A Conceptual Model for Integrated Governance, Risk and Compliance

Pedro Vicente and Miguel Mira da Silva

Instituto Superior Técnico, Universidade Técnica de Lisboa,
Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt

Abstract. As integrated Governance, Risk and Compliance (GRC) becomes one of the most important business requirements in organizations, the market is incongruously struggling to satisfy organizations' needs. The absence of scientific references regarding GRC is leading to a dispersion of concepts involving this topic. Without boundaries and correct domain definition, poor implementation of GRC solutions can lead to low performances and high vulnerabilities for organizations. This paper proposes a set of high level concepts covering the GRC domain. Through literature review and framework research we propose key functions of governance, risk and compliance and their associations, resulting in a reference conceptual model for integrated GRC. The model was evaluated by comparing the GRC capability model from OCEG with a quality model evaluation framework. We concluded that the proposed model is valid and complete.

Keywords: governance, risk, compliance, conceptual model, integrated.

1 Introduction

Some research is starting to finally arise in the study of governance, risk and compliance as an integrated concept. Since PricewaterhouseCoopers introduced the term GRC in 2004 [1], a bewildering amount of definitions have been presented, distinguishing in terms of scope and levels of integration.

The first scientific definition for integrated Governance, Risk and Compliance (GRC) was proposed by Racz et al. [2] and states that: "*GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations, through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness.*"

However, if you ask 10 organizations to describe governance, risk and compliance, probably you will get at least 20 definitions [3]. Therefore, there is not a common understanding of what GRC is. Instead, there are very different perspectives [4].

Just like Enterprise Resource Planning (ERP), GRC is becoming one of the most important business requirements of an organization [5], mainly due to the

H. Mouratidis and C. Rolland (Eds.): CAiSE 2011, LNCS 6741, pp. 199–213, 2011.

rapid globalization, increasing regulations like BASEL II, the Sarbanes-Oxley Act (SOX), Anti-Money Laundering (AML), etc., and growing demands of transparency for companies [5].

Traditionally, governance, risk and compliance activities were scattered in silos all over the organization, which has a negative impact on transparency and decision making. GRC activities are important in organizations, not only to boost their performance, but above all, to protect organizations from the inside and the outside. To accomplish this objective, organizations need to shift these activities from niche groups to business units [5] in order to improve these same activities.

Although many organizations agree on the benefits that arise from integrating GRC processes, there is no congruence between software vendors, organizations and market research [4].

In this paper we use conceptual modelling to define the domain of integrated GRC. It is widely accepted that conceptual models are a prerequisite for successfully planning and designing complex systems, particularly information systems [6,7,8,9]. Over the last decades, conceptual modelling has been employed to facilitate, systematize, and aid the process of information system engineering [8].

Based on the four design artefacts produced by design science research in information systems - *constructs*, *models*, *methods* and *instantiations* - we will focus on constructs and models. Constructs are necessary to describe certain aspects of a problem domain and allow the development of the research project's terminology [10]. In other words, they provide the language in which problems and solutions are defined and communicated [11]. Models use constructs to represent a real world situation, the design problem and the solution space [12].

A conceptual reference model, a specific type of conceptual models, is a "claim that the model comprises knowledge that is useful in the design of specific solutions for a particular domain" [10]. A conceptual model is a typically graphical representation, hence can provide limited vocabulary [10], constructed by IS professionals of someone's or some group's perception of a real-world domain [13].

Conceptual modelling may be used to ease the implementation of an information system or to provide a common understating between the organization's needs and an enterprise application [13]. It is also suitable to systematize knowledge, provide guiding research and map a portion of reality [14].

In this paper, we use conceptual modelling to supply a reference model to the scientific community that can lead to a common understanding of what constitutes the universe of integrated GRC. Currently, the most complete and recognized framework for integrated GRC was developed by the "Open Compliance & Ethics Group"(OCEG). OCEG is a non-profit organization that uniquely helps other organizations to enhance corporate culture and integrate governance, risk management, and compliance processes. The GRC Capability Model [15] is the central piece of the OCEG framework and describes practices to implement and manage GRC activities.

Our approach is to design a conceptual model that contains domain level concepts, representing a high level of integration between the following sub-domains:

governance, risk management and compliance. The higher the semantic content of those concepts, the better the integration [7]. Although it may seem impossible to find general and meaningful concepts for the entire domain of integrated GRC, it is better to adopt the so-called "constructive" research strategy [7].

2 Methodology

The methodology applied is divided according to the two processes of design science research in information system, *build* and *evaluate* [16]. The build process is composed by two stages whereas and the evaluation process is composed by only one stage (Fig. 1).

