ORIGINAL ARTICLE

A maturity model for governance, risk management and compliance in hospitals

Ronald Batenburg[1, 2], Matthijs Neppelenbroek[3], Abbas Shahim[4, 5]

1. Utrecht University, the Netherlands. 2. Netherlands Institute for Health Services Research, the Netherlands. 3. Air France-KLM Information Services, the Netherlands. 4. ATOS Consulting, the Netherlands. 5. VU University, the Netherlands.

Correspondence: Ronald Batenburg. Address: Utrecht University, Department of Information and Computing Sciences, PO Box 80007, 3508 TA Utrecht, The Netherlands. E-mail: r.s.batenburg@uu.nl

Received: September 3, 2013 **Accepted:** January 23, 2014 **Online Published:** February 24, 2014
DOI: 10.5430/jha.v3n4p43 **URL:** http://dx.doi.org/10.5430/jha.v3n4p43

Abstract

In this paper we propose a preliminary model (hereafter referred to as maturity model) to assess and monitor Governance, risk and compliance (GRC) and GRC maturity in Dutch hospitals. Relevant health care literature and a comprehensive comparison of existing maturity models served as input for the developed maturity model. The maturity model was tested and evaluated by interviewing senior hospital managers, representing 12.4% of the total Dutch hospital bed capacity. The need and relevance of knowledge about GRC was repeatedly emphasized by the interviewees. The model consists of 14 different dimensions based on the headlines of the practice in Dutch hospitals and five levels of maturity. The primary value of the model lies in the compact presentation and its practical approach which can guide hospitals to improve their GRC maturity.

Key words

Maturity model, Governance, Risk and compliance, Hospital management

1 Introduction

Multiple changes in health care fortify the need for a new approach towards Governance, Risk Management & Compliance (GRC) in hospitals. GRC has become highly relevant for hospitals, as they are increasingly under the magnifying glass of the public, government, supervisory bodies and insurance companies. Over the past years, governments, for several reasons, introduced many new regulations and policies in the health sector. The Netherlands is a good example to elaborate this.

Today, it is normally presumed that the underlying philosophy of risk management is quite clear for Dutch hospitals. Boards and managers have mostly recognized this vital concept, elaborated corresponding policies and plans, implemented related procedures and handbooks, and undertaken many other activities including training the personnel and developing manuals to explicitly control medical as well as associated non-medical processes (*e.g*. surgery and recording patient information) through which patients usually go. The main aim of this essential and just effort is to manage risks incurred by the patients within hospitals as far as possible to ideally create an event-free hospital and lastly offer a better care. For fulfilling this crucial social task in an appropriate fashion, Dutch hospitals have also a number of possibilities and

instruments at their disposal of which we concisely describe here three examples to help establish a certain image of them. The first one is the Health Care Inspectorate (locally known as IGZ which is part of the Dutch Ministry of Health, Welfare and Sport) that promotes public health through effective enforcement of the quality of health services, prevention controls and medical products. The inspectorate possesses different measures to ensure adherence to legislation, professional standards and guidelines. The second possibility is concerned with the Netherlands Institute for Accreditation in Health-care (nationally called NIAZ) that develops quality standards. It assesses whether health care organizations comply with them and accordingly provides assurance and encourages improvements. The third possibility pertains to the Safety Management System (in the Netherlands referred to as "VMS Zorg") which is the rural system that supports in mitigating risks for patients and reducing (unintended) damages to them. The basic requirements for this goal are stated in NTA 8009 which must be satisfied by Dutch hospitals and are applied for performing external audits as well. Nevertheless, events of various nature occurred at Dutch hospitals are regularly the latest hot news and headlines these days.

