INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

A Reference Architecture for Integrated Governance, Risk and Compliance

Pedro Filipe Oliveira Vicente

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática e de Computadores

Júri

Presidente:	Prof. Doutor João Emílio Segurado Pavão Martins
Orientador:	Prof. Doutor Miguel Leitão Bignolas Mira da Silva
Vogais:	Dr. António Lucena de Faria
	Prof. Doutor André Ferreira Ferrão Couto e Vasconcelos

Julho 2011

Abstract

Due to increasing regulations and tight oversight from governments and financial markets, tied with the immediate need to effectively manage the increasing business and operational risks inherent to competing in a complex global market, integrated Governance, Risk and Compliance (GRC) is becoming one of the most important business requirement in organizations. Consequently, vendors are incongruously struggling to satisfy organizations' needs, that in addition to the absence of scientific references regarding GRC, is becoming a problem in this domain. The lack of guidance in this domain, namely scientific research, results in unaided attempts to improve efficiency and effectiveness in organizations. Without references and correct domain limits, poor implementations of GRC solutions can severely jeopardize organizations.

In this dissertation we propose a reference architecture covering the Governance, Risk Management and Compliance domain. Using Design Science Research, we propose two layers for the reference architecture - Business and Information Systems - that will be designed using TOGAF and ArchiMate. As a preliminary phase of our proposal, the conceptualization of the domain was accomplished. We then proposed as evaluation method, interviews with practitioners, scientific community feedback and the development of a GRC solution. The main objective was to provide a reference for a better understanding of the domain, their processes and relations, and the necessary data and applications to support them.

Keywords: governance , risk , compliance , integrated , GRC , information systems , design research

Resumo

Devido à crescente e apertada regulamentação e fiscalização por parte dos governos e dos mercados financeiros, aliado à necessidade de gerir efetivamente os riscos operacionais e de negócio inerentes a um mercado global complexo, a integraçõo de Governance, Risk and Compliance (GRC) está a tornar-se num dos requisitos de negócio mais importantes e exigentes para as organizações. Consequentemente, os fornecedoers de software debatem-se incongruentemente para satisfazer as necessidades das organizações, o que juntamente com a ausência de referências científicas sobre GRC, origina um problema neste domínio. A falta de orientação neste domínio, nomeadamente investigação científica, tem resultado em tentativas falhadas para melhorar a eficiência e eficácia nas organizações. Sem referências e limites de domínio bem definidos, implementações pobres de soluções de GRC podem comprometer gravemente as organizações.

Nesta dissertação, propomos uma arquitetura de referência que abranja o domínio de Governance, Risk and Compliance. Através de Design Science Research, propomos duas camadas para a arquitectura de referência - Negócio e Sistemas de Informação - sendo que esta será realizada usando o TOGAF e o ArchiMate. Como fase preliminar da nossa proposta, a conceptualização do domínio foi realizada. Propomos como método de avaliação, entrevistas com profissionais e especialistas em GRC, feedback da comunidade científica e a participação no desenvolvimento de uma solução de GRC. O principal objectivo desta tese é propor uma referência para uma melhor compreensão do domínio, ao nível dos seus processos e relações, e a informação e aplicações necessárias para os suportar.

Keywords: governance , risk , compliance , integrado , GRC , sistemas de informacão , design research

Acknowledgements

First of all I would like to give a special thanks to my girlfriend, Tânia Santos, who for nearly eight years has inspired, loved and supported me, since secondary school. Nothing would be the same without you.

I owe my deepest gratitude to Professor Miguel Mira da Silva. This thesis would not have been possible without his motivation, expertise and patience and it was an honour to have him as my advisor. I am also grateful for the opportunity and interest demonstrated by Dr. António Lucena de Faria, whose insight added inestimable value to this research. A deep thank to João Torrado, who has made available his support in a number of ways, from providing important connections to friendship and motivation.

I would also like to thank Nicolas Racz for the scientific support provided to this thesis.

I am indebted to my family, namely my mother and father, for their love, support and education.

It is a pleasure to thank those who participated in the interviews and group discussions, thus adding value to this thesis.

Finally, I would like to show my gratitude to my colleagues and friends, that directly or indirectly helped me during this thesis.

Acronyms

ADM	Architecture Development Method
AML	Anti-Money Laundering
CCO	Chief Compliance Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CRO	Chief Risk Officer
COSO	Committee of Sponsoring Organizations
CRUD	Create Read Update Delete
EA	Enterprise Architecture
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
GRC	Governance, Risk and Compliance
IT-GRC	Information Technology Governance, Risk and Compliance
KPI	Key Performance Indicator
KRI	Key Risk Indicator
OCEG	Open Compliance & Ethics Group
SOX	Sarbanes-Oxley Act
TOGAF	The Open Group Architecture Framework

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The business environment has been experiencing an unprecedented series of issues, surprises, and negative events that have increased the focus on the adequacy of organizations' Governance, Risk and Compliance (GRC) activities (Frigo & Anderson, 2009).

Over the last few decades, many corporate disasters adversely impacted business and rudely awakened governments to act (e.g., LTCM, Enron, Sub-prime, Societe General, WorldCom, etc.) (Tarantino, 2008). Widespread damage caused by these disasters eroded the trust government and people had in corporations, and resulted in enactment of multiple regulations such as Basel II, Sarbanes-Oxley Act (SOX), Anti-Money Laundering (AML), etc. (Gill & Purushottam, 2008; Tarantino, 2008).

Not only the government's oversight increased, but also corporations had to suffer financial losses, jail terms for executives, law suits, degradation of credit rankings and stock price drops (Gill & Purushottam, 2008). These factors impelled boards to review their governance, risk management and compliance activities to be on the right side of the law. It is arguable if more regulations means more compliance control, since non-compliance with rules and regulations has not been cited as a main reason for the financial crisis of 2007-2009. However, it has been pointed out that weaknesses in regulations were a contributing factor to the crisis (Godellawatta, 2009).

The motivation is not only legal. Integrating GRC activities also improves both effectiveness and efficiency of many internal functions of organizations, such as risk and control functions (Frigo & Anderson, 2009). In other words, a holistic and systematic approach to governance, risk and compliance leads to deeper management understanding of what is going on in a business. Such approach improves strategy setting, decision making, tracking and monitoring risks, enhance performance, improve processes and internal controls, etc. (Llanaj, 2010).

Just like Enterprise Resource Planning (ERP), GRC is becoming one of the most important business requirement of an organization (Gill & Purushottam, 2008), mainly due to the rapid globalization, increasing regulations and increasing demands of transparency for companies (Frigo & Anderson, 2009; Tarantino, 2008; Wagner & Dittmar, 2006).

A main trigger to improve GRC activities in organizations was SOX (Tarantino, 2008). The exhaustive requirements of SOX forced organizations to implement or adapt mechanisms, mainly risk, control and compliance mechanisms, to be compliant with the Act. In addition, the banking sector was addressing operational risk with its new capital adequacy accords known as Basel II.

In 2004, the first year in which SOX became mandatory, companies started throwing whatever resources they had, being people, auditors and spreadsheets, to handle the "problem". This was far from efficient. However, companies are now understanding how to transform their GRC activities from a burden into advantages (Wagner & Dittmar, 2006).

At the same time, many organizations were expanding globally and thus needed to increase their compliance budgets to address all the legal, financial and operational requirements. However, the investments used to fulfil the requirements were usually driven by specific issues (Frigo & Anderson, 2009; Tarantino, 2008), thus there was a tendency to overcome these issues from business units perspective, leading to duplication of information, activities and efforts, caused by siloed perspectives.

The acceleration of globalization exposed organizations to new risks and challenges. Globalization can be viewed as activities that increase cross-border activities such as trade, communication, treaties, travel, and compliance protocols (Tarantino, 2008), thus organizations need improved governance, risk and compliance levels to enhance their chances in the global marketplace.

More recently, the financial crisis demonstrated all the value of having an enterprise view of risks and regulations needed to address. Organizations, regulators and politicians should be more united in the objective for all companies to have an integrated and holistic system in place that crosses silos in business units.

We now present a brief description of Governance, Risk Management and Compliance definitions.

Governance

Corporate governance addresses the processes, systems, and controls by which organizations operate (Tarantino, 2008). A more concrete definition states that "governance is the culture,

values, mission, structure, layers of policies, processes and measures by which organizations are directed and controlled" (OCEG, 2009). ISO/IEC 38500 subdivides IT Governance in three main tasks: Evaluate, Direct and Monitor the implementation of plans and policies in order to meet business objectives (ISO/IEC38500, 2008).

According to the three definitions above we can affirm that one of the most important responsibilities of governance is the definition, evaluation and monitorization of guidelines, translated into policies and controls objectives that are composed by culture, values, mission, objectives supported by the processes, systems and controls.

Risk Management

Definitions of risk typically refer to the possibility of a loss or an injury created by an activity or by a person (Tarantino, 2008). Risk management seeks to identify, assess, and measure risk and then develop countermeasures to handle it, while communicating risk and risk decisions to stakeholders. This typically does not mean eliminating risk but rather seeking to mitigate and minimize the impacts.

From a GRC perspective, the most adequate notion is Enterprise Risk Management (ERM): "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004).

A well-structured risk management must be aligned and linked with both governance and compliance activities in order to attain advantages, such as better decision making and increased level of trust among stakeholders and regulatory compliance.

Compliance

Compliance means accordance not only with established laws, regulations and standards, but also with contractual obligations and internal policies (OCEG, 2009; Tarantino, 2008). Compliance must assure that the organization is following all its obligations, and thus is operating within the defined mandated and voluntary boundaries.

The myriad of activities, processes and behaviours that lay on compliance can be overwhelming. But if organizations can manage all these activities and prove it, they will operate more efficiently, compete more effectively, and build their brands and good names in the marketplace.

Governance, Risk and Compliance as separate concepts are nothing new (PricewaterhouseCoopers, 2004), but the activities of each area share a common set of information, knowledge, methodology, processes and technology. Traditional siloed GRC systems reinforced decreasing transparency, and hence governance agility, impacting effectiveness of decision making (Gill & Purushottam, 2008).

The ultimate goal is to identify, integrate and optimize processes and activities that are common across the GRC domain. For example, managing compliance initiatives separate from risk initiatives results in increased staffing requirements, complexity and costs (Banham, 2007).

To better address GRC requirements such as internal policies, external regulations and risks, a holistic view of the organizations is needed to enhance efficiency and effectiveness. This view can be accomplished by integrating certain processes and activities that are common across the GRC functions, such as risk assessments, or functions that work better together, such as agreeing on the most significant risks or compiling one consensus list of the most critical open issues across the GRC units. Also, by better sharing knowledge, data and technology, a collaborative culture in organizations is enhanced.

Investors are more interested in companies that are well governed and present a lower-risk investment. Major rating agencies (Fitch Ratings Ltd., Moody's Investors Service, and Standard & Poor's) are more focused on good governance, risk, and compliance management in their company assessments (Tarantino, 2008).

1.1 Problem

We already argued for the paramount importance of GRC activities within an organization and we also alerted for the significance of taking an integrated and holistic view of these activities, not only in an internal perspective, but also from an outward perspective.

Vendors and organizations all agree on the benefits delivered through integrated GRC. However, asking organizations to define or describe governance, risk and compliance, is getting very distinct definitions (Hagerty & Kraus, 2009; Rasmussen, 2011). There are probably as many definitions of GRC as there are companies that provide technology or professional services to address GRC challenges (Mccuaig, 2010).

The absence of references for integrated GRC is alarming. A study performed by Racz *et al.* showed that vendors' perceptions of GRC functionalities are diverse and present a low degree of congruence (Racz *et al.*, 2011). This study also showed that the scope of the existing market

research GRC frameworks (AMR, Forrester and Gartner) varies enormously. Additionally, technology architectures differ in their degree of integration. Nonetheless, vendors and organizations strongly agree on the benefits delivered through integrated GRC suites.

Disagreements and inconsistencies between vendors and organizations are not positive, but it is not an abnormal circumstance. The more alarming issue is the absence of scientific research on GRC as an integrated concept, in a market that is controlled by vendors, analysts and consultancies (Racz *et al.*, 2010c). Thus, the incongruence in this domain increased considerably and organizations may not be taking full advantage of integrated GRC systems.

Much of the problem about GRC is a lack of standardized guidance (Rasmussen, 2011). A complete reference for the GRC domain is missing; mainly, the need for a reference, non-market-driven, is paramount to make progress in this domain.

The main problem that we propose to solve can be summarized in the following sentence:

- **Organizations and vendors don't share a common understanding of the GRC domain, mainly due to the lack of scientific research references.**

In order to overcome this problem, the main objective of this thesis is to develop a reference architecture for integrated GRC, with a main focus on the context of Information Systems and aligned with processes.

A reference architecture is no more than a reference model. "A reference model is a generic abstract representation for understanding the entities and their significant relationships" in a defined domain; it defines "a common basis for understanding and explaining (at least at a high level of abstraction) the different manifestations of the paradigm" (Shen *et al.*, 2006).

In this specific case, a business reference architecture can help organizations develop and optimise their information management systems that may be more suitable than standard GRC solutions (Dameri, 2009). Also, the effort to implement and design an in-house complete enterprise architecture that supports GRC processes is, nowadays, the most suitable and supported approach to integrated GRC (Racz *et al.*, 2010a).

Architecture is positioned between business and IT (Schelp & Winter, 2009), and in the GRC domain the gap between business and IT is a major concern since vendors are very focused on standard technological solutions and business knowledge is fragmented and inconsistent (Hagerty & Kraus, 2009; Rasmussen, 2011). Having said this, a complete architecture definition is paramount to align and serve both business and IT.

1.2 Research Methodology

The research methodology that was used in this thesis is *Design Science Research*. This methodology is conducted in two complementary phases, *build* and *evaluate*. In contrast with behaviour research, design-oriented research builds a "to-be" conception and posteriorly seeks to build the system according to the defined model taking into account the restrictions and limitations (Österle *et al.*, 2011). Design science addresses research through the building and evaluation of artefacts designed to meet the identified business needs (Hevner *et al.*, 2004), instead of analysing existing information systems in order to identify causal relations (behavioural science) (Österle *et al.*, 2011).

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 (Schermann *et al.*, 2009). In other words, they provide the language in which problems and solutions are defined and communicated (Schon, 1983). Models use constructs to represent a real world situation, the design problem and the solution space (Simon, 1996).

