnterviewden kon- den zich met de uitkomsten van het empirisch onder

[FIGUUR 1]

LITTERATUUR

Aartsen, C. van. (2009). Bestuurder moet in- grijpen. Geraadpleegd op http://www.sin-nl.org/pdfs/bestuurder_moet_ingrijpen.pdf.

Beuving, J., & Wal, G. van der. (2008). Infor- matiebeveiliging in ziekenhuizen voldoet niet aan de norm. Geraadpleegd op www.igz.nl.

Brancheorganisaties Zorg (BoZ) (2010). Zorg- brede governancecode 2010. Geraadpleegd op http://www.brancheorganisatieszorg.nl/doc/ZorgbredeGovernancecode2010BoZ.pdf .

Brancheorganisaties Zorg (BoZ) (2005). Zorg- brede governancecode 2005. Geraadpleegd op http://www.nvtk.nl/uploads/media/Zorgbrede_GovernancecodeBoZ__dec._2005 01.pdf .

Bruin, T. de, Freeze, R., Kaulkarni, U., & Rose- mann, M. (2005). Understanding the main phases of developing a maturity assessment model (Conference Paper). Geraadpleegd op http://eprints.qut.edu.au/25152/.

Carroll, R. (2003). Risk management hand- book for health care organizations (4th ed.). San Francisco, CA: Jossey-Bass.

Commissie Health Care Governance (1999). Health care governance; Aanbevelingen voor goed bestuur, goed toezicht en adequate verantwoording in de Nederlandse gezondheids-zorg. Voorzitter P. Meurs. Leusden: C3 adviseurs en managers.

Dückers, M., Faber, M., Cruijsberg, J., Grol, R., Schoonhoven, L. & Wensing, M. (2009). Safety and risk management in hospitals. Londen: The Health Foundation.
Elsen, W., van der (2011). Excuses VUmc om fout met tv-opnames. Geraadpleegd op http://www.zorgvisie.nl/Kwaliteit/Nieuws/2012/2/Excuses-VUmc-om-fout-met-tv-opnames-ZVS013378W/.
Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.
Hoeff, N.W.S. van der, & Schaaf, T.W., van der. (1995). Risk management in hospitals: Predicting versus reporting risks in a surgical department (Conference paper). Eindhoven: Safety Management Group. Geraadpleegd op http://home.versatel.nl/crbakker/pdf/article_annual.pdf .
Knackstedt, R., Pöppelbuß, J., & Becker, J. (2011). Developing maturity models for IT management – A procedure model and its application. Business & Information Systems Engineering, 1(3), 213-222.
Lahrmann, G., & Marx, F. (2010). Systematiza- tion of maturity model extensions. In R. Winter, J.L. Zhao, & S. Aier (Eds.), Global perspectives on design science research (vol. 6105, pp. 522-525). Berlin, Heidelberg: Springer.
Maier, A. M., Moultrie, J., & Clarkson, P. J. (2009). Developing maturity grids for asses- sing organisational capabilities: Practitioner guidance. In: 4th International Conference on Management Consulting, Academy of Ma- nagement (MCD'09), Wenen, Oostenrijk.
Ministerie van Volksgezondheid, Welzijn en Sport (2006). Goed bestuur in de zorg. Informatie over de transparantie-eisen Wet toelating zorginstellingen. Geraadpleegd op http:// www.vgn.nl/media/download/index/mediaid/4ca5c371ae363 .
Moultrie, J. (2004). Development of a design audit tool to assess product design capability. (Ph.D. Thesis). University of Cambridge, Department of Engineering, Cambridge, United Kingdom.
National Patient Safety Agency (NPSA). (2006). Patient safety resources. Manchester Patient Safety Framework. Geraadpleegd op http://www.nrls.npsa.nhs.uk/resources/?entryid45=59796 .
Nederlands Normalisatie Instituut (NEN). (2005). NEN7510 - De norm in zijn omgeving. Geraadpleegd op http://www.nen7510.org/publicaties/3420 .
Nederlandse Vereniging van Ziekenhuizen (2010). NVZ toetsingsreglement informatiebeveiliging. NVZ.
Netherlands Institute for Accreditation in Heal- thcare (NIAZ), NIAZ in a nutshell. Geraadpleegd op http://en.niaz.nl/corporate-brochure.
The Open Compliance and Ethics Group (OCEG). (2009). GRC capability model (Red Book 2.0). Geraadpleegd op http://www.oceg. org/resources/GRC-capability-model-red-book/.
Pederiva, A. (2003). The COBIT maturity model in a vendor evaluation case. Information Systems Control Journal, 3, 26–29.
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. 19th European Conference on Information Systems (ECIS). Geraadpleegd op http://aisel.aisnet.org/ecis2011/28/.
Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). Communications and Multimedia Security, 6109, 106–117.
Rasmussen, M. (2008). GRC perspectives research: 2008 GRC drivers, trends, & market directions. Geraadpleegd op http://www.GRC2020.com .
The Risk Management Society (RIMS). (2006). RIMS enterprise risk management – Risk maturity model. Geraadpleegd op http://www.rims.org/ERM/Pages/RiskMaturityModel.aspx
Rosmalen, A. van, Kastelein, E., & Prinsenberg, M. (2010). Risicomanagement Nederlandse zorginstellingen nog in ontwikkeling, Spotlight, 17(2), 40-44. Geraadpleegd op http://www.pwc.nl/nl/spotlight/assets/documents/spotlight- jaargang17-2010-uitgave-2.pdf .
Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I., van de, & Bekkers, W. (2010). The design of focus area maturity models. In R. Winter, J.L. Zhao, & S. Aier. Global perspec- tives on design science research (pp. 317- 332). Berlin, Heidelberg: Springer.