To further illustrate the relevance of GRC in hospitals can be done by the high and straight level of anticipation people have when they end up at hospitals to be medically treated. For instance, it is plainly expected that we deal with reliable specialists, are in a hygienic environment and our privacy is not at risk. In reality, none of these can simply be true. Here, we clarify this by briefly explaining three serious hospital events exclusively disclosed in the Dutch news. The first one concerns an addicted neurologist that between 1990 and 2004 suggested misdiagnosis and falsified recipes repeatedly at Medisch Spectrum Twente located in Enschede [1]. The second adverse event relates to the Maasstad Ziekenhuis in Rotterdam that failed in timely preventing the Klebsiella bacteria from spreading as a result of which three patients died in September 2011 and many others got infected [2]. The third event revealed in February 2012 is about Eyeworks, a TV producer that was able to watch medical treatments and listen to conversations of patients at VU Medisch Centrum (VUmc) in Amsterdam by the use of 35 cameras operated remotely [3]. It was only afterwards asked for permission in most cases. It is currently evident that medical errors are increasingly getting intolerable in modern society, not only from an ethical point of view, but lately also due to a rising trend in the number and amount of damages paid to ex-patients. In the past years, much research has hence been conducted with the objective to assess the prevalence, severity and causes of numerous types of adverse events in hospitals, to evaluate the effectiveness of different used approaches in order to improve risk management practices, and to examine the achieved level of compliance with legislations, policies, procedures and guidelines [4, 5]. However, it can generally be stated that studies aimed at risk management in close relation with the applicable laws and pertinent standards and indicators (*e.g.* the Dutch Healthcare Law which is the literal translation of "De Nederlandse zorgwetgeving", and Joint Commission International [JCI] that is an initiative intended as a response to the growing demand for standard-based evaluation in health care) in an interconnected fashion enabling healthcare organizations to adequately govern are quite scarce. This overall and coordinated view on GRC can potentially serve as a valuable means to ascertain that this integrated business concept cohesively enters into the DNA of Dutch hospitals.

2 Method

As made clear above, hospitals, in addition to their economic/financial task, specifically hold a social responsibility. The management of a hospital is constantly under pressure to ensure that the available funds are used in a way that is efficient, effective and verifiable. Hospitals must make clear that they deal with risks in a responsible way and have an adequate risk management. In a formal sense they are obligated to report all relevant aspects of their functioning to inspection bodies and governmental agencies. Moreover, society expects hospitals to be accountable and transparent. For instance, in case of a bacteria outbreak in a hospital, it is strongly demanded that adequate measures are taken to prevent similar situations and to prove that those measures are effective.

Whereas GRC is fairly common in multinationals, banking, insurance and listed companies however, little is known about the actual adoption and maturity of GRC in hospitals. So far, no maturity models are available to facilitate hospitals to put in order and carry out their internal GRC and direct policies leading to a higher level of maturity in their GRC, as well as to

facilitate meeting obligations associated with new regulations. In this paper we develop such a model that explicitly focuses on hospitals and is built on dimensions and levels of development geared to their practice. We aim to answer the following question:

To what extent is GRC adopted in hospitals and how can the maturity of GRC in hospitals be improved?

In order to answer this question we first perform a scoping review. Then we develop the frame of the preliminary maturity model, by defining levels of GRC maturity of hospitals. The initial measurement of GRC maturity is then developed and executed as an assessment. Also subsequent measurements are proposed as monitoring. To be able to improve the level of GRC in a hospital, reasons and relations are investigated to explain levels of GRC maturity. From this, it is determined what the drivers and barriers are relevant to improve GRC maturity. This contributes to the practical part of this paper, *i.e*. how improvement can be achieved by overcoming barriers and using drivers into practical guidance on how to improve GRC maturity.

3 Results

3.1 A scoping review on GRC

When overlooking the literature on GRC the most common theme is integration. This is reflected in aspects such as cooperation, sharing information and a holistic approach to GRC. An integrated approach to GRC allows a consistent view by which the efficiency of processes can be improved [6-10]. A holistic approach is characterized by communication and sharing of information which can be supported by appropriate IT infrastructure.

In general, the three parts of GRC can be described as follows:

- Governance includes how the board and management should be structured and what their roles and responsibilities consist of. Governance also means that the board and management ensure that the right procedures are in place and communicated. Additionally, these policies and procedures should be checked so that the board and management know that procedures are followed [8, 11].
- Risk management aims to mitigate and minimize the impact of risk. There will always be a trade-off between risk and opportunities. It is important how those risks are identified, analyzed, evaluated and treated, in other words: managed. Several aspects of risk management are described that will be used as input for the maturity model: the scope of risk management, the structure of risk management, the frequency or risk analysis, the awareness of risk management and to what extent risk indicators are used [6, 8, 12, 13].
- Compliance is the term indicating that an organization operates in accordance to established laws, regulations, protocols, standards and specifications. This can be achieved in several ways. It is recommended to install specific controls to monitor that an organization is compliant. Another useful aspect for the maturity model is compliance mapping. Compliance mapping aims to streamline external and internal standards by removing discrepancies and detecting redundancies [8, 14].