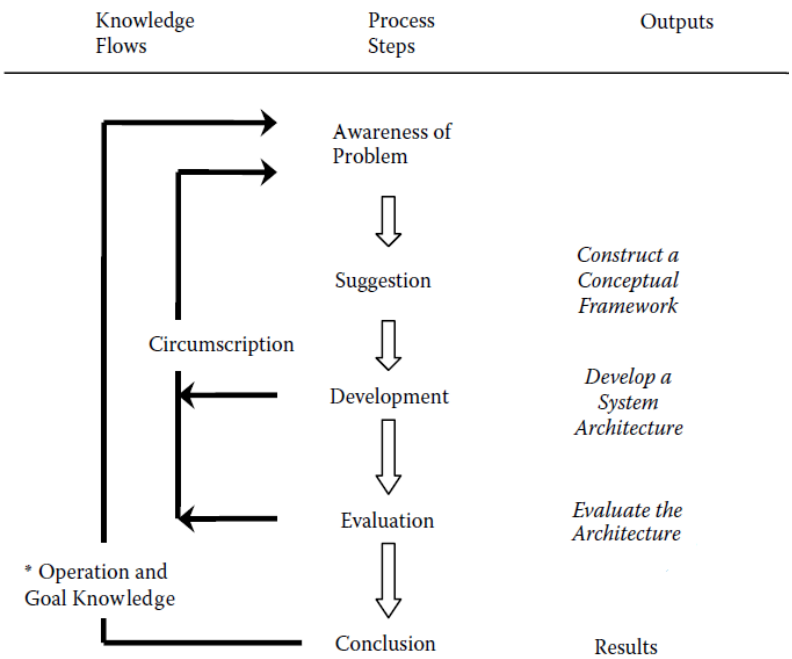

Figure 1.1: Reasoning in the Design Cycle - adapted from (Takeda *et al.*, 1990)

The research methodology cycle proposed is presented in Fig. 1.1.

In this thesis we began with literature review and benchmarking of some GRC solutions, since the "first priority for a reference model is to consolidate the most general concepts that are common to all types" (Shen *et al.*, 2006). The *Awareness of Problem* phase was already described in Sect. 1.1. Consequently we propose as hypothesis to the solution a reference architecture for integrated GRC. We began the *Development* phase with the conceptualization of the domain that we present in Sect. 3.1. Some understanding can only be gained in the act of construction or evaluation (see circumscriptum in Fig. 1.1), hence the *Awareness of Problem* and *Suggestion* can be improved during the process.

The development phase proceeded with the architecture construction, following a top-down approach using the Architecture Development Method (ADM) from The Open Group Architecture Framework (TOGAF) (The Open Group, 2009).

The utility, quality and efficacy of a design artefact must be rigorously demonstrated via well executed evaluation methods (Hevner *et al.*, 2004). For example, IT artefacts can be evaluated with metrics in terms of functionality, completeness, consistency, accuracy, performance, reliability, usability, and other relevant quality attributes (Hevner *et al.*, 2004).

A design artefact is complete and effective when satisfies the requirements and constraints of the problem that was meant to solve. In this thesis we evaluated the architecture using interviews and internet discussion groups with GRC professionals. The architecture was presented to practitioners to determine whether or not it is suitable for organizations. They evaluated functionality, completeness and consistency of the reference architecture. We also used, as an evaluation criteria the appraisal of the scientific community, through the submission of scientific publications to respected international conferences.

Additionally, we participated in a project aiming at the development of an integrated GRC application, that was supported by Methodus Inovação. This project assisted in the development and implementation of the proposed architecture, and can be seen as an instantiation of the architecture.

To complement the above mentioned criteria, we used a data model quality evaluation framework based on quality factors (Moody & Shanks, 2003) that will be described in more detail in the evaluation methodology in Chapter 4.

Österle *et al.* also point four principles that design oriented IS research must comply with, and that we followed (Österle *et al.*, 2011):

- **Abstraction.** This thesis proposes a reference architecture, hence it must be abstract in

order to be able to generalize the GRC domain. For example, the architecture should be applicable to both IT-GRC and Financial GRC.

- **Originality.** The artefact proposed is not present in the body of knowledge of the domain.
- **Justification.** The various methods proposed to evaluate the artefact should justify the artefact.
- **Benefit.** An architecture comprising the alignment of processes, application and data can assist organizations in a better understanding of the domain of GRC, and also stimulate the scientific community to research this topic.

Additionally, we followed the guidelines for design science research proposed by Hevner (Hevner *et al.*, 2004). These guidelines are: Design as an artefact; Problem relevance; Design evaluation; Research Contributions; Research rigour; Design as a search process; Communication of research.

1.3 Scientific Publications

During the execution of this thesis, two scientific papers were published in international conferences. The details of each paper and conference name and rating[1] follows:

- *A Conceptual Model for Integrated Governance, Risk and Compliance* (Vicente & Mira da Silva, 2011b) was published at the 23rd edition of CAiSE - rank A conference.
- *A Business Viewpoint for Integrated IT Governance, Risk and Compliance* (Vicente & Mira da Silva, 2011a) was published in a workshop at the 7th edition of IEEE Services 2011 - rank B conference.

Both papers describe parts from the proposal of this thesis and the full papers are present in Appendix A.

[1] source: http://www.arc.gov.au/xls/ERA2010_conference_list.xls

1.4 Thesis Structure

This document is divided in five main chapters:

1. Introduction: This chapter focuses on the general context in which the theory fits, the methodology used in the research, and the problems and objectives proposed for this thesis.
2. Related Work: The second chapter identifies and discusses artefacts (frameworks, models, methods, etc.) that address GRC as an integrated concept. Related work is divided in market and scientific research. The problem described in Sect.1.1 is supported by the related work presented. The theoretical background used in this research is presented as the guidelines and modelling tools used to develop the artefacts.
3. Proposal: Describes the conceptual model and the reference architecture using several viewpoints, representing the build phase of design science research.
4. Evaluation: Provides an analysis and discussion of the artefacts developed, including the evaluation phase of design science research.
5. Conclusion: Presents a summary of the main scientific contributions of the thesis and some proposals for future work.

Chapter 2

Related Work

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 (PricewaterhouseCoopers, 2004), a bewildering amount of definitions and frameworks have been presented, differentiating in terms of scope and levels of integration.

The objective of this Section is to describe and analyse frameworks and models that envisage GRC as an integrated domain.

2.1 Market Research

Many surveys, white papers, data sheets and reports, elaborated by vendors and market research companies, are available on-line, and provide at least some hints, instructions and guidelines for the implementation of GRC solutions. However, this type of information must be carefully and critically analysed and compared, because they provide disparate components and conclusions. For example, in Table 2.1 the differences of the functionalities from the three market research GRC frameworks are obvious.

Forrester and Gartner focuses their evaluation criteria on GRC management capabilities and AMR focuses more on GRC execution. AMR classification apparently covers more categories but we can only guess if Gartner and Forrester cover the same aspects or not.

These inconsistencies between the functional classifications may mislead vendors and organizations about the real functions and processes supported by GRC solutions.

Michael Rasmussen, an expert in GRC, proposed an Enterprise GRC Reference Architecture

Table 2.1: Comparison of market research GRC frameworks - adapted from (Racz *et al.*, 2011)

	Forrester	**AMR**	**Gartner**
GRC Management	Policy and procedure management	Risk and control framework	Policy management Compliance management
	Risk management software	Risk and control management	Risk management
	GRC management and analytics	Dashboards and reporting	
	Event and loss management		
GRC Execution	Parts of the "technical functionality" category, but no focus of the framework	Access controls	
		Identify management	
		Business processes controls	
		Audit testing	Audit management
		Data security	
GRC Application	Application for specific areas		

(Fig.2.2). The architecture presents an information architecture containing information needed for GRC activities, linking the applications that manage information.

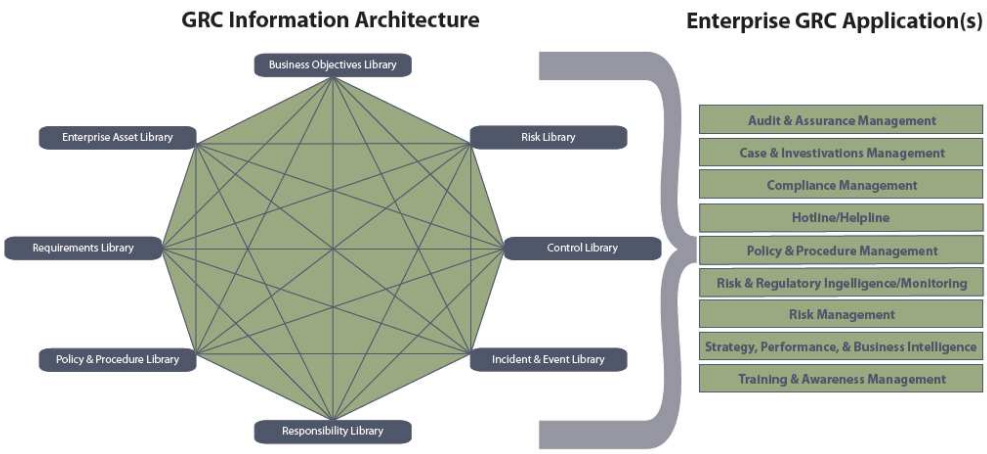

Figure 2.2: Enterprise GRC Reference Architecture (Rasmussen, 2010c)

In first place, in scientific terms, we can affirm that the architecture presented in Fig 2.2, cannot be considered as an architecture, because neither does provide scientific rigour nor a research methodology to support it. Secondly, the relations between information are somehow random, and the content of each information library listed is also unknown. Thirdly, a direct relation between the information libraries and the applications is not represented.

Nonetheless, the architecture represents the insight of an expert with plenty of experience and

that can be very useful in our research.

2.2 OCEG Framework

The most recognized framework for integrated GRC, is the “GRC Capability Model” (OCEG, 2009) from the Open Compliance & Ethics Group (OCEG).

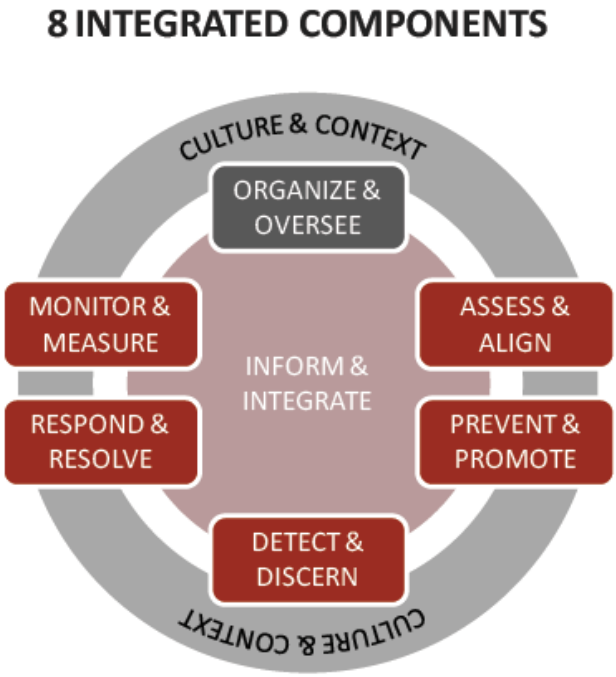

Figure 2.3: GRC Capability Model (OCEG, 2009)

OCEG is a non-profit organization that uniquely helps organizations enhance corporate culture and integrate governance, risk management, and compliance processes.

The Capability Model (see Fig. 2.3), is an exhaustive model consisting in eight components (categories) and 29 sub-elements, for each of which, core sub-practices are listed (OCEG, 2009).

The OCEG model is a very interesting reference for addressing GRC as an integrated concept. However there is not distinction between operative and management processes (Racz *et al.*, 2010b). Also, it does not explicitly denotes where the integration of governance, risk and compliance takes place. Furthermore, no mapping was done with existing standards.

A very interesting article from Mitchel (Mitchell, 2007), proposes a framework to address GRC. A meta-process is defined to comprise the GRC domain: Objective setting; Boundary identification; Risk assessment; Proactive actions; Detection and checking; Response; Evaluation;

Improvement; Communication.

While identifying these common meta-processes shared by different functional areas but with the basic operational model, the details and relations between the processes are not detailed (Racz *et al.*, 2010b).

2.3 Scientific Research

Existing publications about integrated GRC are mostly driven by software vendors, consulting and auditing companies, and market analysts. In this Section, we present some important scientific research references in the domain of GRC.

2.3.1 Frame of Reference for Research of Integrated GRC

The first scientific definition for GRC was proposed by Racz *et al.* (Racz *et al.*, 2010c) 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.*"

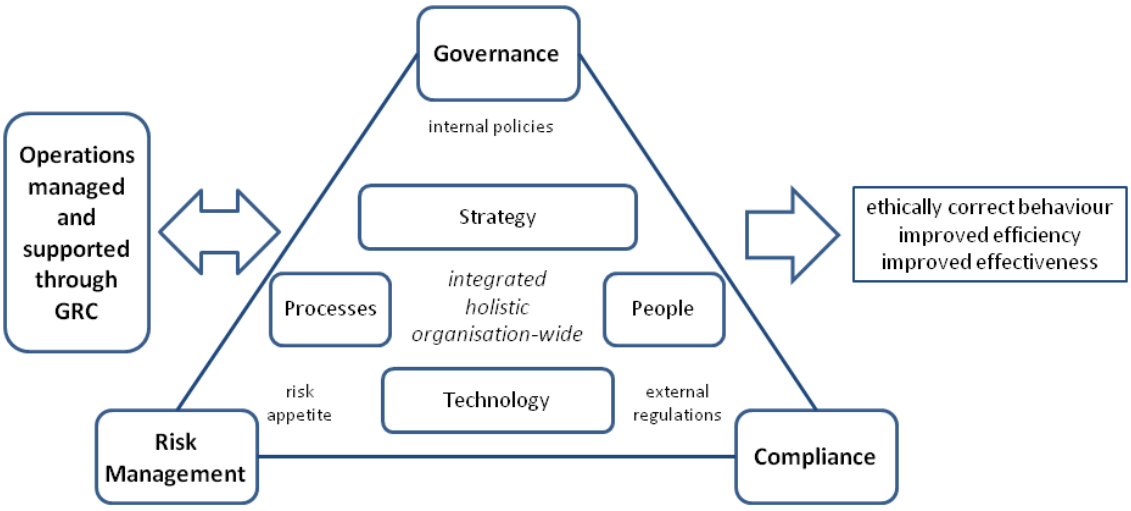

Figure 2.4: Frame of Reference for Research of Integrated GRC (Racz *et al.*, 2010c)

Racz *et al.* also defined a frame of reference for research of integrated GRC (see Fig. 2.4), that contains four components in the context of the Information Systems discipline to address

GRC: strategy, processes, technology and people. The rules of GRC are the organization's risk appetite, internal policies and external regulations.

The components and their rules have been merged in an integrated, holistic and organization-wide manner, aligned with the business operations managed and supported through GRC.

Although this frame of reference is an important initial step in scientific research, it is only a frame for research, that represents graphically the proposed definition, and not a solution. Nonetheless, approaching GRC research in accordance with strategy, processes, technology and people, is the right path to address integrated GRC.