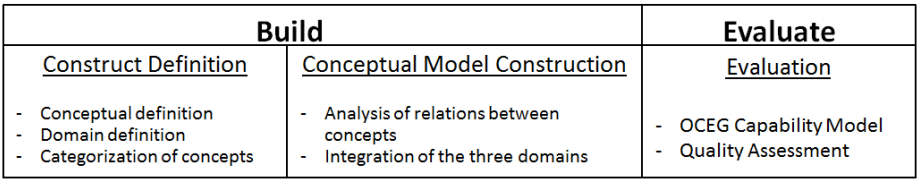

Fig. 1. Research Methodology

The first stage, construct definition, has two main milestones: conceptual domain establishment and conceptual definition within the set up boundaries established. In this stage we have proceeded with literature study and benchmarking of integrated GRC solutions in the market. Throughout it, we have come to support the observations made by Racz et al. [2]: "there is basically no scientific research on GRC as an integrated concept", "software vendors, analysts and consultancies are the main GRC publishers" and "software technology is the prevailing primary topic". Hence, gathering solid information was a hard task due to the lack of scientific research. Also, at this stage, we began to categorize the concepts that we will present in Sect. 3.

According to Hevner et al. [17], the results from this stage can be called constructs. "Constructs provide the vocabulary and symbols used to define problems and solutions" within an outlined domain. To favour the boundary definition of the domain, we used the design science research pattern proposed by Vaishnavi and Kuechler [18], *building blocks*, which consists in dividing "the given complex research problem into smaller problems that can form the building blocks for solving the original problem". Especially in this case, we divided the domain in G, R and C areas so as to simplify it and the concepts involved.

In the second stage the concepts were separated according to their most evident domain. For example, risks are more likely to belong to the risk domain (R in GRC). However, this does not imply that they could not be represented in governance and compliance domains for they might maintain relations with other concepts. One of the goals of this phase was to identify the concepts duplicated among domains. This way we could determine the integration points

between the three areas. Also, by having concepts divided into smaller domains, it became simpler to define the relations between them.

Still at this stage, three conceptual models were built, one for each area, G, R and C (Sects. 3.1, 3.2 and 3.3). In Sect. 3.4 we present the domain of integrated GRC with concepts and relations adjusted to the integrated context.

Even though little is known about how to validate conceptual models effectively and efficiently [13], in the final stage, we proceeded with the evaluation of the final conceptual model, by mapping the relations between concepts with the eight components of the GRC Capability Model presented by OCEG [15]. We used this mapping to evaluate the quality of the conceptual model according to its syntactic and semantic quality, using the Conceptual Model Quality Framework proposed by Moody et al. [19].

3 Conceptual Model

Information integration is one of the core problems in cooperative information systems [20]. Also, GRC functionalities have shown to overlap themselves [15,21] making integration difficult. Governance, risk and compliance as separate concepts are nothing new [1] and many researchers have addressed each area. The proposed model describes GRC functionalities and information that are considered to be within the scope of each of the three areas (G, R and C).

The components of the model. Before we begin describing each of the three scopes, a proper explanation concerning the model is required. The model has three types of concepts, represented by different colours and different shapes. The rectangular concepts, coloured orange, stand for what we propose to be the GRC main functionalities:

1. Audit Management
2. Policy Management
3. Issues Management
4. Risk Management

We have chosen the four functionalities for three reasons. First, a study performed by Racz et al. [4] concluded that Risk Management, Policy Management and Audit Management were mentioned seven times by GRC vendors as GRC functionalities. Issues Management was mentioned six times. Second, we decided to propose these four core functionalities to maintain the conceptual model simple without withdrawing GRC capabilities. Finally, although there are diverse opinions, the benchmarking performed supports these functionalities. The importance and role of each one will be described in the next sections.

Additionally, rectangular concepts, coloured grey (Reporting, Dashboards and Monitoring), also represent imperative functionalities to access and deliver important information in real-time through an automated manner. It is arguable that the four main functionalities presented implicitly cover reporting, dashboards and monitoring but we opted to include them since they represent essential functions for GRC to perform in an adequate, efficient and effective basis [22].

For this reason, they are explicitly represented. We have distinguished these four from the key functions, because they represent horizontal functionalities available through the three areas.

The concepts, in a blue round shape, represent information that is managed by these functionalities or are presented as a responsibility of the G, R or C areas. As stated before, G, R and C areas overlap [15,21], and some information is managed by different areas simultaneously. One way to observe the points of integration of GRC is through the information that is used collaboratively between governance, risk management and compliance.

Next, we address governance, risk and compliance separately and in more detail.

3.1 Governance

OCEG states that "governance is the culture, values, mission, structure, layers of policies, processes and measures by which organizations are directed and controlled" [15]. According to this definition, one of the most important responsibilities of governance is to determine guidelines, which are translated into policies composed by culture, values, mission, objectives and supported by procedures (see Fig. 2).