Tarantino, A. (2008). The Governance, Risk, and Compliance Handbook: Technology, finance, environmental, and international guidance and best practices (1st ed.). Hoboken, NJ: Wiley. Veiligheidsmanagementsysteem (VMS) Zorg. (2009). Veilig werken met VMS Zorg: Het landelijke systeem voor patiëntveiligheid, VMS Zorg. Veiligheidsmanagementsysteem (VMS). (2009). Praktijkgids: Prospectieve risico inventarisatie (PRI). Geraadpleegd op http://www.veiligezorgiederszorg.nl/speerpunt-vms/prak- tijkgids-pri.pdf . Vrije Universiteit (VU) Amsterdam (2010). Compliance in de Zorg. VU magazine.

Wagner, C., Smits, M., Wagtendonk, I. van, Zwaan, L., Lubberding, S., Merten, H., & Timmermans, D.R.M. (2008). Oorzaken van incidenten en onbedoelde schade in ziekenhuizen: Een systematische analyse met PRISMA op afdelingen spoedeisende hulp (SEH), chirurgie en interne geneeskunde. Utrecht, Amsterdam: NIVEL & EMGO Instituut.

Wal, G., van der. (2012). Falen infectiepreventie in het Maasstad Ziekenhuis verwijtbaar (Inspectie voor de gezondheidszorg, Ministerie van volksgezondheid, welzijn en sport). Geraadpleegd op www.igz.nl.

Wetering, van der, R. & Batenburg, R. (2010). Evolutionistic or revolutionary paths? A PACS maturity model for strategic situational planning. International Journal of Computer Assisted Radiology and Surgery, 5(4), 401-409.

TABELLEN EN FIGUUR

Tabel 1 Bestaande volwassenheidsmodellen

Model/ organisatie naam	Niveaus	Dimen-sies	Aard	G R C Z	IT focus
AMR research	4	1	D	G R C	
IT Policy Compliance Group	5	13	P	R C	Ja
NHS Infrastructure	5	12	D	G Z	Ja
CobiT 4.1	6	6	P	G	Ja
OCEG Corp. Governance	5	5	D	G	
OCEG RIMS Risk	5	7	D	R	
OCEG Corporate Compliance	5	6	D	C	
OCEG GRC Capability Model	0	8	P	G R C	
SAP	4	1	D	G R C	
Deloitte	5	1	D	G R C	Ja
KPMG	4	3	D	G R C	
COSO	0	8	D	R	
CMMI for services	5	24	P	R	
Nolan's Growth Model	6	4	D	G	Ja
MaPSaF	5	9	P	R Z	