2.3.2 Situational Method for GRC

Gericke *et al.* proposed a Situational Method Engineering for GRC Information Systems (Gericke *et al.*, 2009), identifying method fragments for GRC conceptual, strategic, organizational, technical and cultural aspects (see Table 2.2).

Table 2.2: Method Fragments Activities for the Implementation of a GRC Solution - Adapted from (Gericke *et al.*, 2009)

Method Fragments	
Conceptual	-Establish a governance management process -Establish risk management based on an enterprise architecture -Establish a compliance management process -Establish a corporate wide GRC repository -Introduce risk and regulatory intelligence
Strategic	-Assure support of top management -Develop a GRC strategy
Organizational	-Integrate the GRC solution into the planning processes -Integrate the GRC solution into the budgeting processes -Integrate the GRC solution into the reporting processes -Integrate the GRC solution into the investor relations processes -Adapt the business processes from which the GRC key figures are identified -Create and integrate new organizational units and roles
Technical	-Prepare the steps necessary to set the GRC software system into operation -Integrate the GRC software system into the IS landscape -Do a final inspection and handover the GRC software system
Cultural	-Adapt incentive systems of executives/employees -Conduct road shows -Develop a communication strategy -Provide training and education -Establish an expert team

Although the method fragments describe important activities and techniques to implement an

integrated GRC system, they are very abstract and do not specify the steps needed to maintain the GRC system. Additionally, the relations between method fragments are not explicit and the steps presented are somehow abstract. Comparatively, the OCEG Capability Model provides in much more detail, the processes and activities needed to address GRC.

Nonetheless, the aspects chosen are very important in the scope of integrated GRC and they are aligned with the components of the framework proposed by Racz *et al.* in Section 3.1 - strategy, processes, technology and people.

2.3.3 Process Model for IT-GRC

For information systems research, a subcategory of GRC is of special interest: GRC processes that support the information technology operations of an organization, commonly referred to as IT-GRC. Although this thesis focuses on the overall GRC processes and activities, there is an obvious alignment with IT-GRC.

The process model presented in Fig. 2.5 is the first model explicitly developed for IT-GRC (Racz *et al.*, 2010b). IT-GRC is best understood as a subset of GRC that supports IT operations in the same way as GRC, as a whole, supports business operations. There is a direct alignment between the IT operations and the organisation's overall strategy (Hevner *et al.*, 2004).

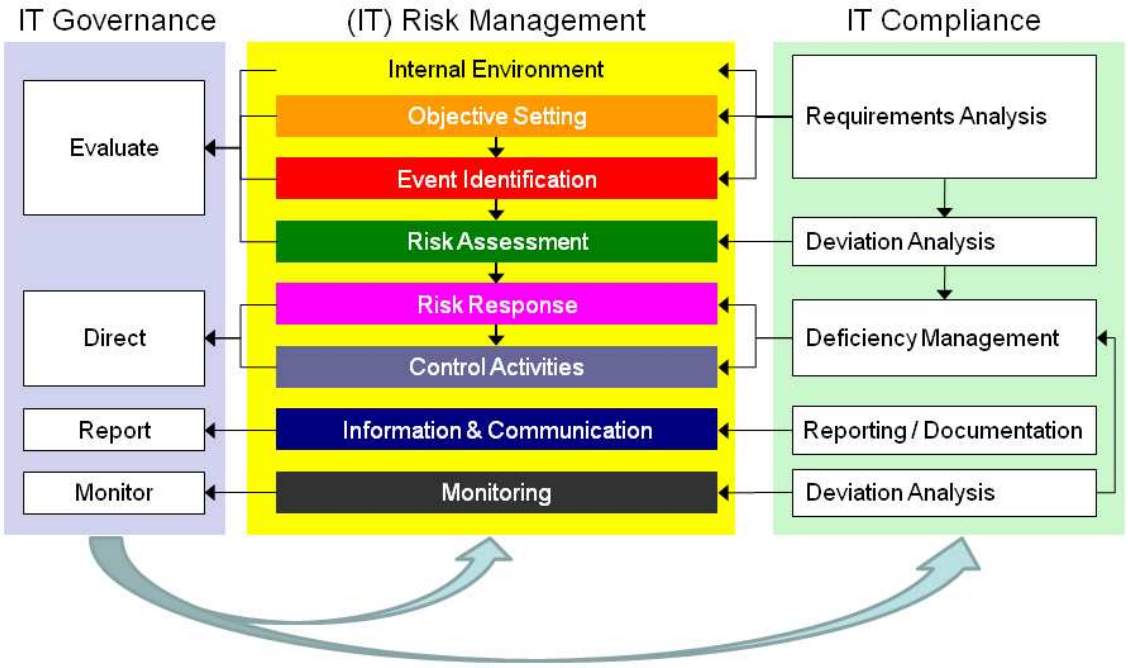

Figure 2.5: Process Model for Integrated IT GRC management (Racz *et al.*, 2010b)

Enterprise GRC is bigger than IT-GRC. Technology supports and enables enterprise GRC processes to deliver sustainability, consistency, efficiency, and transparency. Technology is important in all the domains of GRC. The GRC concerns that fall on the shoulders of the IT department - security, disaster recovery, IT governance, IT risk, IT compliance, are IT-GRC concerns.

Some of these concerns are very specific of IT, but IT-GRC processes are very similar and mutual to the overall GRC processes. The processes are presented in Fig. 2.5.

For example, the IT Risk Management components in Fig. 2.5, were based on the ERM framework from the Committee of Sponsoring Organizations (COSO). According to the COSO ERM definition, ERM fits in the entire organization, including IT.

The Compliance components presented in Fig. 2.5 are also non-IT specific (Racz *et al.*, 2010b).

Regarding IT Governance, the components are more specific of IT, and the components are referenced from the ISO/IEC 38500:2008 (ISO/IEC38500, 2008). IT governance enables the enterprise to take full advantage of its information, and can be seen as a driver for corporate governance. Therefore, IT governance and corporate governance are not distinct disciplines and IT governance needs to be integrated into the overall governance structure.

In short, the process model in Fig. 2.5, is a very important artefact to define and identify the relations between the GRC processes. However, the selection of frameworks and standards could be different, that would lead to changes in the process model presented. Also there is a lack of structure in the process, and the model has not been demonstrated in terms of its applicability (Racz *et al.*, 2010b).

2.3.4 Conclusion

Through this research stage, we have come to support observations made by Racz *et al.* (Racz *et al.*, 2010c), in which it is stated that “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”. Therefore, gathering solid and valid information was a hard task due to the lack of scientific research.

This Section proves the two sentences of the problem that this thesis addresses. First, organizations and vendors don’t share a common understanding of the GRC domain. Second, there is indeed a lack of scientific research references in GRC.

2.4 Theoretical Background

In this Section we present theory, concepts and tools used to conduct this research, namely Enterprise Architecture, TOGAF and ArchiMate.

2.4.1 Enterprise Architectures and Reference Architectures

Enterprise Architecture (EA) is a holistic approach to systems architecture (Zachman, 1987) with the purposes of modelling the role of information systems and technology on the organization, aligning business processes and information with information systems, among others. Hence, it covers several layers of the organization.

The concept of architecture is defined as “the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution” (IEEE, 2000). According with the same source, a reference architecture is a way of recording a specific body of knowledge to address a problem, thus making it available for further practical reuse. Their purpose is to form a starting point for architectural development. Reference architectures describe one or more architecture building blocks for architectures in a particular domain.

A more specific definition states that a “reference architecture is a generic model that can be used as basis for building a more specialized architectural model. Reference architecture is represented in the same way as the resulting individual architecture” (Halttunen, 2004). In the context of enterprise modelling, reference architecture describes the features that are common to a set of concepts of the same domain.

Based on these descriptions, it is our belief that a reference model representing an architecture, suits well the objectives of this research.

2.4.2 TOGAF

TOGAF is a high-profile EA - with a detailed method and a set of supporting tools - for developing an enterprise architecture. The core of TOGAF is the ADM (see Fig. 2.6). The highlighted steps are the ones that were accomplished in this thesis.

There are four architecture domains that are commonly accepted as subsets of an overall EA, all of which TOGAF is designed to support, plus two introductory phases:

- **Preliminary Phase** in which the context, relevant guidelines and standards and the goals

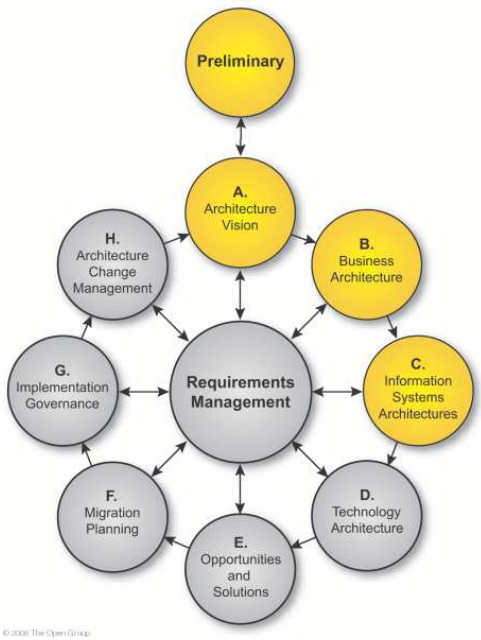

Figure 2.6: Selected Phases of the TOGAF Architecture Development Method (ADM) (The Open Group, 2009)

of the architecture process are identified.

- **Architecture Vision - Phase A** in which the main process begins with the elaboration of an architecture vision and the principles that should guide the architecture. This provides the basis for developing the business architecture, information systems architecture, and technology architecture.
- **Business Architecture - Phase B** defines the business strategy, governance, organization, and key business processes.
- **Data Architecture - Phase C** describes the structure of an organization's logical and physical data assets and data management resources.
- **Application Architecture - Phase C** provides a blueprint for the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the organization.
- **Technology Architecture - Phase D** describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc.

This method provides enough guidance and concepts to achieve the ultimate goal of this research. We chose not to include Phase D in the scope of this thesis due to the minor significance it provides to a reference architecture in this domain.

2.4.3 ArchiMate

In addition, a high-level modelling language is needed to describe the architecture. Complementing TOGAF with ArchiMate is a valid choice, since it represents a standard language and vendor-independent concepts (Lankhorst & van Drunen, 2007).

The three main layers of ArchiMate are:

- **Business layer** about business processes, services, functions and events of business units.
- **Application layer** supports the business layer with application services which are realised by (software) application components.
- **Technology layer** offers infrastructural services needed to run applications, realised by computer and communication devices and system software.

The selected concepts from ArchiMate are present in Fig. 2.7. Additionally, some viewpoints (not all) proposed to accomplished in this research were added. A brief description of the elements follows (Iacob *et al.*, 2009).

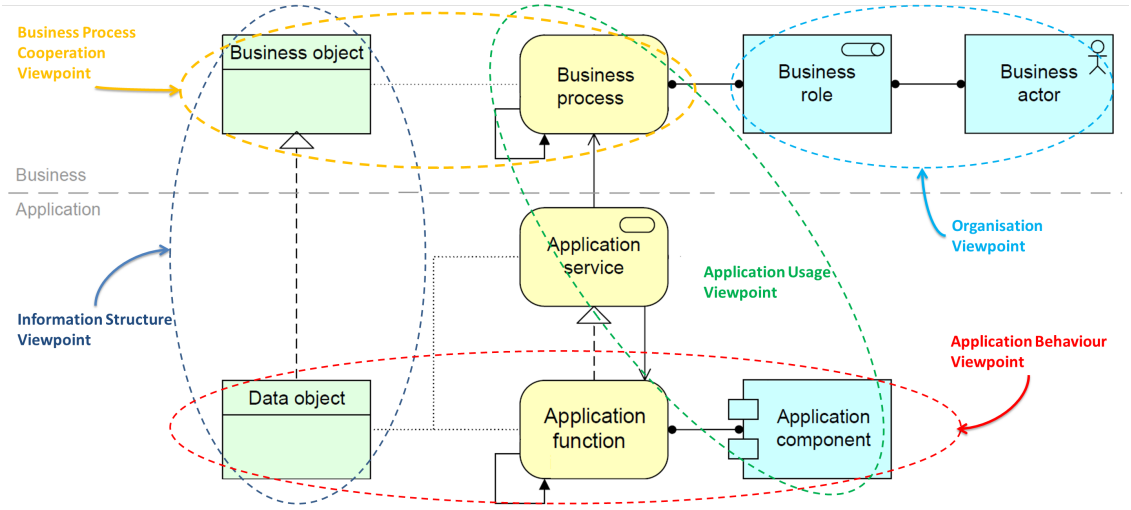

Figure 2.7: Selected concepts and viewpoint examples from ArchiMate (Iacob *et al.*, 2009)

Business Role: A business role is defined as a named specific behaviour of a business actor participating in a particular context.

Business Actor: A business actor is defined as an organizational entity capable of (actively) performing behaviour. A business actor performs the behaviour assigned to (one or more) business roles.

Business Process: A business process describes the internal behaviour performed by a business role that is required to achieve certain objectives.

Business Object: A business object is defined as a unit of information that has relevance from a business perspective. A business object may be accessed (e.g., created, read, written) by behavioural element.

Data Objects: A data object is defined as a coherent, self-contained piece of information suitable for automated processing. It should be a useful, self-contained piece of information with a clear meaning to the business, not just to the application level.

Application Services: An application service is defined as an externally visible unit of functionality, provided by one or more components, meaningful to the environment. An application service is realized by one or more application functions that are performed by the component. It may require, use, and produce data objects.

Application Components: An application component is defined as a modular, deployable, and replaceable part of a system. It performs one or more application functions.

Application Functions: An application function is defined as a representation of a coherent group of internal behaviour of an application component. An application function abstracts from the way it is implemented. Only the necessary behaviour is specified. It may realize application services and use application services realized by other application functions.

We will use viewpoints to represent the concepts in isolation, and for relating two or more concepts. Viewpoints define abstractions on the set of models representing the enterprise architecture, each aimed at particular set of concerns (Iacob *et al.*, 2009).

2.4.4 Conclusion

Using the structure of the ArchiMate language has its advantages, because the structure of ArchiMate neatly corresponds with the three main architectural domains of TOGAF (Iacob *et al.*, 2009). Due to the broader scope of TOGAF, some viewpoints are not matched. TOGAF addresses more

high-level strategic issues and the lower-level engineering aspects of system development. ArchiMate is limited to the enterprise architecture level of abstraction (Iacob *et al.*, 2009; Lankhorst & van Drunen, 2007).

Although there is no one-to-one mapping between ArchiMate and TOGAF, there is a fair amount of correspondence, and the both methods address approximately the same issues (Lankhorst & van Drunen, 2007), because ArchiMate primarily covers the building blocks associated with Phases B, C and D (see Fig. 2.6) of the TOGAF ADM (Jonkers *et al.*, 2009).