Policy Management, a key functionality, can be said to be an important activity with direct governance responsibility. Policy management must "develop, record, organize, modify, maintain, communicate, and administer organizational policies and procedures in response to new or changing requirements or principles, and correlate them to one another" [23].

Policies play an essential role at GRC, because they represent the board and top management's point of view on how the organization should be driven. It can be said that governance defines an interface, and the rest of the organization implements it to operate according with what is established. Once agreed upon, policies have to be transmitted across the organization. It is also important that they be reviewed and preserved. It is all part of the policy life cycle that must be set up (Fig. 2).

Since governance defines how the organization should perform, describing through policies what is acceptable and unacceptable, compliance is the area responsible for inspecting and proving that they are: adequate, being implement and followed. In Sect. 3.3 we will address the influence of compliance in policy management in more detail.

Governance is also responsible for risk and compliance oversight, as well as evaluating performance against enterprise objectives [21]. "The board acts as an active monitor for shareholders' and stakeholders' benefit, with the goal of Board oversight to make management accountable, and thus more effective" [15]. Accordingly, governance should be able to understand and foresee the organization's vulnerabilities and, hence make decisions to reduce them.

Also, governance should distribute power to provide insight and intelligence, at the right time, so that the right people in the management can make risk-aware decisions in accordance with key business objectives. Risk-awareness is possible

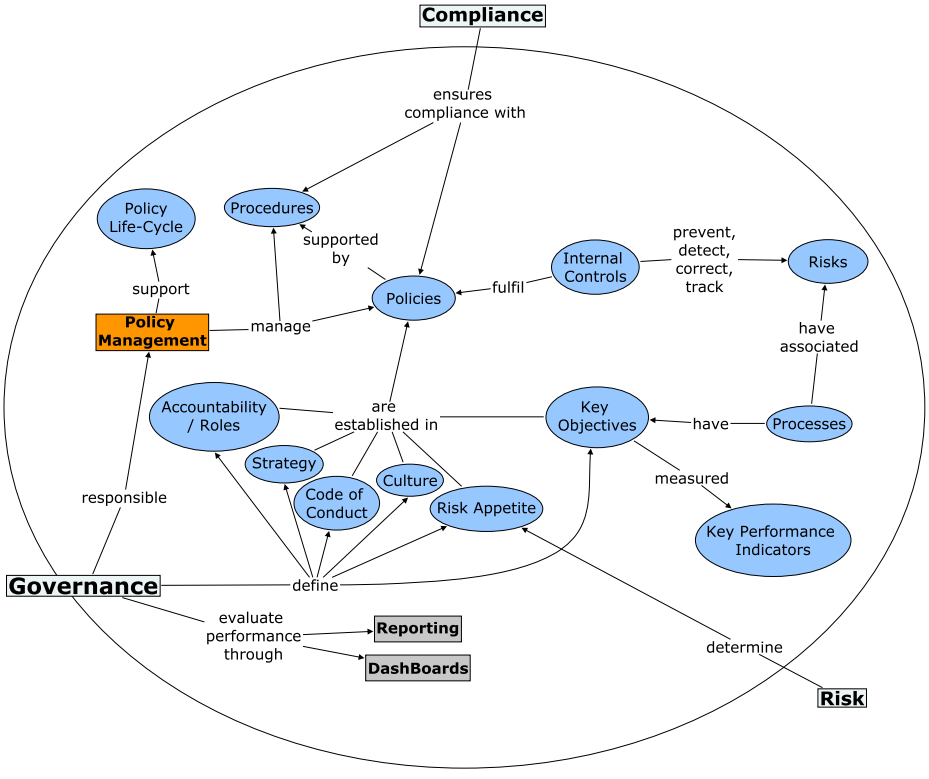

Fig. 2. Conceptual Model for Governance

through the close proximity that governance should have with risk management, which may provide very useful information in strategy setting and decision making. We will address the relation with risk management in Sect. 3.2.

Controlling the organization over intelligent, reliable and real-time information that is available through dashboards, appropriate reporting and monitoring mechanisms, provides C-level executives a paramount tool for an effective and efficient supervision of the performance of all GRC activities.

3.2 Risk Management

Risk management is more than to just identify and respond to risks. Risk management enables us to predict and avoid risk taking consequently decreasing the possibility of unexpected events to occur. A well-structured risk management must be aligned and linked with both governance and compliance information in order to attain advantages (Fig. 3).