When looking at GRC in hospital enterprises, the view is automatically on how a hospital is governed by the board of directors and management is reflected by several sources. The sources pay attention to management transparency, management documentation, the cooperation among management bodies and the separation of powers (*i.e*. the Netherlands [11, 15, 16]). Among many other things, the management of patient safety incidents is of key importance for hospitals. This aspect is of the essence when compared to regular organizations. A hospitals mission revolves around patient safety, and by adequate management of patient safety incidents it is possible to improve the quality of care and secure patient safety [12, 17]. Concerning risk management, several different types of risks are indicated, including

patient care-related risks, employee-related risks and property risks. Historically, risk management is focused on financial and non-compliance risks. But ideally, the scope of risk management covers all types of risks using an internal approach [12, 13, 18]. Within the GRC concept, compliance seems to be dominantly present in hospitals. Many sources focus on compliance issues which might be because it is mandatory. There are several guidelines, regulations and acts a hospital needs to comply to. How this is done, and controlled, is part of compliance management or compliance mapping [8, 19-21].

3.2 Developing a GRC maturity model for hospitals

To develop a specific maturity model for GRC in hospitals we take a systematic and design science approach and follow four steps that are based on existing approaches on how to create a maturity model [22-25]. Firstly, we define the actual purpose of the model. Secondly, the target group is identified. Thirdly, a comparison against existing related maturity models is conducted to find similarities and differences and to decide if fragments of other maturity models can be reused. Fourth and finally, a development strategy is elaborated.

3.2.1 Defining the purpose the model

In general, there are two goals when developing a maturity model: (1) to improve maturity by raising awareness and (2) to improve maturity by benchmarking across companies or industry sectors [24].

3.2.2 Defining the target group of the model

The maturity model developed in this paper is designed to be used by a target group, such as security officers, risk managers and executives of hospitals, as they are expected to have a good overview of GRC practices. In practice, more than one person will be needed to assess the maturity model for validity, reliability and generalisability. The results of the GRC model are intended to provide recommendations for the board.

3.2.3 Comparing and assessing existing maturity models

A comparison study is conducted to find differences and similarities from existing related maturity models. The differences and similarities serve as input for the strategy on how our GRC maturity model for hospitals will be developed. Structures, contents or dimensions from related maturity models are analyzed on their applicability to incorporate these in the final maturity model. In total, 16 models were selected from the literature and compared. The comparison overview is in the table. The explanation of the assessment criteria and the assessment scores can be found in the table below.

Six criteria are used to rank and compare the maturity models to apply an objective manner and to explore the best with fit with our goal and target group.

The criterion “Levels” is used to see if a model has a decent number of maturity levels. Usually, the number of level ranges between four and six [24]. A model with only one maturity level is not regarded as a maturity model. However, the content can still be useful if other criteria are met. The content of single-level maturity models can be assessed using a Likert scale. The following score system is used: If a maturity model has more than 1 level, a score of 2 is awarded.

The criterion “Dimensions” is used to see if a model uses different dimensions. Dimensions are areas to structure the field of interest, sometimes called key-process areas. A dimension can be further specified by activities, common features and measures for each maturity level. Dimensions can be one-dimensional, multi-dimensional and hierarchical. The advantage of multi-dimensional and hierarchical structures is the possibility to separate maturity assessments. Additionally it provides a more comprehensive and solid overview of the field of interest [22, 26]. The following score system is used: If a maturity model has 5 or more dimensions, a score of 2 is added.

The “Nature” of a maturity model can be descriptive or prescriptive. A descriptive model needs to propose measurement criteria for each maturity level. A prescriptive model includes everything of a descriptive model; additionally it needs to include improvement measures and to suggest actions using good or best practices [22, 23, 25]. A prescriptive maturity model

provides richer information and is thereby more desired to use as input for the maturity model to be developed. The following score system is used: If a maturity model has a prescriptive nature, a score of 2 is added.

Table. Comparison of 16 existing maturity models

Name of model and/or organization	Number of levels	Number of dimensions	Descriptive (D) or Prescriptive (P)	Addresses Governance (G), Risk (R), Compliance (C), Hospitals (H)	Has an IT focus?
AMR research	4	1	D	G R C	
IT Policy Compliance Group	5	13	P	R C	Yes
NHS Infrastructure	5	12	D	G H	Yes
CobiT 4.1	6	6	P	G	Yes
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	Yes
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	Yes
MaPSaF	5	9	P	R H	

The criterion "G R C H" is a composition of four elements: Governance, Risk Management, Compliance and Hospitals/ Health care. This criterion indicates to what extend the content of the maturity model is related to the maturity model to be developed. The following score system is used: a score of 1 is added for every element present, ranging between 0 and 4.