As may be noticeable in Fig. 2.6, the technology architecture (Phase D) was not accomplished in this research, since it does not add value for the objectives of this thesis.

Additionally, we concluded that the concepts of enterprise architecture and reference models supply an adequate theoretical foundation for the main contributions that this research proposes.

Chapter 3

Proposal

In order to address the problem described in Sect. 1.1, the proposal of this thesis is a reference architecture that describes the integration of GRC processes and the necessary data and applications to support them.

As stated in Sect. 1.2 this research is based on design science research, and the artefacts produced are focused on constructs and models. This chapter corresponds to the development or build phase of the methodology proposed.

Following the TOGAF ADM, we will first point out the main objectives and scope of the architecture, followed by the proposed architectural layers - Business and Information Systems. In each section we present the constructed artefacts in the form of viewpoints selected from the ArchiMate structure.

3.1 Preliminary and Architecture Vision

The Preliminary phase of the ADM consists of the preparation and initiation of the architectural activities and includes the analysis of key references in order to create a general understanding of the domain, by reconciling and harmonizing concepts and terminology from different sources.

From the architecture vision phase, the definition of the GRC scope was designed. The next section describes the output from this phase: a conceptual model that represents a solution concept diagram which provides “a high-level orientation of the solution that is envisaged in order to meet the objectives of the architecture engagement” (The Open Group, 2009). ArchiMate was not used in this phase.

3.1.1 Conceptual Model

After a careful and rigorous study of integrated GRC, we designed a conceptual model to translate the analysis of the domain and thus define the borders of GRC (Vicente & Mira da Silva, 2011b). A conceptual model is a representation, typically graphical, hence can provide limited vocabulary (Schermann *et al.*, 2009), constructed by IS professionals of someone's or some group's perception of a real-world domain (Shanks *et al.*, 2003).

In this section we describe only the proposed conceptualization, but a complete description can be found in the Appendix Section.

In order to favour the boundary definition of the domain, we used a design science research pattern proposed by Vaishanavi and Kuechler (Vaishnavi & Kuechler, 2008), *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". In this case particularly, we subdivided the domain in G, R and C areas, with the purpose of simplifying the domain and the concepts involved.

Components of the model

The model presents three types of concepts, represented by different colour and different shape concepts. Concepts with orange colour stand for GRC main functions which are:

- Audit Management
- Policy Management
- Issue Management
- Risk Management

We have chosen these four main functions for three reasons. First, a study performed by Racz *et al.* (Racz *et al.*, 2011) concluded that Risk Management, Policy Management and Audit Management were mentioned seven times by GRC vendors as a GRC functionality. Issue Management was mentioned six times. The second reason to support this decision is a Gartner report that describes three of these four key functions for Enterprise GRC, used to evaluate market products (Audit, Policy and Risk Management). Finally, we opted to present these four core functionalities to maintain the conceptual model simple without withdraw GRC capabilities. The importance and role of each one will be described in the next sections.

The round concepts coloured with blue represent information that is managed by these functionalities or are presented as a responsibility of the G, R or C areas. G, R and C areas overlap themselves (Mitchell, 2007; OCEG, 2009), 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 and compliance.

Reporting, Dashboards and Monitoring represent imperative functionalities to access and deliver important information in real-time through an automated manner. They are essential functionalities for GRC to behave in an adequate, efficient and effective basis. We have distinguished them from the key functionalities, because they represent horizontal functionalities, available through the three areas. However, we opted not to include these functionalities to remove complexity from the model (see Fig. 3.8).

3.1.1.1 Integrated GRC Conceptual Model

In this section we present the integration result of Governance, Risk Management and Compliance (Fig. 3.8), along with a brief description of the constructed model.

Governance

Policy Management, a key functionality, can be said to be one important activity with direct responsibility of governance. Policy management is responsible to "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" (Rasmussen, 2010b).

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

Governance is also responsible for risk and compliance oversight, as well as evaluating performance against enterprise objectives (Mitchell, 2007). "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" (OCEG, 2009). Accordingly, governance should be able to understand and foresee the organization vulnerabilities and thus take decisions to reduce them.

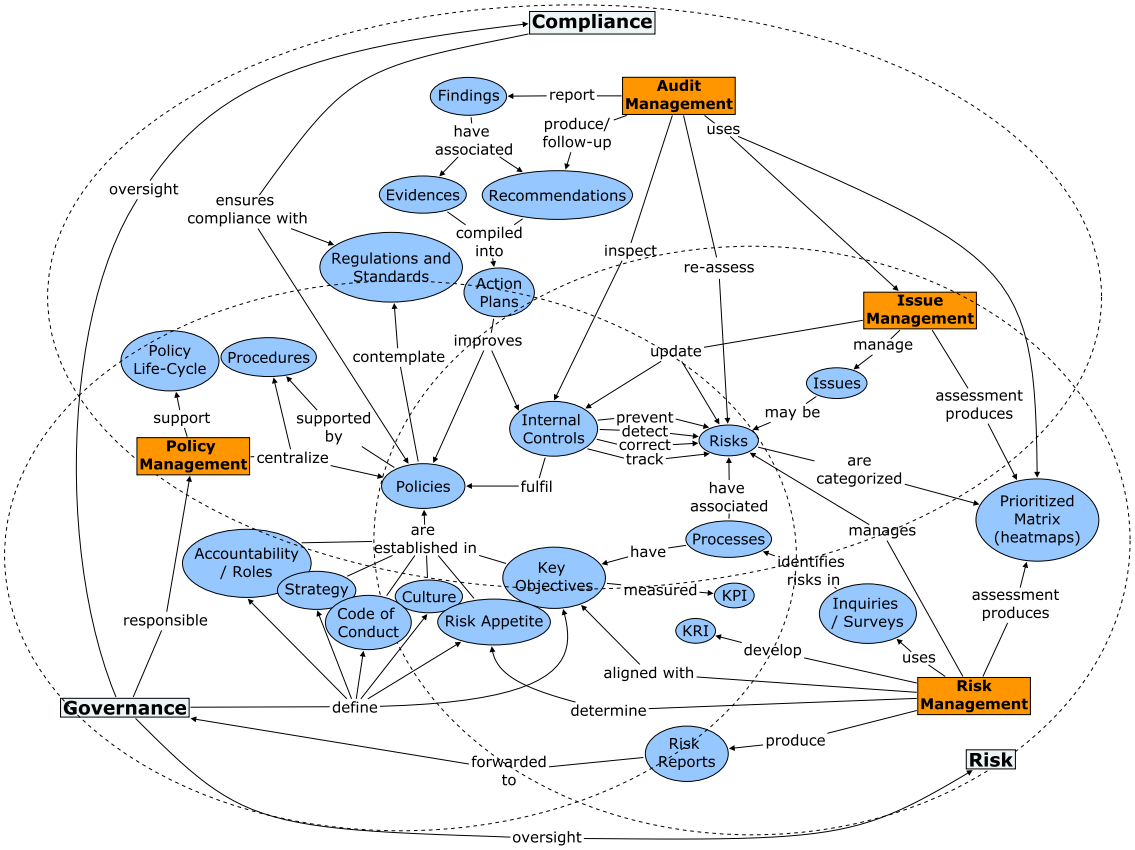

Figure 3.8: Integrated GRC Conceptual Model (Vicente & Mira da Silva, 2011b)

Also, governance should distribute power to provide insight and intelligence to the right people in management, at the right time, to make risk-aware decisions in accordance with key business objectives. Risk-awareness is possible through the close proximity that governance should achieve with risk management, that can provide very useful information in strategy setting and decision making.

Risk Management

Risk management cannot take full advantage of its features without structured compliance management and governance in order to better align business objectives with risks and assist audit management in improving controls, which in turn will help detect and prevent risks. This way the entire organization can benefit from all risk management capabilities.

More specifically, in order to make risk management more effective in detecting and mitigating risks that can compromise the achievement of business objectives, risk identification should be

based on a holistic top-down approach by aligning risk management with key corporate objectives defined by governance (see Fig. 3.8). This approach enables risk management to become infused into the corporate culture, quickly identifying gaps, while maintaining a proactive approach (Chatterjee & Milam, 2008). Accordingly, risk appetite must be seen as a component of both culture and strategy of organizations.

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

- 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;
- Reporting and dashboards are also very appreciated by management, allowing consolidation in real-time of important information. It allows stakeholders to get an increased level of trust on the organization since they possess valuable and trusted information concerning the level of exposure to risks of the organization;
- The level of risk appetite must be collaboratively defined, in order to make governance and business performance more risk-aware in decision making (OCEG, 2009).

Another important aspect that can be very helpful in risk identification is the information concerning complaints, incidents, suggestions, etc. that are reported when something happened, that we present as issues. An issue is a nonroutine stimulus that requires a response (Brache, 2001). It may be positive or negative, internal or external to the organization. Issues can be risks that occur or risks that weren't 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 from the interest of the organization not only to correct what is wrong, but also to have in place a mechanism 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 risks and improve the activities of the organization.

Compliance

Since governance defines how the organization should behave, describing through policies what is acceptable and unacceptable, compliance is the area responsible for inspecting and proving that they are implemented, adequate and being followed.

Compliant organizations need an effective approach to verify that they are in compliance with external (standards, regulations) and internal rules (internal policies). This approach is assisted by risk management, which role is to identify and prioritize risks that are already aligned with corporate objectives defined by governance (Fig. 3.8).

This way, audit management, one of the key components of GRC, is responsible for auditing the processes or departments of the organization in which were identified risks that menace and compromise the achievement of objectives. By having risks aligned with objectives, audit teams can address the most important risks that place organizations' compliance under menace.

Audit management is responsible for internal controls testing and policies review (Tarantino, 2008) in order to report findings and produce recommendations that will posteriorly improve controls and policies (Fig. 3.8). Findings and issues are very similar. Organizations need to pay close attention to findings and issues to know what needs to be fixed, who is responsible and what is the progress in accomplishing it (Tarantino, 2008).

Although audit management is very important and a crucial piece of the puzzle, it must be presented as an independent and neutral component (Mitchell, 2007), in order to preserve reliable conclusions and results that can be translated in important improvements for the organization. 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. Giving an example of tactical approach, we mean implementing communications so that everyone knows about the compliance problems (Mitchell, 2007), through training, surveys and self-assessments.

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

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

- Risk categorization is used to schedule and prioritize audits. Subsequently, investigations and recommendations, have an impact on risks due to the improvement of controls;
- 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.

3.1.1.2 The Core of GRC

According to COSO, controls are indispensable to achieve key business objectives through the mitigation of risks that menace the same objectives, and thus have a tremendous impact in effective risk management. Compliance manages controls through audit management, that is responsible for testing and improving controls based on findings and respective recommendations, travail of auditors work.

Figure 3.9: GRC Information Core

By having adequate, effective and efficient controls, organizations not only are better prepared and safeguarded from external audits, but also guarantee organizations' healthiness.

Internal controls are paramount in this model, since they are crucial for governance, risk and compliance activities (OCEG, 2009). Controls are clearly a common thread among the GRC components (Fig. 3.8), and an organization should develop adequate controls that mirror objectives from policies and procedures.

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, thus giving the organization the key for identifying opportunities and mitigating "risks in the context of corporate strategy and

performance" (Chatterjee & Milam, 2008). 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.

Real-time monitoring also provides the possibility to eliminate or greatly reduce sample-based audits. This way, through continuously monitoring, auditors can rely in the existence of automated controls as evidence of compliance (Rasmussen, 2010a).

Risks and processes are also presented with a central role in integrated GRC (Fig. 3.9), because they are linked to everything. In all activities, there are processes and subsequently, risks. In order to manage effectively and efficiently all GRC activities, processes must be associated with risks, and risks must be linked with controls. This way, all information is organized, thus making it highly manageable and traceable.

Finally, we opted to include policies into this crucial group (see Fig. 3.9), not only because they are linked to controls that help ensure the fulfilment of policies, but also because policies articulate culture and accountability at the level of governance, risk and compliance, and thus have an impact across the entire organization.

The integrated conceptual model in Fig. 3.8 shows the information with central roles in integrated GRC, thus it should be centralized and properly associated to improve the efficiency and effectiveness of governance, risk management and compliance activities.

Establishing a common, integrated discipline around policies, risks, controls, and processes, organizations can replicate improvements in one GRC area across other GRC areas with the overall goal of uncovering business advantage and driving shareholder value. The result should be fewer avoidable loss events and failures and a lower overall cost of control (Mccuaig, 2010).

3.2 Business Architecture

The business architecture was not developed entirely from scratch. We used the process model for ITGRC (Racz *et al.*, 2010b) that was presented in Sect. 2.3.3. A deep analysis was made in order to figure out if the process model could be adapted to the scope of this research. The authors concluded affirmatively. Recent research showed that both the process model and the conceptual model (see Sect. 3.1.1) are aligned and complement each other (Vicente & Mira da Silva, 2011a). Additionally, the reuse of design research artefacts has been supported in scientific research (Aier & Gleichauf, 2010; Brocke & Buddendick, 2006).

Nonetheless, the process model was analysed. For example, the Risk Management macro-processes include the components from the COSO ERM (COSO, 2004). However, there are

more frameworks and standards that could have been used, namely ISO 31000:2009 (ISO31000, 2009), CMMI (Software Engineering Institute,, 2010), PMI:PMBOK (PMI, 2004), Risk IT (Information Systems Audit and Control Association, , 2009), etc. An analysis to these frameworks was made, and we concluded that all of them were quite similar and aligned, hence we opted not to modify the risk management processes.

Concerning the compliance processes other literature was analysed (El Kharbili *et al.*, 2008; Namiri & Stojanovic, 2007; Schumm *et al.*, 2010) besides the one proposed on the process model (Rath & Sponholz, 2009). We concluded that the compliance processes presented in the process model were generic and did fit with the remaining frameworks analysed. Another point in favour lies in the fact that the processes are non IT-specific.

We also chose to maintain the governance processes (ISO/IEC38500, 2008) for three reasons. According to the authors know-how, we argue that although those processes are directed to IT, they are applicable in this domain. Like virtually all ISO standards, the ISO/IEC 38500 follows the Deming cycle, which also applies in the role of governance in integrated GRC. Finally, since we decided to maintain Risk Management and Compliance intact, we opted not to distort the already integrated process model.

We now present the viewpoints selected from ArchiMate to model the business architecture.

- Organisation Viewpoint (Sect. 3.2.1);
- Business Process Viewpoints (Sect. 3.2.2);
- Business Process Cooperation Viewpoint (Sect. 3.2.3);
- Information Structure Viewpoint (Sect. 3.2.4);

3.2.1 Organization Viewpoint

The organisation viewpoint is typically used to identify authority, competencies, and responsibilities within an organisation, using actors and their respective roles.