According to OCEG [15], risk management is "the systematic application of processes and structure that enable an organization to identify, evaluate, analyse, optimize, monitor, improve, or transfer risk while communicating risk and risk

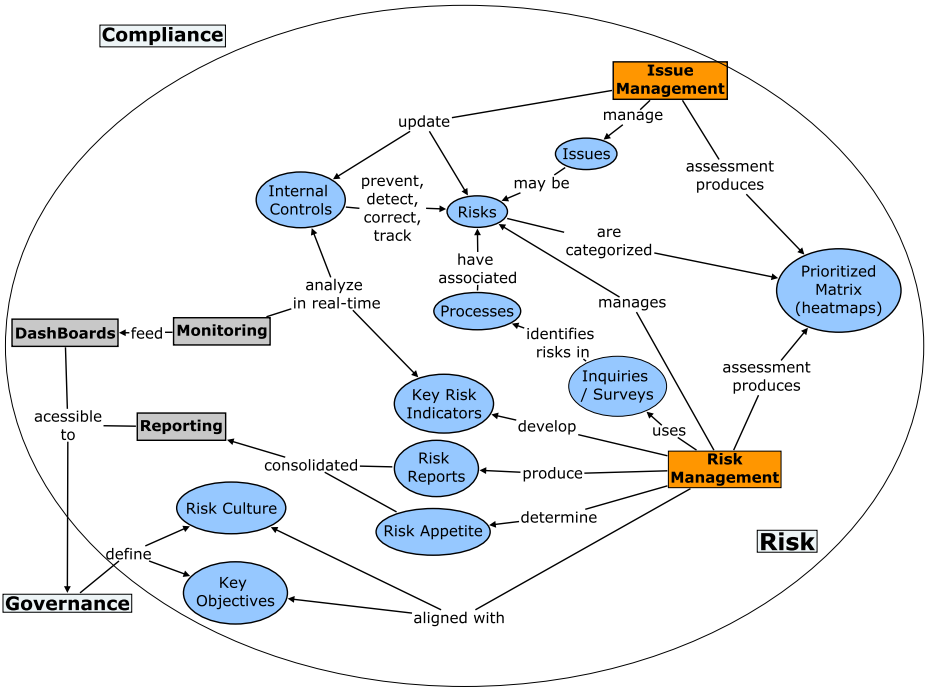

Fig. 3. Conceptual Model for Risk Management

decisions to stakeholders". A strong risk management structure can provide for a better decision making and strategy setting.

Nowadays, risk management itself cannot take full advantage of its features. It needs structured governance and compliance management in order to better align business aims with risks and assist audit management in improving controls which in turn will help detect and prevent risks. This way the organization as a whole can benefit from all risk management capabilities.

So, in order to make risk management more effective in detecting and mitigating risks that can compromise the achievement of business goals, risk identification should be based on a holistic top-down approach by aligning risk management with key corporate objectives defined by governance (see Fig. 3). This approach enables risk management to be infused into the corporate culture, quickly identifying gaps, while maintaining a proactive approach [24]. Accordingly, risk appetite must be seen as a component of both the culture and strategy of organizations.

By identifying information that is mutual or has influence between governance and risk management, we can identify several specific points of integration:

1. The defined corporate objectives should be taken into consideration in the identification of risks, adopting a top-down approach while avoiding an expensive and ineffective bottom-up approach;

2. Reporting and dashboards are also very appreciated by management, allowing for the consolidation of important information, in real-time. It also lets stakeholders reach an increased level of trust on the organization since they possess valuable and trusted information concerning the level of exposure to risks;
3. The level of risk appetite must be collaboratively defined in order to make governance and business performance more risk-aware in decision making [15].

Another important aspect that can be very helpful in risk identification is the information concerning complaints, incidents, suggestions, etc., that are reported when something happens. This we present as issues. An issue is a nonroutine stimulus that requires a response [25]. It may be positive or negative, internal or external to the organization. Issues can be risks that occur or risks that were not identified in the first place.

As risk management acts on the prediction of events, issue management identifies threats that occurred and need to be categorized and addressed. Additionally, it is in the organization's interest not only to correct what is wrong, but also to have a mechanism in place that could help improve the organization itself, for example, through suggestions from clients. By integrating this functionality in the GRC system, the information from issues management can be helpful in identifying new sources of risk and improve the activities of the organization.

Monitoring plays a crucial role on the efficiency of risk management, since it provides the capability to effectively and efficiently identify potential risks and issues. Therefore, it gives the organization the key to identify opportunities and mitigate "risks in the context of corporate strategy and performance" [24]. Internal Controls can be seen as a monitoring tool, since their role in risk management is to help prevent, detect, correct and also track risks.

Monitoring, reporting and dashboards are essential in risk and issue management because they allow organizations to answer very important questions: What are our top 10 risks? What is the percentage of issues that were identified as risks? What are the impacts of those risks and what is their status? Which risks can our organization endure? What objectives are compromised?

3.3 Compliance

Compliance must assure that the organization is following all its obligations, and thus is operating within the defined boundaries. According to OCEG, "compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies" [15]. Through this definition, the relation between governance and compliance becomes clearer.