The criterion "Source" is used to see whether a model is objective or subjective (for example: created by a vendor to suit their product). There is no score associated with specific types of sources; rather, the criterion is there to show that the compared models come from a variety of organizations.

The criterion "IT focus" is used to see whether the model has a technological focus. IT is important in integrating Governance, Risk Management and Compliance and can be seen as an enabler. However, there are also people and processes that cannot be overlooked. Parts of maturity models with an IT focus may be used but for our maturity model, the IT focus is seen as a disadvantage. The following score system is used: If a maturity model has a focus on IT, a score of 1 is deducted.

Based on the scoring of the maturity models on these dimensions, we see that the MaPSaF model is ranked highest. This model is created by the National Primary Care Research and Development Centre of the University of Manchester. The model addresses safety of both patients and staff in health care organizations. The model uses five maturity levels and nine dimensions to describe a safety culture. The content is derived from in-depth interviews with health care professionals and managers. Some of these dimensions do not overlap with other maturity models, as the model is specifically aimed at health care settings.

Based on the previous definitions and selection, the maturity model is constructed by defining its two basic pillars, the maturity dimensions and the maturity levels.

The dimensions of the initial maturity model are based on a literature review and a comparison study. The dimensions are classified into one of the three GRC elements, *i.e.* the alignment of Governance, Risk management and Compliance. The total appropriate number of dimensions to keep the model feasible to assess is estimated to average around 20 [24, 27]. From literature, the following dimensions can be extracted:

With regard to Governance:

- Governance structure
- Whistleblower process
- Information sharing
- Patient co-determination
- Complaint handling
- Incident reporting
- Patient safety incidents

With regard to the Risk:

- Frequency of risk analysis
- Risk management awareness
- Scope of risk management
- Structure of risk management
- Risk indicators

With regard to Compliance:

- Compliance mapping
- Information security
- Compliance controls

There are two approaches to determine maturity levels: a fixed-level approach, using a fixed amount of maturity levels for every dimension to represent a maturation path, and a focus-area approach, using a variable number of maturity levels for each dimension to support differences in granularity. The fixed-level approach is suited for benchmarking and assessments and the focus-area approach is suited for incremental improvement [28]. The fixed-level approach seems to be used most often [22, 24], although it is criticized to "oversimplify" maturity levels. For the initial version of our maturity model, the common fixed-level approach was used, *i.e.* five maturity levels to describe the maturation path. To avoid over-simplifycation, the maturity model was developed flexibly with regard to the number of maturity levels. In case a dimension requires less or more levels to maintain quality, the fixed number of five maturity levels is reconsidered for that dimension. Hereby, the advantages of the focus-area approach are used to improve the fixed-level approach. A second part of determining the maturity levels are the labels. The labels need to be intuitive and need to show logical progression [24]. For the initial version of our maturity model we use five labels that were defined in the 12.1.5 OCEG Corp. Governance model, *i.e.*: forming; developing; normalizing; established; optimized.

Combining the maturity dimensions and levels defined, the resulting maturity model (version 1.0) contained 75 cells (15*5). Each cell was defined by the authors using literature. Subsequently, three Dutch senior hospital managers, active in governance, risk management or compliance with Dutch hospitals, were consulted on the first version of the maturity model. The senior managers work for different hospitals and have over 15 years of working experience as for example: (information) security officer, business continuity manager, CTO and CIO. The managers were employed at Utrecht

University MC, Rotterdam University and Eindhoven Catharina hospital. This is a limited sample, considering that the Netherlands has 91 hospital organizations in total. This selection of hospitals, however, does meet larger qualitative considerations as it includes three of the largest hospitals with a total bed capacity of 3,278, representing 12.4% of the total hospital bed in the Netherlands. A second argument is that the hospitals mentioned are known to consider GRC an issue so that useful information for the research could be expected; this is based on the contacts and information that were available. Finally, this approach offered the opportunity to conduct intensive interviews. The starting point of the three interviews was the initial version of the maturity model. The duration of the interviews was between 50 and 60 minutes, in a face-to-face setting. After every interview, the maturity model was enhanced to gradually refine and to avoid redundant comments. Overall, the interviews revealed three important common issues: a noticeable difference between the theoretical foundation and practice, a certain imbalance in the dimensions and the interviewees felt that the dimensions should be structured, if possible in a layered way. In addition to the substantive input for improving the model, the interviews made clear that hospitals do not have a settled GRC policy yet, but are working on development and (further) implementation.