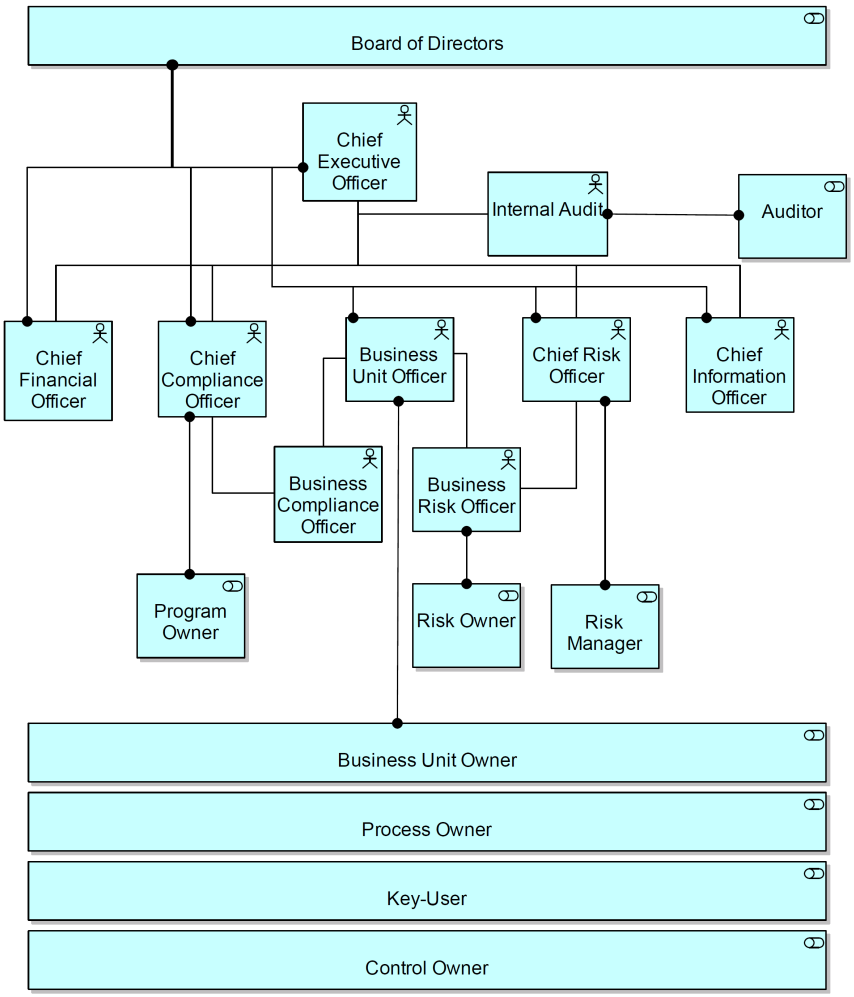

Figure 3.10: Organisation Viewpoint

The viewpoint represented in Fig. 3.10 is not specific for the GRC domain. It simple illustrates an example organizational structure for an organization and it was adapted from (Moerdler *et al.*, 2009). It is also worthwhile saying that at this level of abstraction, it is difficult to elaborate a list of roles and actors to assign to processes, and the most likely outcome should be too much roles assigned to several processes (and vice versa). Nevertheless, the correct definition of roles in organizations is very important, because actors are the main enablers of processes.

In this example, an organization has a Chief Executive Officer (CEO) that oversees all of organization's activities and business departments. The C-suite is usually formed by a Chief Financial Officer (CFO), that oversees the organization from a a financial perspective, a Chief Compliance Officer (CCO) who oversees the organization from a compliance perspective, a Chief Risk Officer (CRO) who oversees all organization's activities from a risk management perspective and a Chief Information Officer (CIO) that oversees the organization from a information management

perspective (Moerdler *et al.*, 2009). The Business Unit Officer oversees the organization from a business perspective. The actors mentioned may have several roles, but they share a common one, the board of directors role. The board of directors role is to oversee, direct and evaluate the entire organization from different perspectives.

With a direct connection to the Business Unit Officer, Business Compliance Officer and Business Risk Officer are responsible to address requirements and risks from a business unit perspective. Risk owners are usually designated for managing particular risks that affect the business unit objectives.

The internal audit department is responsible for auditing the internal activities of an organization. Their role is to determine if the organization is being compliant with their internal requirements (controls and policies) and external requirements (regulations, laws and standards).

Some roles are mandatory in order to increase the effectiveness of certain activities. These roles are: business unit owners, process owners, risk owners, control owners and key-users. Each one of these roles may be assigned to anyone within an organization, therefore process, control and key-users are not assigned to any specific actor in the viewpoint. The risk manager role is responsible for coordinating the overall risk management activity.

The Program Owner role manages the compliance activities for specific regulatory requirements. There should be at least one person dedicated to a specific regulatory program from the compliance office.

3.2.2 Information Structure Viewpoint

The information structure viewpoint is identical to the traditional information models created in the development of almost any information system. It shows the structure of the information used in the enterprise or in a specific business process or application (Iacob *et al.*, 2009).

The objects presented in Fig. 3.11 represent business objects that can be seen as information entities or concepts that are necessary to support the business. The majority of objects are original from the information concepts defined in the conceptual model and its rationale has already been described (Sect. 3.1.1). A brief description follows.

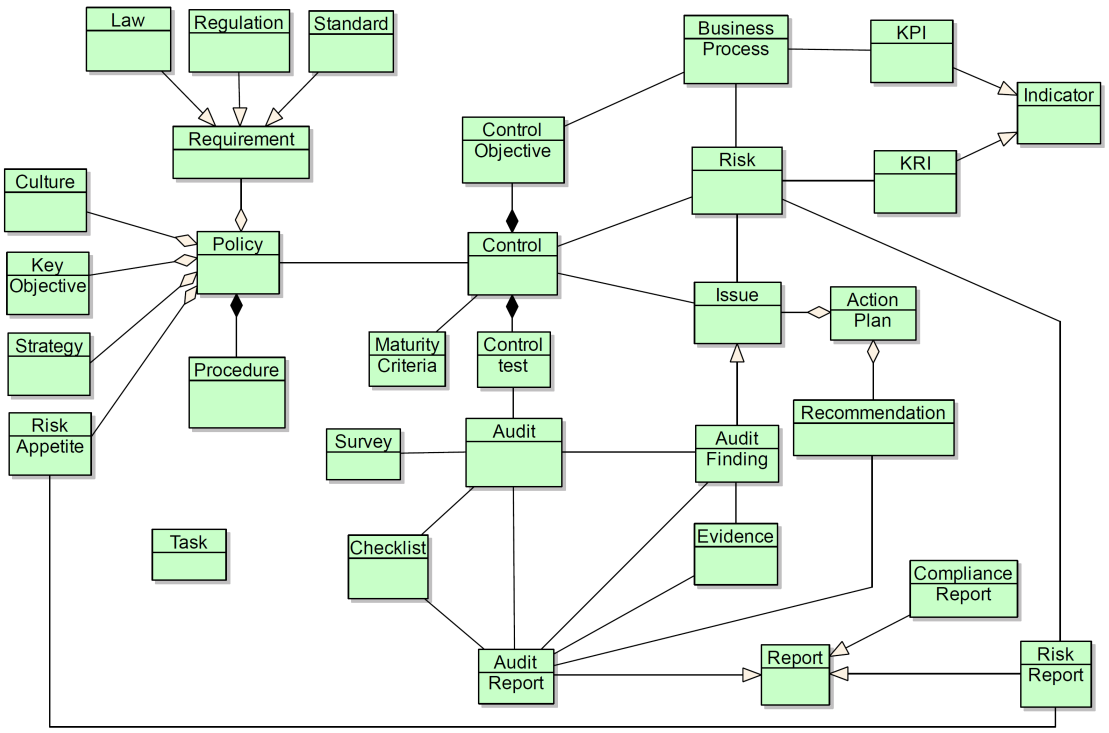

Figure 3.11: Information Structure Viewpoint

Policies may encompass a wide range of aspects of an organization. Internal policies reflect key objectives, strategy, risk appetite, culture, etc. of an organization. External policies are linked with external requirements - regulations, laws or standards. While policies define the *what*, procedures define the *how* and *who* will implement the policy. Policies and procedures are, in a certain extent, controls established to ensure the fulfilment of requirements and achievement of strategic objectives (Moerdler *et al.*, 2009). To each control, control objectives are defined and embedded in business processes. Usually controls are established to mitigate risks that menace the achievement of objectives or affect the normal function of business processes (Moerdler *et al.*, 2009). To business processes and risks, key performance and key risk indicators are developed to measure the performance of processes and the risk levels of certain activities. Risk reports are produced regularly and presented to the board.

Maturity criteria may be defined to measure the maturity level of controls. Normally auditors classify controls using this pre-defined criteria (e.g. COBIT maturity model, pass/fail criteria, etc.). Additionally, control tests may be specified to increase efficiency in controls assessments. During the execution of audits, audit findings are produced (a specific type of issues), along with evidences that prove it. Surveys and checklists are also associated with audits. For each audit,

audit reports are produced, and include all the identified inconsistencies and the associated recommendation.

3.2.3 Business Process Viewpoints

The business process viewpoint is used to show the high-level structure and composition of one or more processes. This viewpoint contains the assignment of business processes to roles and actors, and the information used by the business process (Iacob *et al.*, 2009).

We now present viewpoints for each process individually. Since one of the claims of this thesis relates to the interconnection between the various areas, a description of each of the processes makes more sense from an integrated perspective, i.e. through the business process cooperation viewpoint (Sect 3.2.2). In the following sections we will describe the relations between processes and roles.

Governance

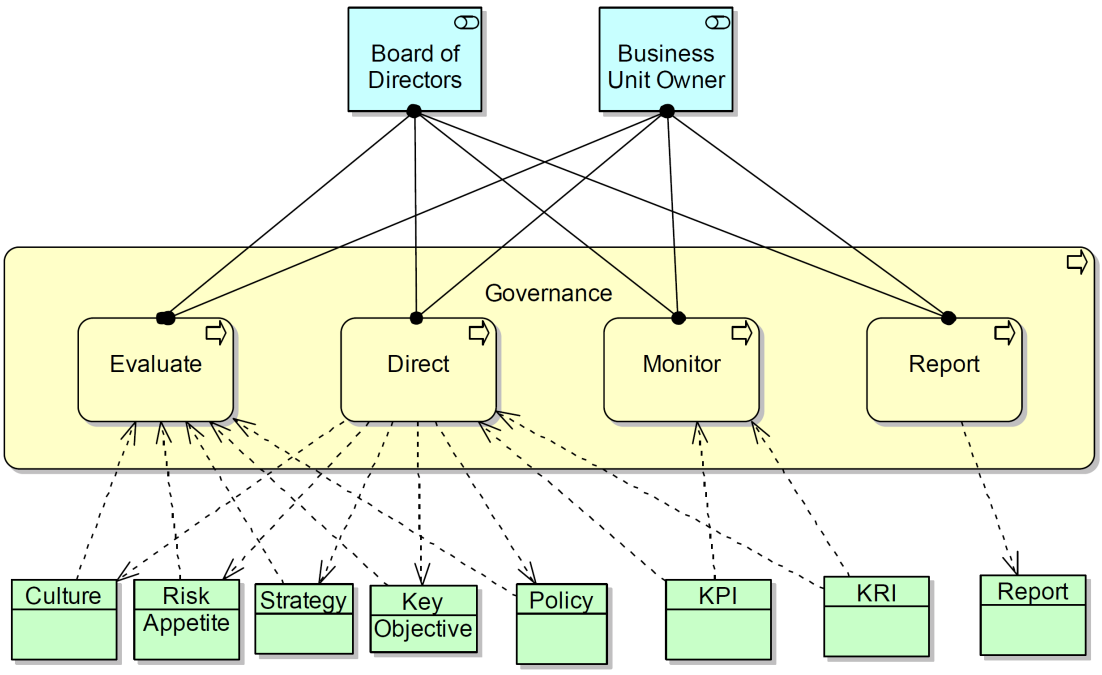

Figure 3.12: Governance - Business Process Viewpoint (adapted from (ISO/IEC38500, 2008; Racz *et al.*, 2010b)

Business unit owners are responsible to oversee their business units. The processes Evaluate, Direct, Monitor and Report mirror all types of oversight. In other words, the board of directors governs the organization thought these macro-processes.

Risk Management

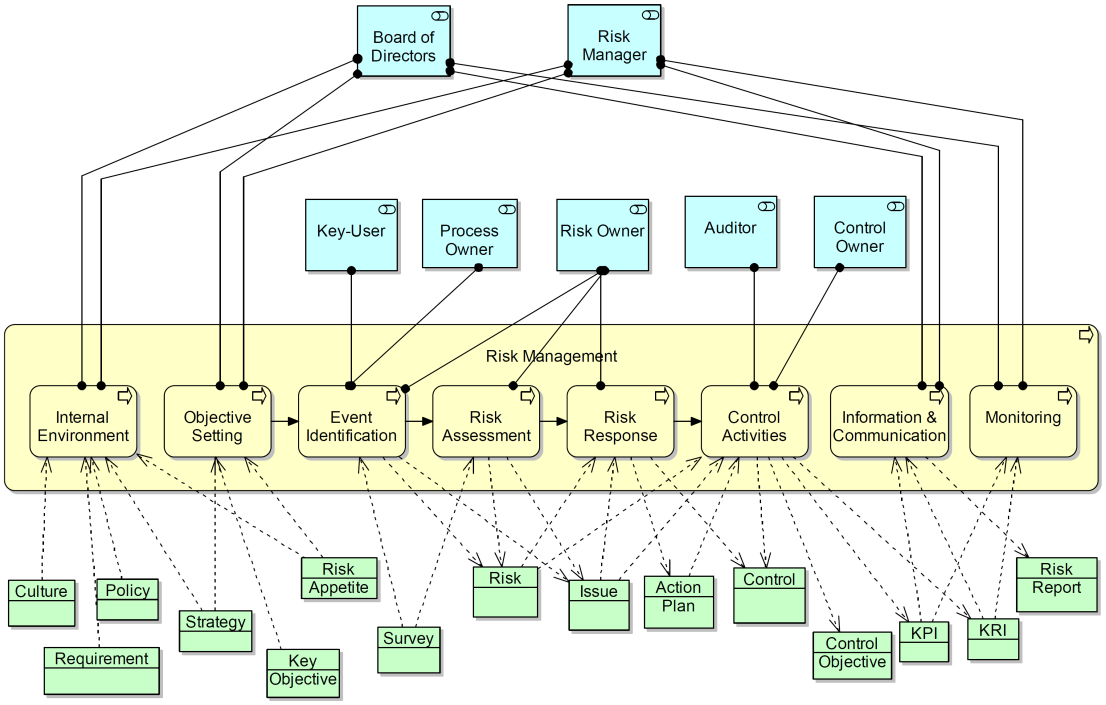

Figure 3.13: Risk Management - Business Process Viewpoint (COSO, 2004; Racz *et al.*, 2010b)

The interaction between processes and roles can be categorized in four types of actions - preventive, detective, corrective and tracking (Vicente & Mira da Silva, 2011b).