Compliant organizations need an effective approach to verify that they are in conformity with external (standards, regulations) and internal (internal policies) rules. This approach is assisted by risk management, which must identify and

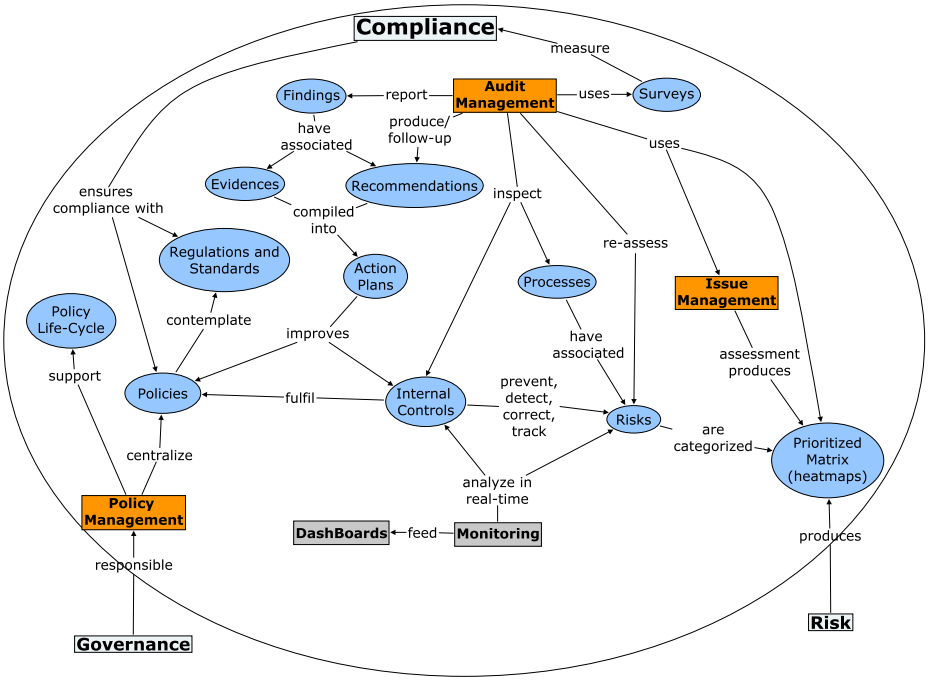

Fig. 4. Conceptual Model for Compliance

prioritize risks that are already aligned with corporate objectives defined by governance (Fig. 4).

This way, audit management, one of the key components of GRC, is responsible for auditing the processes or departments of the organization in which risks that menaced and compromised the achievement of goals were identified. By having risks aligned with objectives, audit teams can address the most important threats that place organizations' compliance under risk. Audit management is responsible for internal controls testing and policies review [22] in order to report findings and produce recommendations that will subsequently improve controls and policies (Fig. 4). Findings and issues are very similar. Organizations, therefore, need to pay close attention to them to know what needs to be fixed, who is responsible and what is the progress in accomplishing it [22].

Although audit management is very important and a crucial piece of the puzzle, it must be presented as an independent and neutral component [21], so as to preserve reliable conclusions and results that can be translated into important improvements. Consequently, compliance is responsible for defining the tactical approach that the organization should follow in order to be compliant with standards and regulations and translate it to policies and procedures. By tactical approach, we mean implementing communications so that

everyone knows about the compliance problems [21], through training, surveys and self-assessments.

This is very much related to policy management, as compliance must determine if the organization is conforming to its defined policies. If it is not, the organization must take the necessary measures to upgrade the current policies and, thus influence the policy life-cycle.

Summarizing, we can identify more relations between compliance, governance and risk areas:

1. Risk categorization is used to schedule and prioritize audits. Consequently, investigations and recommendations have an impact on risks due to the improvement of controls;
2. Policies are reviewed and improved by compliance, mirroring the impact of external regulations, standards and audits, and thus has an influence on policy management and the inherent life-cycle of policies.

Real-time monitoring also provides the opportunity to eliminate or greatly reduce sample-based audits [26]. This way, through continuous monitoring, auditors can rely in the existence of automated controls as evidence of compliance [26].

3.4 Integrated GRC Conceptual Model

In this section we present an integrated view of the three scopes presented(Fig. 5). The points of integration that we specified in each section are now combined in an integrated model. We opted not to include monitoring, dashboards and reporting to remove further complexity from the model.

As previously stated, internal controls are paramount in this model since they are crucial for governance, risk and compliance activities [15]. Controls are clearly a common thread among the GRC components (Fig. 5). An organization should, then, develop and implement adequate controls that mirror policies and procedures' objectives.