The second version of the iterated and validated GRC maturity model for hospitals is presented in Figure 1.

	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 implemented.
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.

Figure 1. The GRC maturity model for hospitals

3.3 Applying the GRC maturity model for hospitals

After the maturity model was validated, a questionnaire was created as a measuring tool to actually measure the level of GRC maturity. This development process is based on Pederiva's approach [29]. The questionnaire was conducted through structured interviews with four Dutch senior hospital managers. The interviewed senior managers work for different hospitals and have over 15 years of working experience. The goal of the interviews was twofold. Firstly to check whether the questionnaire is suitable as a technique to determine GRC maturity and to see whether the questionnaire is understood and can be filled out independently. Secondly the interviews were used to actually collect and analyze hospital scores.

After the questionnaire was filled out, the maturity model was shown to the interviewees to comment and to find any minor errors or uncertainties in the maturity model.

The questionnaire was conducted in four hospitals (Eindhoven Catharina hospital, Nijmegen University MC, Nieuwegein St. Antonius and Heerlen Atrium MC). Like the iteration for the maturity model, this is a limited sample but it includes large hospitals representing 13% (3,430/26,388) of the total hospital bed capacity in the Netherlands.

Based on the questionnaire and interview data, a comparison between the four hospitals can be made as well as charts to interpret the questionnaire results and to display the alignment between the GRC elements. The questionnaire results are interpreted using four graphs. Figure 2 displays the distribution of the 14 individual dimensions. The dashed line represents the score of an average hospital, based on the four hospitals.

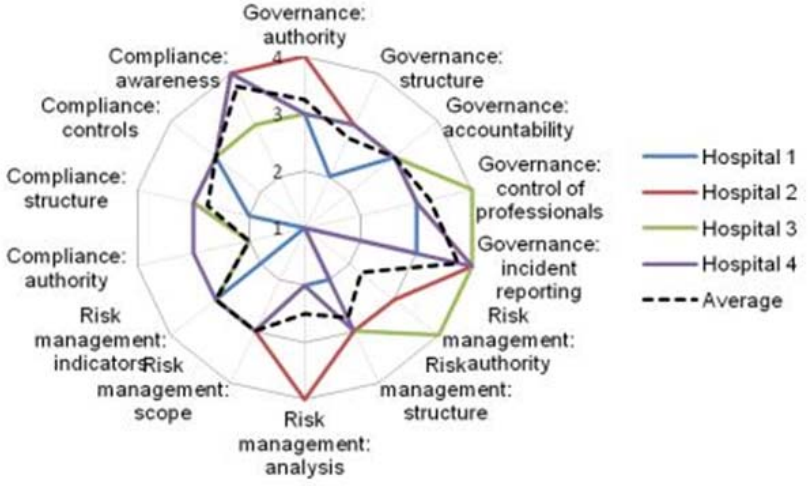

Figure 2. Results from the GRC questionnaire in four Dutch hospitals

Based on the average scores of the four hospitals, Governance scores higher than Risk Management and Compliance. This also holds for hospitals 1-3, hospital 4 scores slightly higher on Compliance than on Governance. Hospital 4 scores relatively high on the dimension "Compliance: authority" which has impact on average Compliance score. The score on "Compliance: authority" can be explained because Hospital 4 has a dedicated security officer who manages compliance. The hospital averages of the GRC element Risk Management vary quite a lot when compared to Governance and Compliance. This is mainly cause by low scores on the dimensions "Risk management: authority" and "Risk management: analysis". While the interviewees provided relatively low scores for these dimensions, they emphasized that those dimensions received increasingly attention and they acknowledged that there is room for development.

The high scores of hospital 2 on Risk Management and Compliance were explained by the interviewee. These two GRC elements received increased interest after serious problems (incompliancy) had occurred.