The board in conjunction with risk managers are responsible for defining objectives and analyse the internal risk environment. As stated in the previous section, the board and high management are always associated with the monitor and report (Information & Communication) processes and are more focused on tracking risks.

Key-users and process owners act in detecting new sources of risks. On the other hand, risk owners assess and plan a response to those risks (correction). Auditors and control owners implement or improve controls in order to mitigate risks (correction and prevention).

Compliance

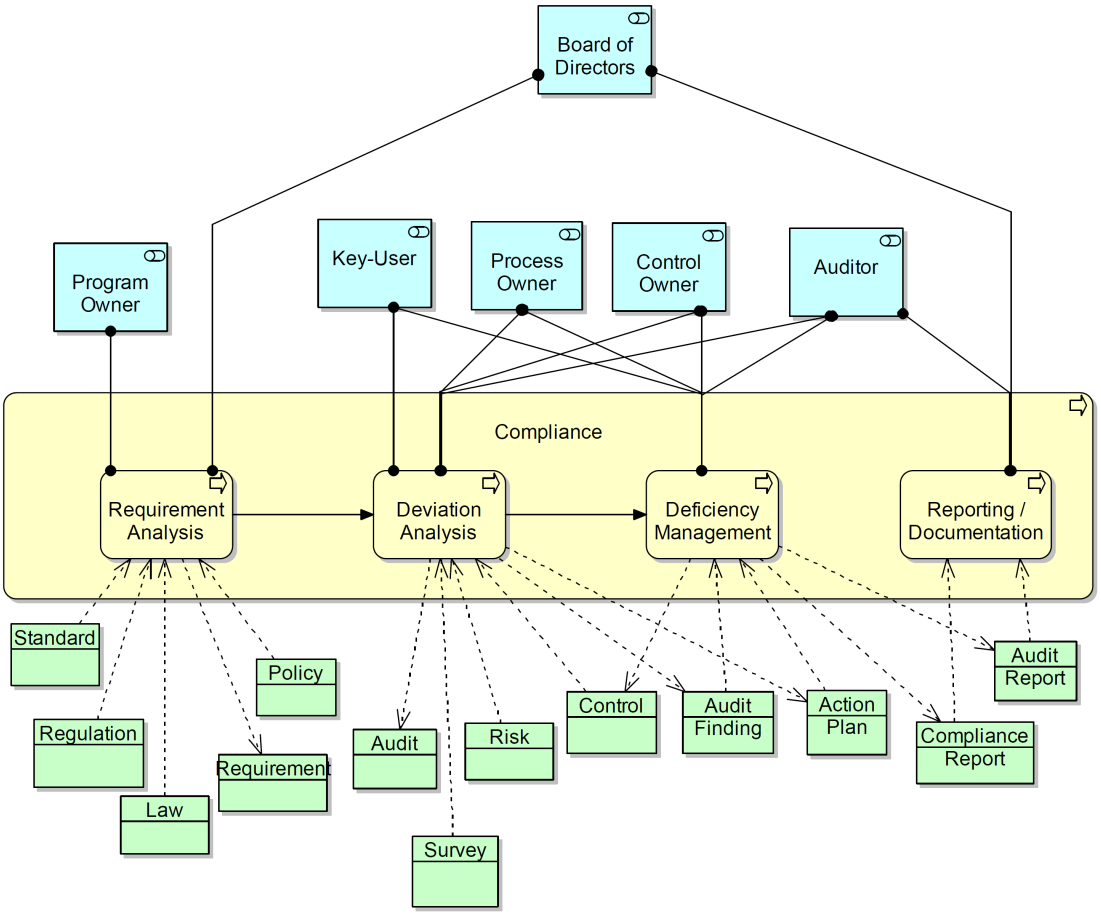

Figure 3.14: Compliance - Business Process Viewpoint (Racz *et al.*, 2010b; Rath & Sponholz, 2009)

Program owners, who are responsible for diverse requirements, establish a requirement analysis. Deviation analysis is based on audits, and the roles involved are auditors, key-users, process owners and control owners. Auditors perform audits and count with the help of these roles to conduct their examinations. When the audit is finished an audit report is created. Compliance reports are also produced based on the compliance levels determined.

As usual, the board of directors is associated with the reporting process, and in this case with the requirements analysis, in which are defined the requirements needed to follow.

3.2.4 Business Process Cooperation Viewpoint

The business process cooperation viewpoint is used to show the relations of one or more business processes with each other and/or their surroundings. In this case it is used to create a high-level design of business processes within their context and to describe the use of shared information (Iacob *et al.*, 2009).

We will now describe the logic of the constructed artefact (see Fig. 3.15).

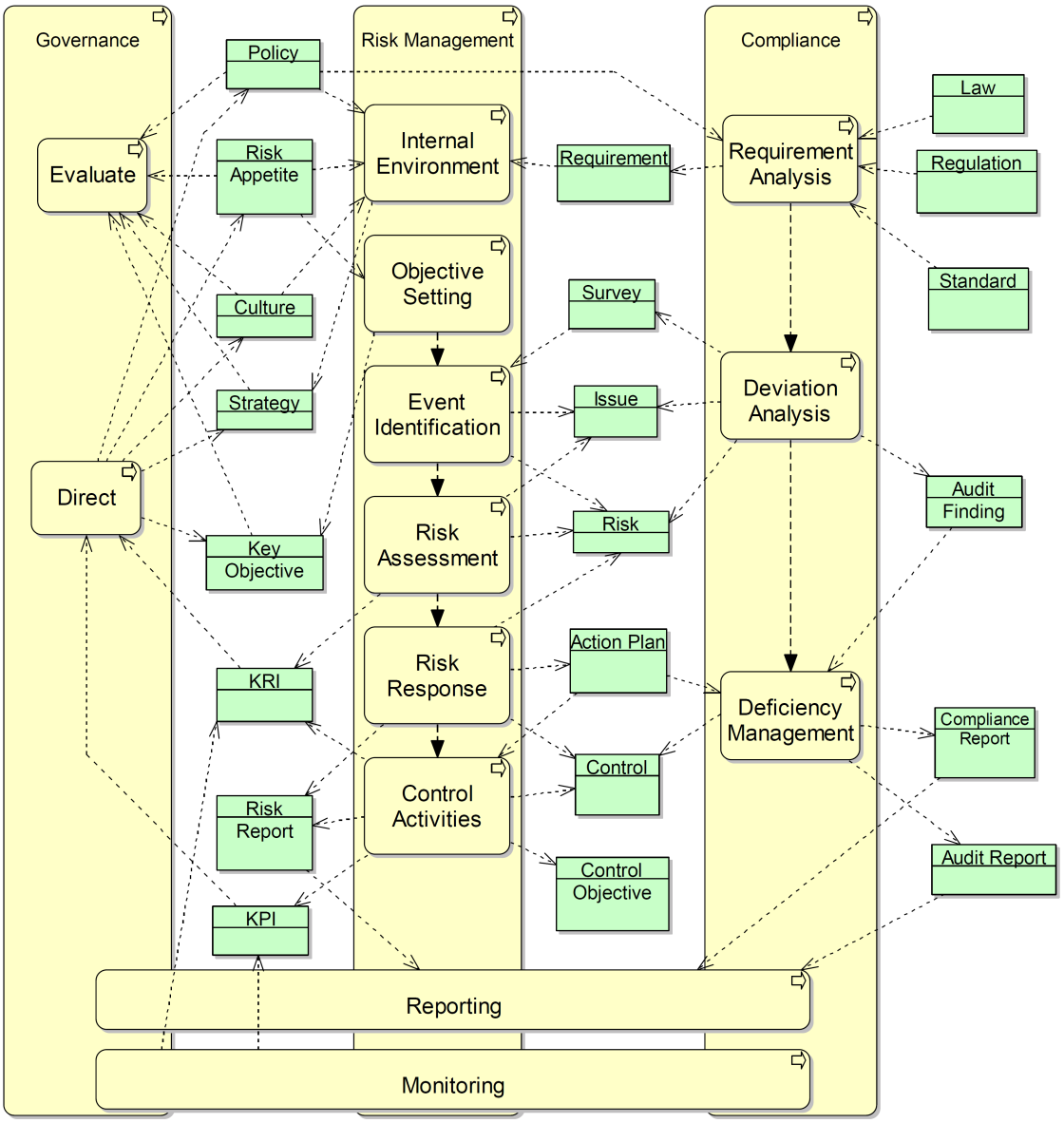

Figure 3.15: Integrated GRC - Business Process Cooperation Viewpoint (Vicente & Mira da Silva, 2011a)

Starting with the Evaluate process of IT Governance, the conceptual model establishes as the

responsibility of governance, the definition of strategy, culture, risk appetite, key objectives and policies. This clearly indicates how the organization is controlled and evaluated.

Based on these concepts, the first processes of risk management have all the information needed to establish the internal environment and objectives (Internal Environment and Objective Setting). The COSO ERM (COSO, 2004) describes internal environment as the establishment of the entity's risk culture, ethics and risk appetite. Additionally, key objectives, risk appetite and the strategy established are requirements to properly identify events that should be aligned with the organization's concerns. These events, that have already occurred (issues) or may occur (risks), can be identified using self-assessment techniques through surveys. Compliance management must gather and convert all the external (regulations, laws, standards) and internal (internal policies and procedures) obligations into policies, in order to complete the requirement analysis process.

Once the requirement analysis is complete, the deviation analysis can be performed through audits or self-assessments. Also, the already identified issues and risks (events) should be marked for review. This is where the risk assessment process is important: to prioritize risks in terms of its impact, probability and velocity.

From the risk assessment and deviation analysis, a response to the risks and findings produced by the audit teams must be conducted (Deficiency management). Action plans and risk response strategies are produced, resulting in the improvement of internal controls that play an essential role to prevent, detect, correct and track risks, and that, as a result, fulfil the control goals that need to be established (control activities).

The processes described represent activities and measures taken to minimize the impact of risks and issues, as well as, to enhance internal controls and, thus, processes, while increasing the level of compliance and decreasing the risk exposure of the organization.

Additionally, and along the previously mentioned processes, governance manages the outputs from risk and compliance processes, namely indicators - Key Risk Indicators (KRI) and Key Performance Indicators (KPI) - among others - and risk and compliance reports that transmit the current organization-wide status of residual risks, controls, policies and compliance levels. The analysis and exchange of information across the levels of the organization is supported by reporting and monitoring processes that provide reliable and real-time information through dashboards and reports.

In the business process collaboration viewpoint presented in Fig. 3.15, we extended the monitoring and reporting process to governance, risk and compliance, since they are important in the three sub-domains and can be easily unveiled through the analysis of each.

After this description, it can be stated that both models used to develop this viewpoint (the conceptual model and the process model) complete each other, leading to a business process cooperation viewpoint comprising the processes and the business objects used between them. On the one hand, this demystifies the relations of the process model and, on the other hand, it organizes and provides more structure to both models.

3.3 Information Systems Architecture

Information systems architecture focuses on identifying and defining the applications and data considerations that support the Business Architecture, by defining views that relate to information, knowledge, application services, etc. (The Open Group, 2009). Although TOGAF divides the information systems architecture in application and data architectures, ArchiMate presents only one layer - application architecture - to describe the information systems layer.

The viewpoints selected from ArchiMate to model the application architecture are:

- Application Usage Viewpoint (Sect. 3.3.1);
- Application Structure Viewpoint (Sect. 3.3.2);
- Application Behaviour Viewpoints (Sect. 3.3.3);
- Application Cooperation Viewpoint (Sect. 3.3.4);

We will start describing the information systems architecture by defining the application services that are exposed from the application layer to support the processes from the business layer (application usage viewpoint). To do so, we will also need to define the application components. In order to define consistently the necessary applications to support the processes, we present a CRUD (Create Read Update Delete) matrix (see Fig. 3.16) that relates processes (or actions) with informational entities defined in the business architecture from the previous Section.

We opted not to include all information entities in order to simplify the matrix. For example, the Report entity represents all type of reports - audit, risk and compliance. Additionally, the Requirement entity aggregates the Law, Standard and Regulation entities. The same applies to the Policy entity.

This matrix was built in order to identify clusters that represent application solutions. The relation between processes and information entities provides a more structured approach to the identification of application components and services needed to support the processes.

Through the analysis of the obtained clusters (see Fig. 3.17) some optimization could be suggested by integrating some systems. For example, issue and risk management are very similar, but they manage information entities that are, by definition, distinct, so we opted to maintain both.

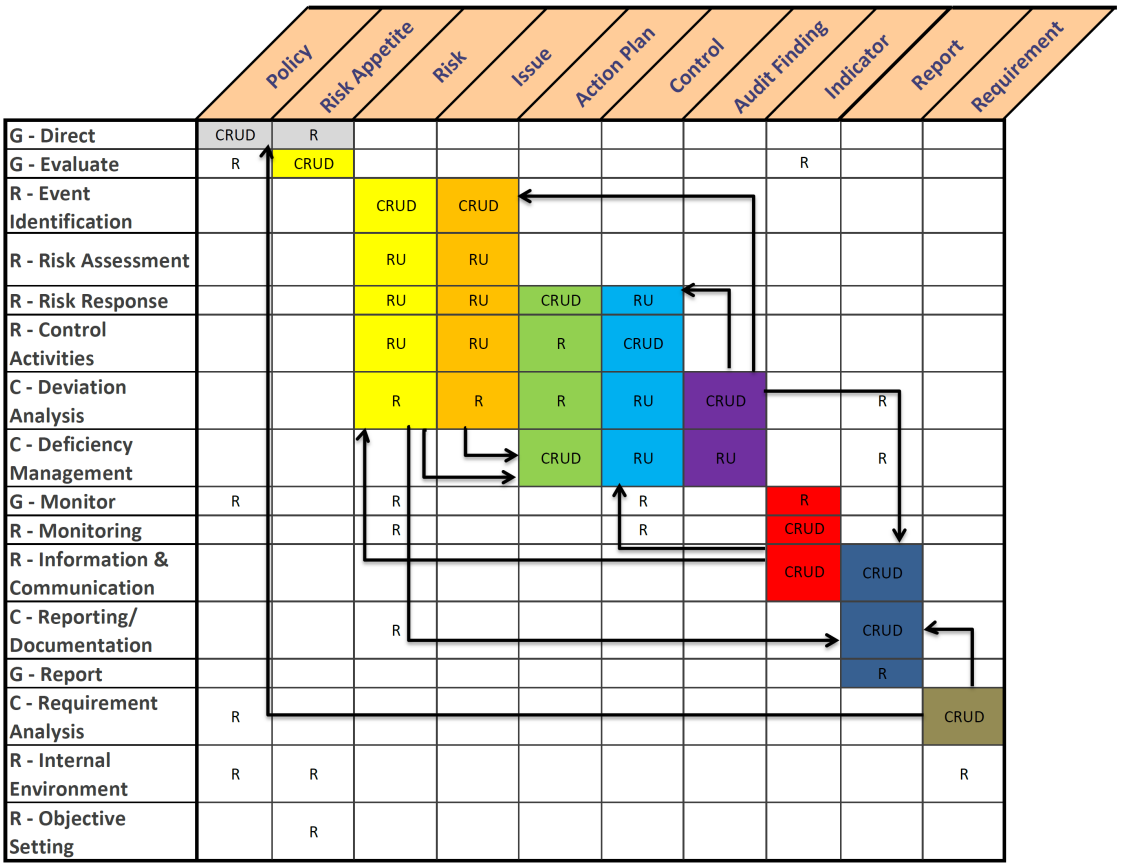

Figure 3.16: CRUD Matrix

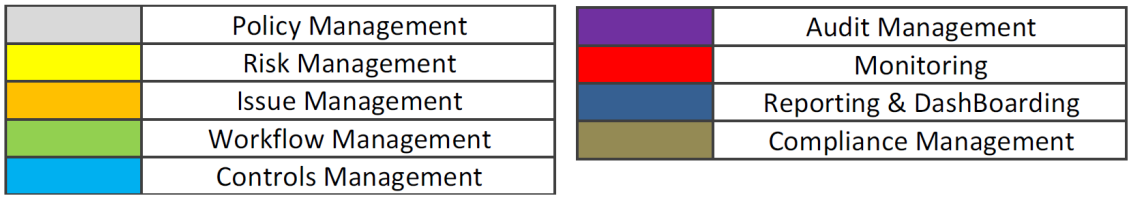

Figure 3.17: Application Components

The matrix also came to support the expansion of both reporting and monitoring processes across Governance, Risk and Compliance proposed in Fig. 3.15, because the processes manage the same information.