Tabel 2 Het GRC-volwassenheidsmodel voor ziekenhuizen

	Volwassenheids-model Versie 2	Niveau 1 Formeren	Niveau 2 Ontwikkelen	Niveau 3 Normaliseren	Niveau 4 Vaststellen	Niveau 5 Optimaliseren
1	Governance: autoriteit	Ad-hoc autoriteit, in feite hebben de professionals de macht.	De directie is verantwoordelijk, maar heeft feitelijk geen enkele macht.	De directie is verantwoordelijk en heeft macht.	De directie is verantwoordelijk, heeft macht en de professionals protesteren er niet tegen.	De directie en professionals delen de macht op gebalanceerde wijze.
2	Governance: structuur	Er is geen P&C (planning & control) ter plaatse.	P&C is matig gestructureerd en niet gedocumenteerd.	P&C is gestructureerd en bekend bij de professionals.	P&C is geïmplementeerd en de meeste professionals dragen eraan bij.	Alle professionals dragen proactief bij aan een geïntegreerde P&C.
3	Governance: verantwoordelijkheid	Professionals hoeven geen verantwoording af te leggen tegenover management.	Professionals zien verantwoording afleggen als een bureaucratisch proces.	Iedere professional dient verantwoording af te leggen tegenover management.	Iedere professional omarmt zijn/haar verantwoordelijkheid.	Iedere professional is intrinsiek gemotiveerd om zijn/haar verantwoordelijkheid te dragen.
4	Governance: controle over professionals	Er wordt geen controle uitgevoerd over professionals.	Een interne controle wordt uitgevoerd op basis van kwaliteits-indicatoren.	Een externe controle wordt uitgevoerd op basis van kwaliteits-indicatoren	Een onaangekondigde externe controle wordt uitgevoerd.	Er is een goede balans tussen vertrouwen en controle.
5	Governance: rapportage van incidenten	Incidenten worden op ad-hoc basis gerapporteerd.	Een papieren formulier wordt gebruikt voor de rapportage van incidenten.	Er is een makkelijke (elektronische) manier om incidenten te rapporteren.	Professionals voelen zich gemakkelijk (veilig) bij het rapporteren van incidenten.	Professionals vertrouwen de kwaliteit van het proces van incidentenrapportage.
6	Risicomanagement: autoriteit	Er is geen CRO (Chief Risk Officer) aanwezig.	Een CRO is door de directie benoemd.	De CRO rapporteert direct aan de directie.	De CRO heeft autoriteit om veranderingen door te voeren.	De directie en de CRO communiceren het belang van ERM.
7	Risicomanagement: structuur	Er is geen risicomanagement framewerk ter plaatse.		Er is een risicomanagement framewerk ter plaatse in ontwikkeling.		Er is een volledig risicomanagement framewerk geïmplementeerd.
8	Risicomanagement: analyse	Er wordt geen risicoanalyse uitgevoerd.	Een gedecentraliseerde risicoanalyse wordt uitgevoerd.	Een gecentraliseerde risicoanalyse wordt uitgevoerd.	Strategische risicoanalyse wordt uitgevoerd.	Risicoanalyse wordt geïntegreerd in de planning van nieuwe ontwikkelingen.
9	Risicomanagement: scope	Risico's worden op gefragmenteerde wijze gemanaged.		Sommige typen risico's worden gezamenlijk gemanaged.		Risico's worden op een geïntegreerde wijze gemanaged.
10	Risicomanagement: indicatoren	Er zijn geen risico-indicatoren ter plaatse.	Indicatoren worden gebruikt voor interne regulering en beleid.	Indicatoren worden gebruikt voor interne en externe regulering en beleid.	Een risicomanagement dashboard wordt gebruikt om risico's te monitoren.	Er is een systeem ter plaatse om stakeholders te informeren.
11	Compliance: autoriteit	Er is geen CCO (Chief Compliance Office) ter plaatse.	Er is een CCO door de directie benoemd.	De CCO rapporteert direct aan de directie.	De CCO heeft autoriteit om veranderingen door te voeren.	De directie, de CRO en de CCO werken nauw met elkaar samen.
12	Compliance: structuur	Er worden geen pogingen gedaan om soortgelijke processen te standaardiseren.	Er worden bescheiden pogingen gedaan om soortgelijke processen te standaardiseren.	Soortgelijke processen worden binnen delen van het ziekenhuis gestandaardiseerd.	Soortgelijke processen worden binnen het ziekenhuis geëvalueerd.	Soortgelijke processen worden binnen het ziekenhuis gestandaardiseerd.
13	Compliance: controlemechanismen	Afhankelijkheid van handmatige compliance processen en controlemechanismen.	Handmatige & geautomatiseerde compliance processen en controlemechanismen.	Tactische geautomatiseerde compliance processen en controlemechanismen.	Strategische geautomatiseerde compliance processen en controlemechanismen.	Flexibele strategische geautomatiseerde compliance processen en controlemechanismen.
14	Compliance: besef	Het ziekenhuis is onverschillig met betrekking tot compliance.	Het ziekenhuis zet zich in voor het rechtzetten voor non-compliance.	Het ziekenhuis monitort constant compliance.	Het ziekenhuis plant controles om compliance te handhaven.	Het ziekenhuis incorporeert compliance controles.

Figuur 1