 ISSN 1927-6990 E-ISSN 1927-7008

4 Discussion

In this paper we showed that there are many references to GRC, but many hospitals struggle to combine these perspectives into a holistic and integrated concept. We propose a management instrument for Dutch hospitals to support them in transforming their fragmented and uncoordinated approach to risk management. The preliminary model presented in this paper is a valuable tool to monitor the GRC maturity of hospitals.

An initial version of the maturity model was based on literature and related maturity models. The model was tested and evaluated by interviewing experts working in the field, combining know-how on GRC within the context of healthcare in the Netherlands. Although the number of interviewees and applied test cases was limited, this provided important information about the applicability and opportunities for improvement of the maturity model. The need and relevance of knowledge about GRC was repeatedly emphasized. GRC certainly appears to be a key issue in the field of health care and hospital management. It therefore seems worthwhile to further enhance the model.

The primary value of our model lies in the compact presentation and its practical approach. The model consists of 14 different dimensions based on the headlines of the practice in Dutch hospitals and five levels of maturity. In so doing, the model offers insight and overview on an A4 paper format. The maturity model can guide hospitals to improve their GRC maturity, but the use of the model is not necessarily the same for each hospital. A hospital can use the model to improve their GRC maturity in an evolutionary or revolutionary way cf. [30]: through small steps, for example from the second level to the third level, or by radical fundamental changes in which one or two maturity levels are skipped. There is no generic approach; the hospital has to determine which of the approaches suits best for every single dimension. Finally, with our model, we aim to contribute to awareness in both the scientific and hospital management community. In a practical sense, our model can easily be applied as assessment-tool and presents information about possible steps for incremental improvement.

Given the limited scope of our current study, still further research on this imperative topic is necessary. A first point fort elaboration concerns the applied validation method. What could be interesting is to interview different stakeholders, such as consultants, nurses or employees from the health care inspection (*i.e.* for a balanced evaluation perspective). Secondly, different additional ways of gathering information can be used. By conducting case-studies or focus groups more interaction and criticism can lead to new perspectives and beliefs towards the maturity model and questionnaire. Thirdly, the interaction between the board and professionals in hospitals will be under more pressure due to on-going development in the Netherlands. Insurance companies can exert more power by preferring certain hospitals. This is such a perplexing relationship that it makes sense to develop a governance structure that is future-proof (taking Williamson's transaction-costing theory into account). This could then be included in the maturity model for another enhancement. Our interviewees suggested incorporating existing "accreditation" results to fill out the questionnaire and map scores of the hospital on the maturity model. This would improve the efficiency and the relevance of the model and tentatively verify our claim that increased "GRC maturity" leads to improved quality and performance of hospitals.

Furthermore, the assessment of GRC in Dutch hospitals can be addressed further in a quantitative manner using our staged-based maturity model. Interviewees repeatedly said to be interested in results of all Dutch hospitals. To quantitatively assess GRC, it is important that the measuring tool (questionnaire) measures correct variables. It is required to validate whether the questions correspond to the maturity levels. A statistical method, such as factor analysis, or path analysis (using Structural Equation Modelling, SEM) could be used to detect unknown factors that influence results. Also, the GRC maturity model can be used as a self-assessment tool. To support this application, a comprehensive roadmap (*i.e.* blueprint) with suggestions and improvement opportunities for a hospital's GRC makes sense. Interviewees indicated that information technology is an important driver of GRC; thus as enabler. An example is the registration of incidents. By registering incidents in a structured manner, electronic audit trails can be applied and issues can be investigated when necessary. Reported incidents can then be used as part of the risk analysis procedure within the hospital. Hereby, incidents and risks that do not appear in the primary care process still get attention.

Finally, we plea for a review or comparison with hospitals in other countries in terms of GRC. This would be valuable to find additional knowledge and possible best practices. A more "commercially" driven hospital market (*e.g*. the US-private hospital market) and the resulting interaction between the board and medical professionals could enhance our principal approach.

Acknowledgements

The authors are thankful to the hospital and all the interviewees for their cooperation and so made this research possible.