The integration between applications was also represented in the form of arrows. These integrations will be better justified in the description of the application behaviour viewpoints.

In Fig. 3.17 the proposed application components are listed. Some applications are the same from the conceptual model. Workflow, controls and compliance management were added. The application components will be described in the next sections.

3.3.1 Application Usage Viewpoint

The application usage viewpoint describes how applications are used to support one or more business processes. It can be used in designing an application by identifying the services needed by business processes (Iacob *et al.*, 2009).

In this viewpoint (Fig. 3.18) we chose to maintain the original processes, i.e. not expanding the monitor and report processes through the governance, risk and compliance processes, in order to simplify the viewpoint.

According to the ISO/IEC38500 (ISO/IEC38500, 2008), the Direct process is based on the assignment of responsibilities, direct preparation and implementations of policies. In order to support this process, a Policy Life Cycle Service should be defined to support all actions needed to manage policies across the organization.

On the other hand, the Evaluate process is based on the current and future organizational objectives, thus the service provided by the risk management application - Risk appetite calculation service - is an important method to evaluate the readiness of the organization to apply new strategies and proposals.

An automated monitoring service should also be present to support the monitoring process of governance and risk management.

During this research, we defined an event as a risk or an issue. Following the same line of thought, the Event Identification process, uses two separate application services from two different application components, but with the same behaviour: risk and issue creation. Similarly, to support the assessment of these events, assessments or analysis should be supported by application components, using once again, two separate application services to risks and issues. Risk Response and Control Activities processes are closely related to the treatment of the identified and assessed events, in order to address and resolve the event. Consequently, both processes use the risk and issue treatment service. Controls may also need to be created, thus a control creation service is needed.

The Control Activities process also has a direct relation with audits, since their function is to

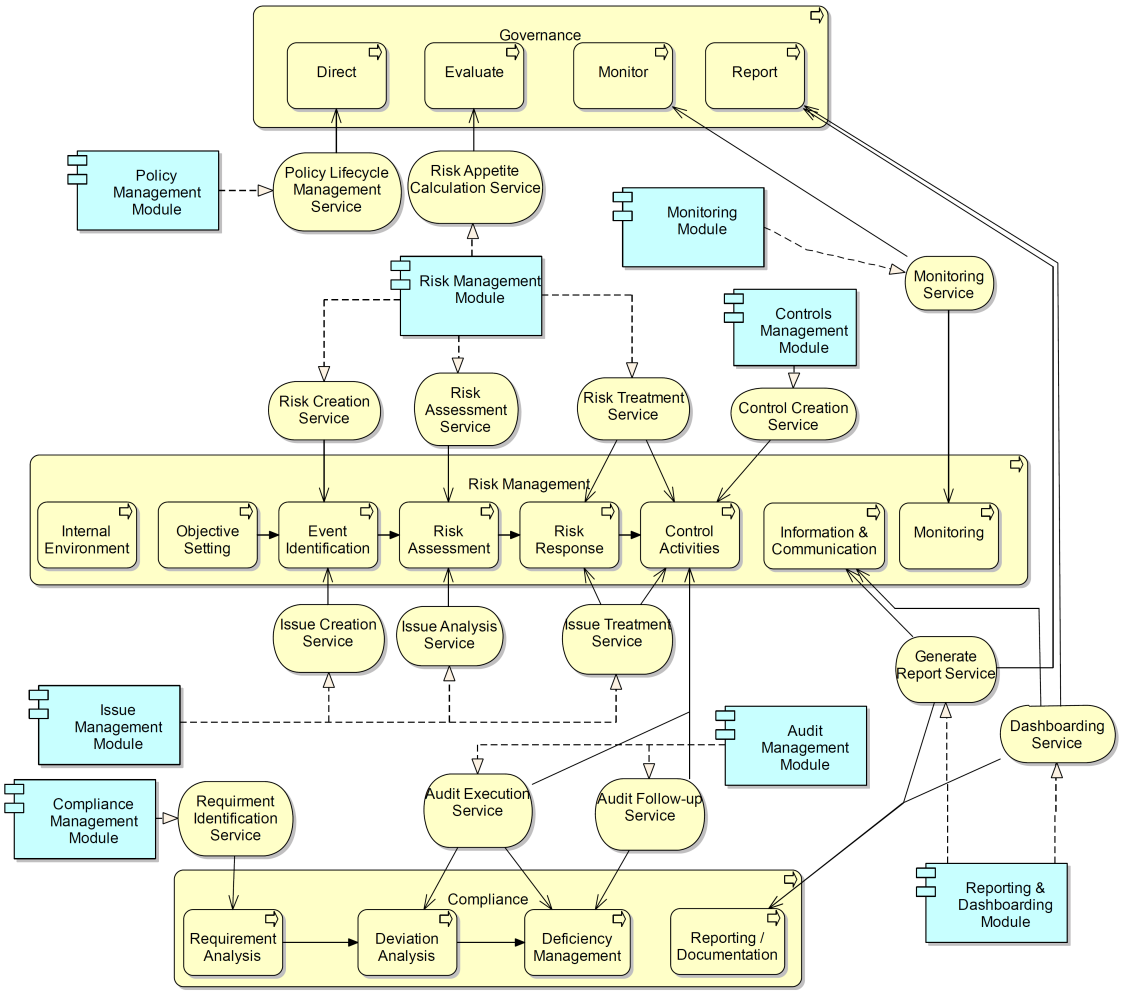

Figure 3.18: Application Usage Viewpoint

improve internal controls. For that reason, the audit execution and follow-up services are used by this process. These two services, may assist the Deviation Analysis and Deficiency Management processes, in order to support the execution and follow-up of audits.

The Requirement Analysis process, should be simplified through an application service, in order to ease the management of requirements and its relations across other information components in the organization.

As stated before, reporting is truly a common and important factor in integrated GRC, mainly due to the extensive relation among information structures. A reporting service may aid the documentation and communication of important information across the organization, and facilitate the implementation of a dashboarding service, that is much valued in organizations.

Through the identification of the necessary application services needed to support the identified processes, we will now describe how the application layer provides the mentioned services.

3.3.2 Application Structure Viewpoint

The application structure viewpoint shows the structure of one or more application components. This viewpoint is useful in designing or understanding the main structure of applications and the associated information (Iacob *et al.*, 2009).

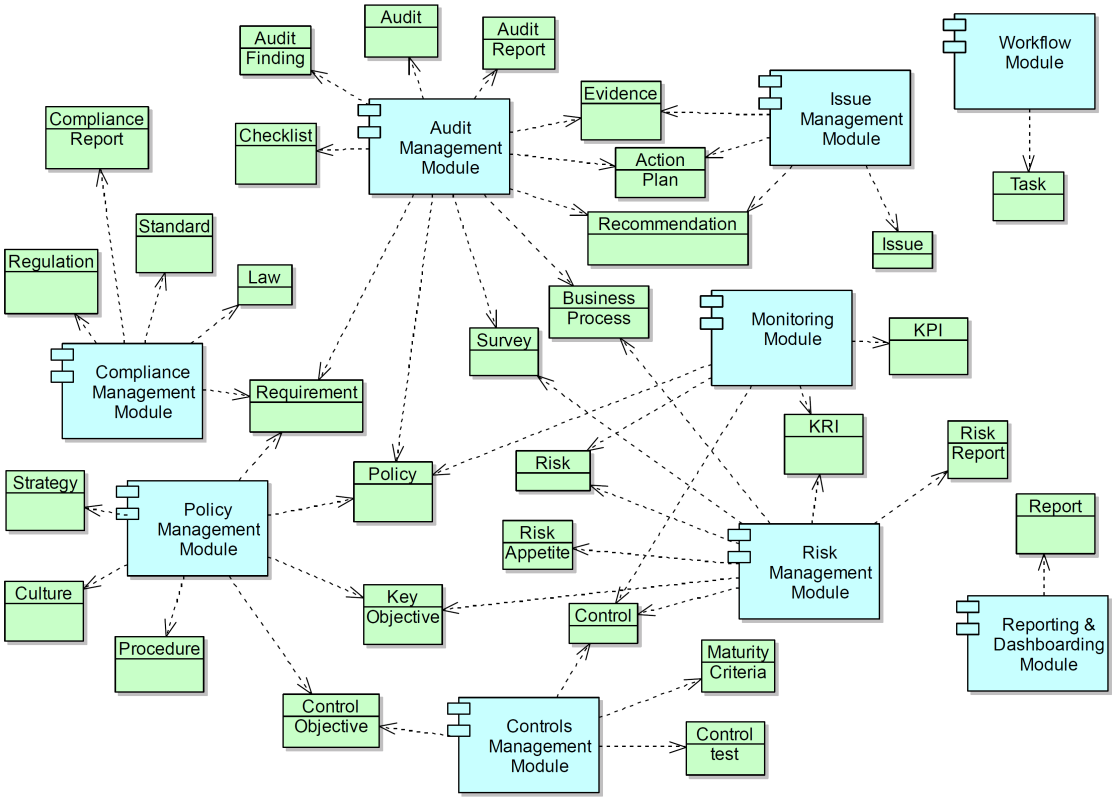

Figure 3.19: Application Structure Viewpoint

This viewpoint (Fig. 3.19) describes the structure of the applications through the sharing of information. This view re-enforces the problem that integrated GRC addresses. Traditionally, the application components present in this viewpoint, represent departments, that usually do not communicate effectively and efficiently because they are isolated. The usage of mutual information between at least seven out of nine application components is impressive, and an integrated and holistic approach to all GRC activities makes indeed much more sense.

In the next section we will describe in further detail how each application manages these information.

3.3.3 Application Behaviour Viewpoints

The Application Behaviour viewpoint describes the internal behaviour of an application component, e.g. as it realises one or more application services. This viewpoint is useful in designing the main behaviour of applications, or in identifying functional overlap between different applications (Iacob *et al.*, 2009).

Workflow Management Module

The workflow module (Fig. 3.20) is pretty simple, but very important, since it promotes collaboration through the assignment of tasks and creation of dynamic processes. This model realizes internal services, i.e., services that will be used by other application components. The services provided by this component include the elaboration of processes to create action plans, or simple to assign tasks in cases of approvals or important notifications.

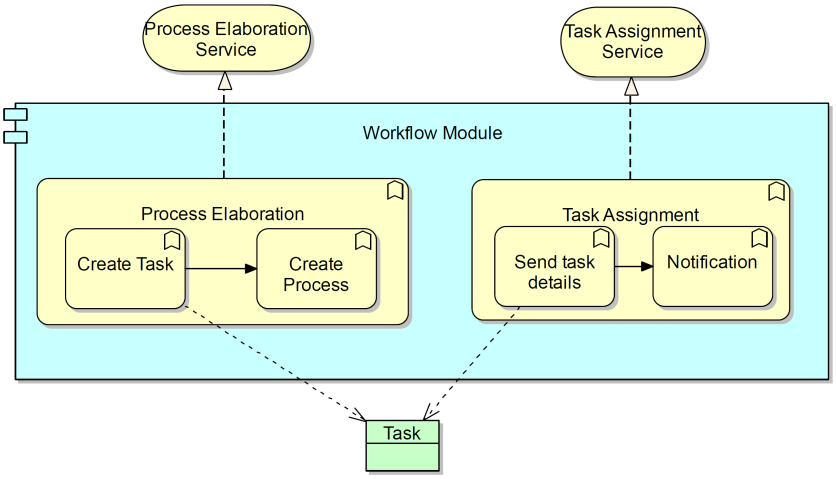

Figure 3.20: Workflow Module - Application Behaviour Viewpoint

Controls Management Module

This module is responsible for internal controls (Fig. 3.21). It includes the administration of controls - creation of controls, control objectives and definition of maturity criteria - and supports the controls assessment and definition of controls tests. Just like the workflow management module, this component provides internal services (Control Test Creation Service and Test Control Service) and one external service (Control Creation Service).

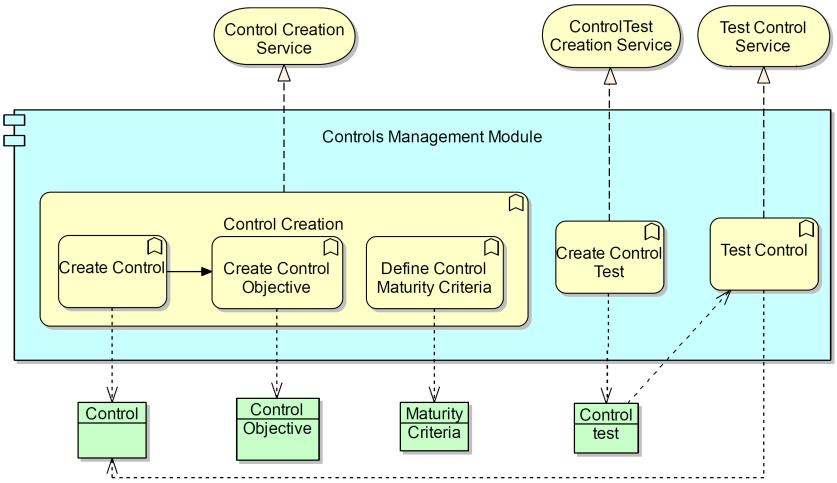

Figure 3.21: Controls Management Module - Application Behaviour Viewpoint

Reporting and Dashboarding Module

It is paramount for the GRC strategy, that applications are able to report and feed information in order to maintain a "360-degree view of GRC" (Rasmussen, 2010c). The reporting and dashboarding module (Fig. 3.22) is important to gather, relate, customize and report information that will be used to generate reports and dashboards (Bastos *et al.*, 2010), thus providing the so-called holistic-view of GRC.