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), controls are also indispensable to achieve key business objectives through the mitigation of risks that menace the same objectives, and thus have a tremendous impact on effective risk management. Compliance manages controls through audit management, which is responsible for testing and improving controls based on findings and respective recommendations, a travail of auditors' work. By having adequate, effective and efficient controls, organizations are not only better prepared and safeguarded from external audits, but also guarantee organizations' health.

Risks and processes are also presented with a central role in integrated GRC, because they are linked to everything. In all activities, there are processes and subsequently, risks. In order to successfully and proficiently manage all GRC activities, processes must be associated with risks, and risks have to be linked with controls. This way, all information is organized, making it highly manageable and traceable.

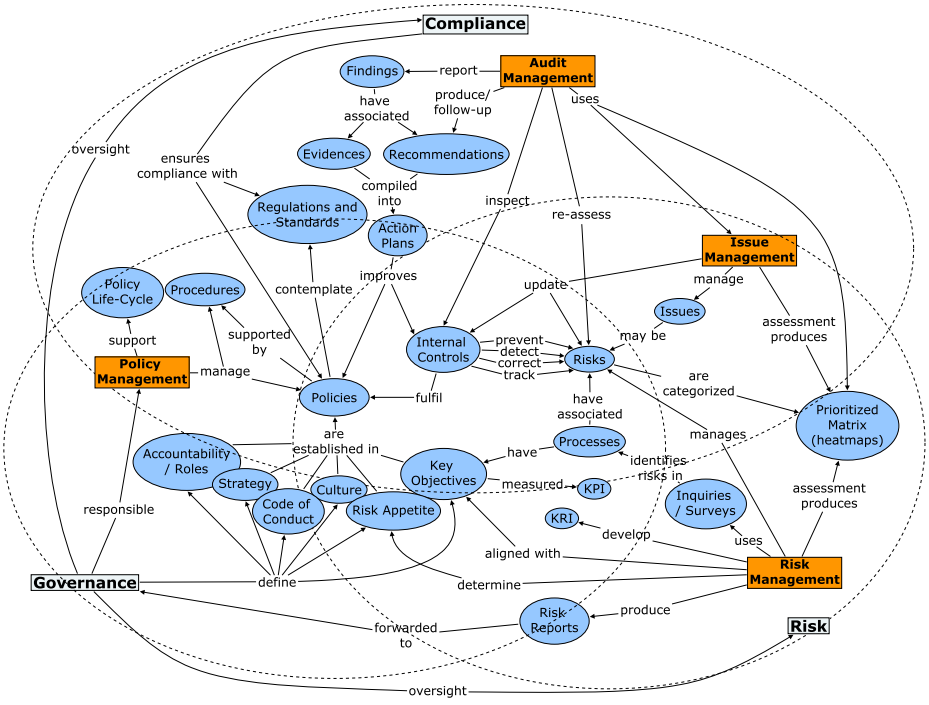

Fig. 5. Integrated GRC Conceptual Model

Finally, we opted to include policies into this crucial group that represents the integration of the three areas. On the one hand, because they are linked to controls that help ensure the fulfilment of policies, and on the other hand, because policies articulate culture and accountability at the level of governance, risk and compliance, consequently having an impact across the entire organization.

The integrated conceptual model in Fig. 5 shows the information with central roles in integrated GRC, thus it should be centralized and properly associated.

4 Evaluation

4.1 OCEG Capability Model

We opted to map the relations between the concepts of the model with OCEG Capability Model components (Fig. 6), a recognized framework that provides eight components that gather detailed practices (Fig. 7).

The components contain 32 associated elements with 132 practices. The relations that cover elements and practices of the component have been coloured with the according shade attributed to the component(Fig. 7).