References

[1] Aartsen, C. van. Managers must act. ZorgVisie. 1 April 2009; 39(4).
[2] Van der Wal, G. Failure infection prevention in Maasstad hospital was culpable. Dutch Health Inspectorate. Utrecht. January 2012.
[3] Van der Elsen, W. VU Medical Centre apologieds for TV recording failure. Zorgvisie. 2011, February 23. Available from: http://www.zorgvisie.nl/Kwaliteit/13378/Excuses-VUmc-om-fout-met-tvopnames.htm
[4] Dückers, M., M. Faber, J. Cruijsberg, R. Grol, L. Schoonhoven, M. Wensing. Safety and risk management in hospitals, IQ Scientific Institute for Quality of Healthcare, Radboud University, Nijmegen Medical Center, The Health Foundation. December 2009.
[5] Van der Hoeff, N.W.Sand T.W., Van der Schaaf. Risk management in hospitals: Predicting versus reporting risks in a surgical department, Safety Management Group, Eindhoven University of Technology, Eindhoven, The Netherlands, 1995.
[6] OCEG. RIMS Enterprise Risk Management Maturity Model. November, 2006. Available from: http://www.oceg.org
[7] OCEG. Demystifying Principled Performance. GRC 360 - Perspectives on governance, risk, compliance & culture. 1 September 2007; 4-8.
[8] OCEG. GRC Capability Model. Red Book 2.0. April, 2009. Available from: http://www.oceg.org
[9] Rasmussen, M. GRC Drivers, Trends, & Market Directions. Corporate Integrity, LLC, 1-17. Magazine, 1 April 2008.
[10] Meurs, P. Health Care Governance. Commission Health Care Governance, 1 October 1999.
[11] Carroll, R. Risk Management Handbook for Health Care Organizations (4th ed.). Jossey-Bass, 2003.
[12] Van Rosmalen, A., Kastelein, E., Prinsenberg, M. Risk management in heath care organizations is developing. Vaktechnisch bulletin van PricewaterhouseCoopers Accountants. 2010; 2(17).
[13] Tarantino, A. The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices (1st ed.), Wiley, 2008. http://dx.doi.org/10.1002/9781118269213
[14] Van den Boomen, I. Good governance in health care. Ministry of Health. 2 February 2006.
[15] Brancheorganisaties Zorg (BoZ). Health care governance code. 2005.
[16] NPSA. Patient safety resources. 1 July 1 2011. Available from: http://www.nrls.npsa.nhs.uk/resources/?entryid45=59796
[17] Brancheorganisaties Zorg (BoZ). Health care governance code. 2010.
[18] Beuving, J., Van der Wal, G. Information security in hospitals not compliant. Dutch Health Inspectorate. 2008.
[19] NEN. NEN 7510 – The norm in its context. Dutch Normalisation Institute. 2005.
[20] Vrije Universiteit Amsterdam. Compliance in health care. VU, 3 December 2010.
[21] De Bruin, T., Freeze, R., Kaulkarni, U., Rosemann, M. Understanding the Main Phases of Developing a Maturity Assessment Model. Conference Paper. Available from: http://eprints.qut.edu.au/25152/
[22] Knackstedt, R., Pöppelbuß, J., Becker, J. Developing Maturity Models for IT Management – A Procedure Model and its Application. Business & Information Systems Engineering. 2011; 1(3): 213-222.
[23] Maier, A. M., Moultrie, J., Clarkson, P. J. Developing maturity grids for assessing organisational capabilities: practitioner guidance. Conference or Workshop Item. Available from: http://publications.eng.cam.ac.uk/16129/
[24] Pöppelbuß, J., Röglinger, M. 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). 2011.
[25] Lahrmann, G., Marx, F. Systematization of Maturity Model Extensions. In R. Winter, J. L. Zhao, & S. Aier (Eds.), Global Perspectives on Design Science Research. Berlin, Heidelberg: Springer Berlin Heidelberg. 2010; 6105: 522-525. Available from: http://www.springerlink.com/content/k41wt533l907mvk1/
[26] Moultrie, J. Development of a Design Audit Tool to Assess Product Design. 2004.
[27] Steenbergen van, M., Bos, R., Brinkkemper, S., Weerd van de, I., Bekkers, W. The Design of Focus Area Maturity Models. Global Perspectives on Design Science Research. 2010; 317-332.
[28] Pederiva, A. The COBIT® Maturity Model in a Vendor Evaluation Case. Information Systems Control Journal. 2003; 3: 26-29.
[29] Van de Wetering, R., R. Batenburg. Evolutionistic or Revolutionary Paths? A PACS Maturity Model for Strategic Situational Planning. International Journal of Computer Assisted Radiology and Surgery. 2010; 5(4): 401-409. PMid: 20379793. http://dx.doi.org/10.1007/s11548-010-0414-y