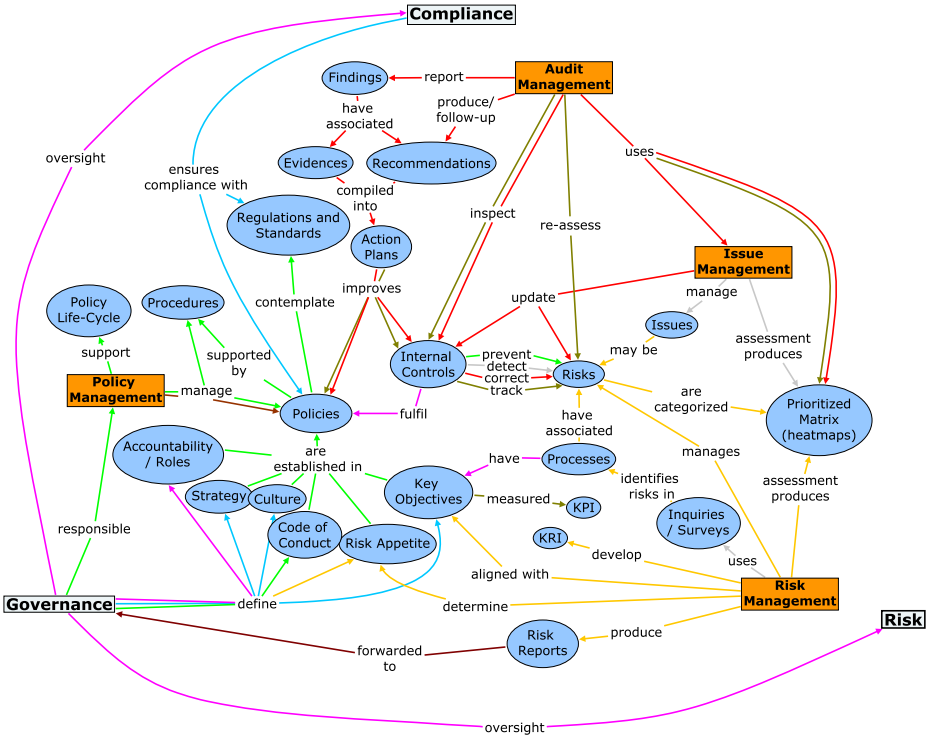

Fig. 6. Mapping between the Reference Model and the OCEG Capability Model

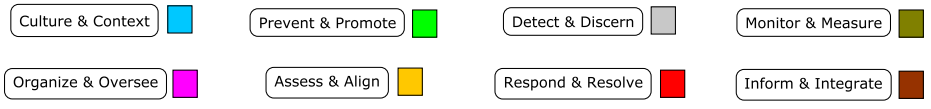

Fig. 7. GRC Capability Model Components

4.2 Conceptual Model Quality

The quality framework used to assess the conceptual model (Fig. 8) presents four components (Interpretation, Domain, Language and Model) and three quality categories (Syntactic, Semantic and Pragmatic quality) [19].

A model has syntactic correctness if there are no statements included in the model that are not a part of the language [19]. Syntactic quality is the relationship between the model and the language while semantic quality is the relationship between the model and the domain, and it is divided into two goals: Validity and Completeness. A model is valid if there are no statements in the model that are not correct and relevant about the domain [19]. A model is complete if there are no statements that are correct and relevant about the domain, but are not included in the model [19].

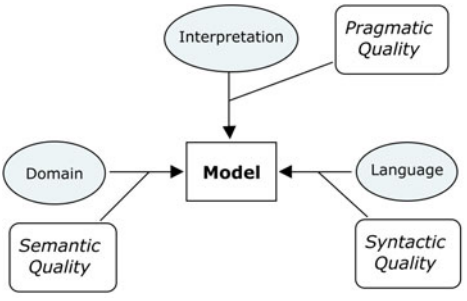

Fig. 8. Conceptual Model Quality Framework - adapted from [19]

The model presented in Fig. 6, shows that every relation is signalled with a colour, proving the validity of the model. Concerning the model's completeness, this attribute is not entirely fulfilled, because some elements of the components were not shown in the conceptual model. Since the language used to create the model was ad-hoc, we will not consider syntactic quality.

The completeness of the model can be measured by calculating the relation between the number of elements and practices covered by the conceptual model and the total number of elements and practices of the OCEG Capability Model. After an analysis of the elements presented in the capability model, we have identified 100 practices and the corresponding 24 elements that our model fulfils, with a result of approximately 76% of coverage (75,75%).

Pragmatic quality is the relationship between the model and the audience's interpretation and has not been accomplished in this research.

5 Conclusion

In this paper, we developed and evaluated a high-level conceptual model for integrated GRC and thus providing new research concerning the topic. The conceptual model was built from the integration of the three domains - governance, risk Management and compliance - but always maintaining an integrated context.

Through the identification of the concepts of each domain, the conceptual models were merged through common concepts and relations between G, R and C, resulting in a conceptual model for integrated GRC. The evaluation was performed by combining two frameworks: the OCEG capability model [15] and a conceptual model quality framework [19].

However, the evaluation is not yet complete. The pragmatic quality of the conceptual model needs to be assessed. As a future research, we will conduct surveys to obtain critical enhancements from GRC professionals in order to improve the model, and thus feed the build and evaluate loop of design science research.

Acknowledgments. We would like to acknowledge the support provided by Methodus to our research work in the scope of an innovation project partly financed by QREN.

References

1. PricewaterhouseCoopers: 8th annual global CEO survey (2004), http://www.grc-resource.com/resources/pwc_integritydrivenperformance.pdf
2. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: De Decker, B., Schaumüller-Bichl, I. (eds.) CMS 2010. LNCS, vol. 6109, pp. 106–117. Springer, Heidelberg (2010)
3. Hagerty, J., Kraus, B.: GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency (2009)
4. Racz, N., Weippl, E., Seufert, A.: Governance, Risk & Compliance (GRC) Software An Exploratory Study of Software Vendor and Market Research Perspectives. In: Proceedings of the 44th Hawaii International Conference on System Sciences (2011)
5. Gill, S., Purushottam, U.: Integrated GRC - Is your Organization Ready to Move? In: Governance, Risk and Compliance. SETLabs Briefings, PP. 37–46 (2008)
6. Moody, D.L., Shanks, G.G.: Improving the Quality of Data Models: Empirical Validation of a Quality Management Framework. Inf. Syst. 28, 619–650 (2003)
7. Frank, U.: Conceptual Modelling as the Core of the Information Systems Discipline: Perspectives and Epistemological Challenges. In: Proceedings of the Fifth America's Conference on Information Systems (AMCIS 1999), Milwaukee, Association for Information Systems, pp. 695–698 (1999)
8. Recker, J.C.: Conceptual Model Evaluation. Towards more Paradigmatic Rigor. In: Halpin, T., Siau, K., Krogstie, J. (eds.) Proceedings of the Workshop on Evaluating Modeling Methods for Systems Analysis and Design (EMMSAD 2005), Held in Conjunctiun with the 17th Conference on Advanced Information Systems (CAiSE 2005), Porto, Portugal, EU, FEUP (2005)
9. Jeusfeld, M.A., Jarke, M., Nissen, H.W., Staudt, M.: ConceptBase: Managing Conceptual Models about Information Systems. In: Bernus, P., Mertins, K., Schmidt, G. (eds.) Handbook on Architectures of Information Systems. International Handbooks Information System, pp. 273–294. Springer, Heidelberg (2006)
10. Schermann, M., Böhmann, T., Krcmar, H.: Explicating Design Theories with Conceptual Models: Towards a Theoretical Role of Reference Models. In: Becker, J., Krcmar, H., Niehaves, B. (eds.) Wissenschaftstheorie und Gestaltungsorientierte Wirtschaftsinformatik, pp. 175–194. Physica-Verlag, HD (2009)
11. Schon, D.A.: The reflective practitioner: how professionals think in action. Basic Books, New York (1983)
12. Simon, H.A.: The Sciences of the Artificial - 3rd Edition, 3rd edn. The MIT Press, Cambridge (1996)
13. Shanks, G., Tansley, E., Weber, R.: Using Ontology to Validate Conceptual Models. Commun. ACM 46, 85–89 (2003)
14. Järvelin, K., Wilson, T.D.: On Conceptual Models for Information Seeking and Retrieval Research. Information Research 9 (2003)
15. OCEG: GRC Capability Model (2009), http://www.oceg.com
16. March, S.T., Smith, G.F.: Design and natural science research on information technology. Decis. Support Syst. 15, 251–266 (1995)

17. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28, 75–106 (2004)
18. Vaishnavi, V.K., Kuechler, W.: Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 1st edn. Auerbach Publications, Boca Raton (2008)
19. Moody, D.L., Sindre, G., Brasethvik, T., Sølvberg, A.: Evaluating the Quality of Information Models: Empirical Testing of a Conceptual Model Quality Framework. In: Proceedings of the 25th International Conference on Software Engineering. ICSE 2003, pp. 295–305. IEEE Computer Society, Los Alamitos (2003)
20. Calvanese, D., de Giacomo, G., Lenzerini, M., Nardi, D., Rosati, R.: Information Integration: Conceptual Modeling and Reasoning Support. In: IFCIS International Conference on Cooperative Information Systems, P. 280 (1998)
21. Mitchell, S.L.: GRC360: A Framework to help Organisations drive Principled Performance. International Journal of Disclosure and Governance 4, 279–296 (2007)
22. Tarantino, A.: Governance, Risk and Compliance Handbook: Technology, Finance, Environmental and International Guidance and Best Practices. John Wiley & Sons, Hoboken (2008)
23. Rasmussen, M.: Defining a Policy Management Lifecycle. (2010), http://www.corp-integrity.com/compliance-management/defining-a-policy-management-lifecycle
24. Chatterjee, A., Milam, D.: Gaining Competitive Advantage from Compliance and Risk Management. In: Pantaleo, D., Pal, N. (eds.) From Strategy to Execution, pp. 167–183. Springer, Heidelberg (2008)
25. Brache, A.P.: How Organizations Work: Taking a Holistic Approach to Enterprise Health. Wiley, Chichester (2001)
26. Rasmussen, M.: Achieve GRC Value: Efficient Business Process and Application Monitoring (2010), http://www.corp-integrity.com/wp-content/uploads/2010/12/Achieve-GRC-Value-Efficient-Business-Process-and-Application-Monitoring.pdf