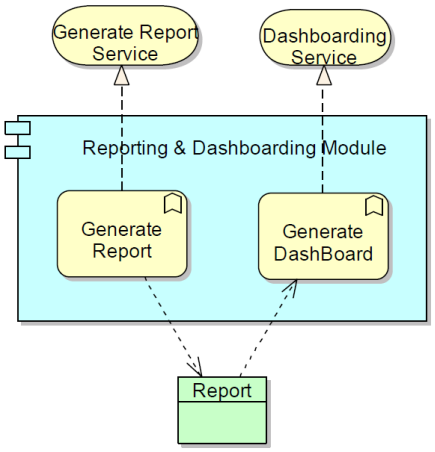

Figure 3.22: Reporting and Dashboarding Module - Application Behaviour Viewpoint

Monitoring Module

Monitoring is based on value protection thought the insurance that violations are identified within a certain time limit that minimizes losses and errors (Rasmussen, 2010a). To improve monitoring efficiency, processes and controls should be synchronized with objectives, policies and risks. The monitoring application component (Fig. 3.23) focuses on monitoring controls, policies, risk and indicators (KPI and KRI). Further application details are very specific to each implementation.

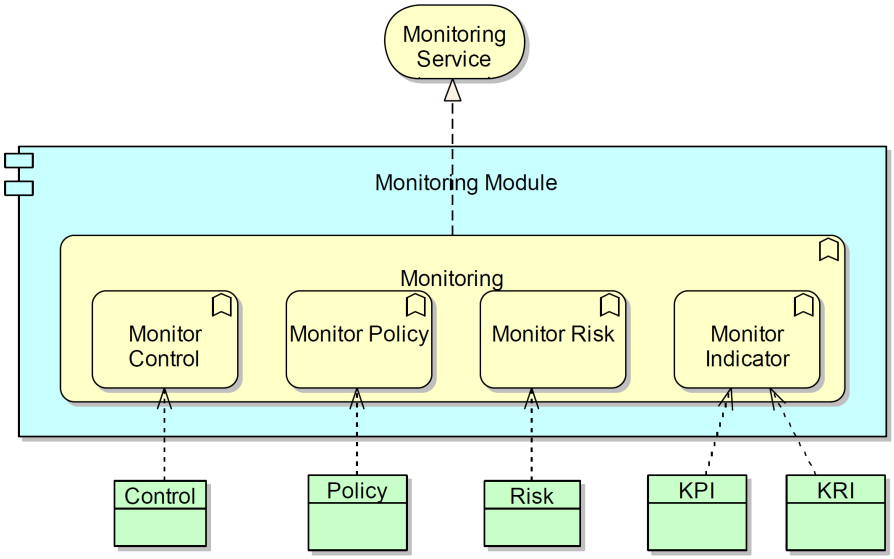

Figure 3.23: Monitoring Module - Application Behaviour Viewpoint

Policy Management Module

The policy management module (Fig. 3.24) is closely related to support the policy life-cycle management. According to (Rasmussen, 2010b; Sumner Blount Director,, 2009) the policy life-cycle is based on: environment changes, policy development, policy communication, policy monitoring and policy maintenance.

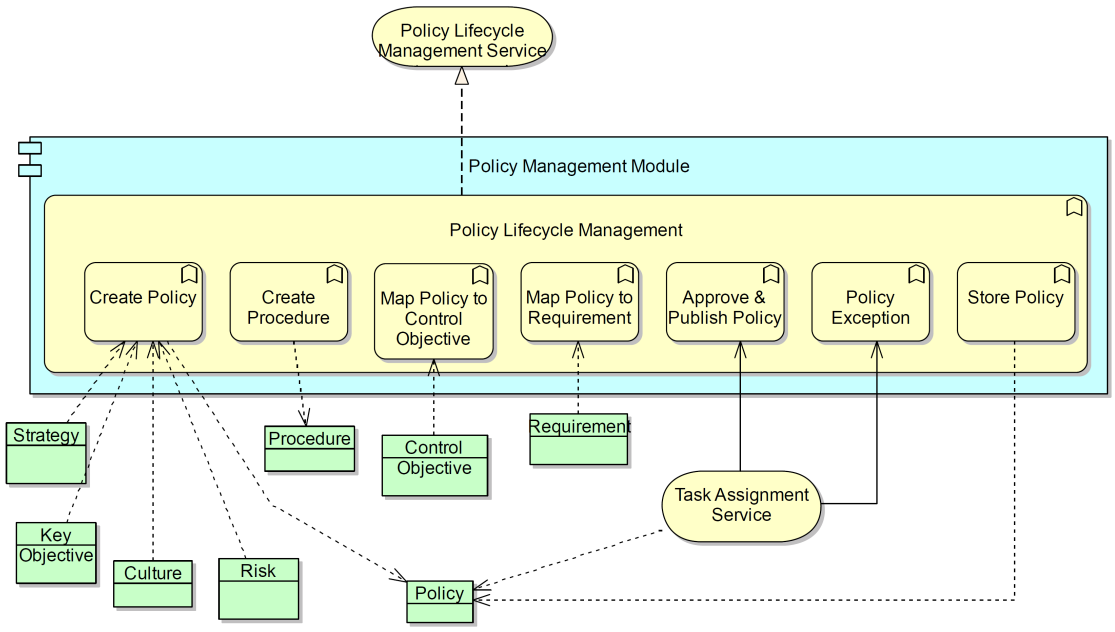

Figure 3.24: Policy Management Module - Application Behaviour Viewpoint

To support this life-cycle, this application module must be able to create policies and procedures, and map them to controls and requirements. The approval function uses a service from the workflow module, based on the assignment of tasks in order to gather opinions, followed by the publication of policies. Policies exceptions are also handled by this application.

Compliance Management Module

The compliance module (Fig. 3.25) is responsible for the requirements that affect the organization (both externally - mandatory boundary - and internally - voluntary boundary) (Bastos *et al.*, 2010).

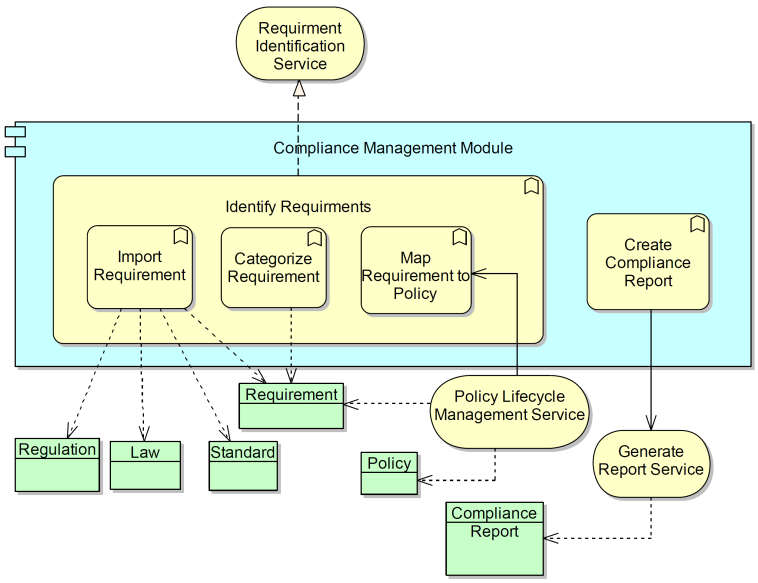

Figure 3.25: Compliance Management Module - Application Behaviour Viewpoint

The requirements are imported by the application and categorized. They can also be linked with policies, using the policy life-cycle management service, described in the previous section. This component realizes one external service - requirement identification service. This module also allows the creation of compliance reports using the generate reporting service.

This relation follows the rationale from the conceptual model that identifies a touch point between compliance and governance through policy management.

Issue Management Module

The issue module (Fig. 3.26) functions mainly as a repository. As stated in Sect. 3.1.1, an issue is a positive/negative, internal/external nonroutine stimulus that requires a response (Brache, 2001). In the scope of this research issues are more likely to be classified as risk events or audit findings.

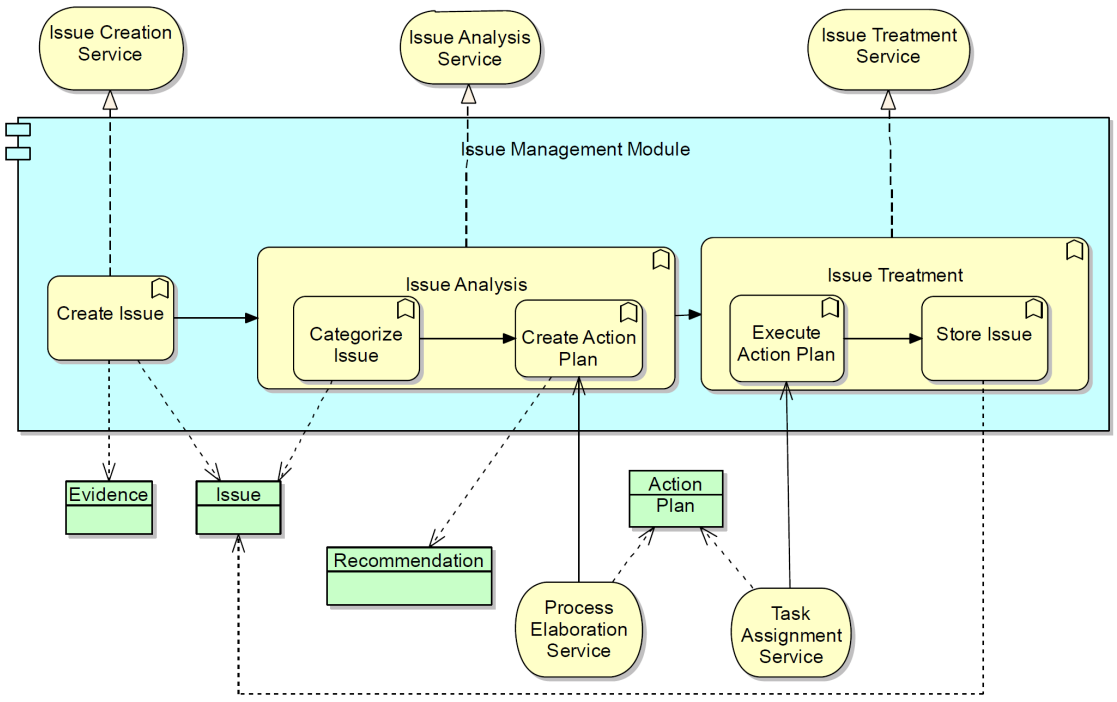

Figure 3.26: Issues Management Module - Application Behaviour Viewpoint

To support the management of issues, the following phases are proposed: creation, analysis and treatment. Analysis is based on the categorization of issues followed by the elaboration of an action plan that should be carried out in order to address the issue. Action plans consists in tasks assigned to people who should implement the necessary mechanisms to treat the issues. After the treatment the issue can be stored. Once again these relations are depicted in the conceptual model.

Risk Management Module

This module (Fig. 3.27) is more complex than the others. Everything is connected to risks and these connections must be properly managed. The risk management module component realizes four services that support the risk management processes.

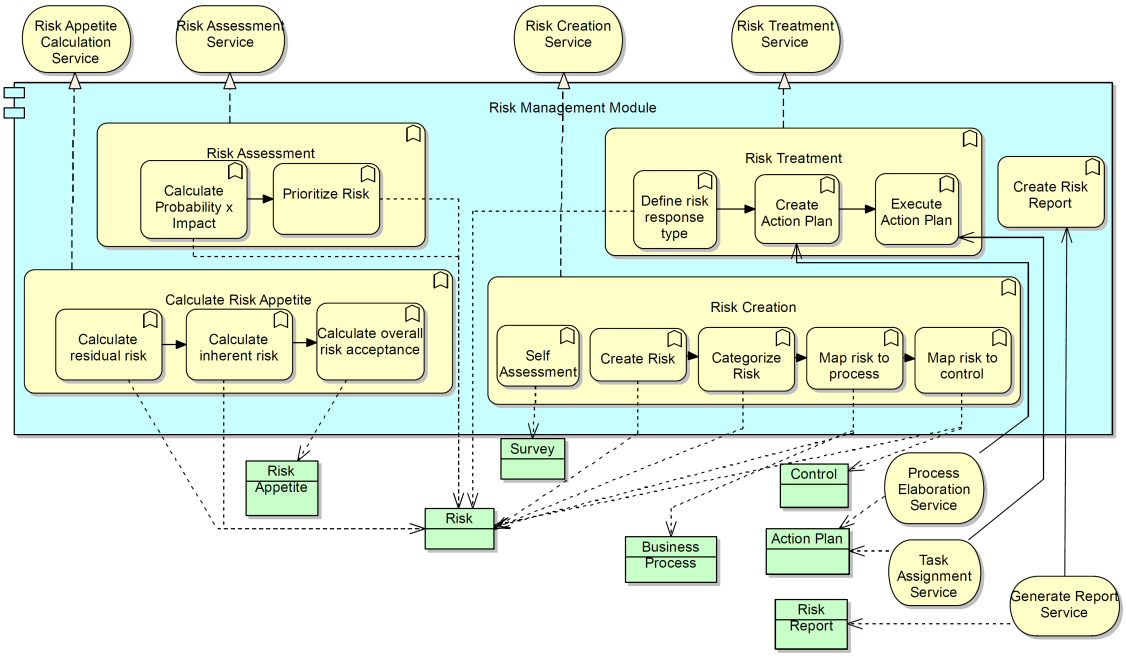

Figure 3.27: Risk Management Module - Application Behaviour Viewpoint

The risk appetite calculation allows the calculation of residual and inherent risk and thus the overall risk appetite. Risks can be created, categorized and mapped into processes and controls. Risk assessments allow the prioritization of risks and risk treatment is analogous to issue treatment. Risk report generation is also possible through the usage of the generate report service from the reporting and dashboarding module.

Audit Management Module

In order to meet the compliance process needs, two external services are realized by the audit management module. This selection divides the execution and follow-up of audits. Audit execution is focused on the scheduling and prioritization of audits according to risks, issues, etc. The selection of functionalities was made taking into account the ISO 19011 (ISO19011, 2002) that describes the functions necessary to support the audit execution.

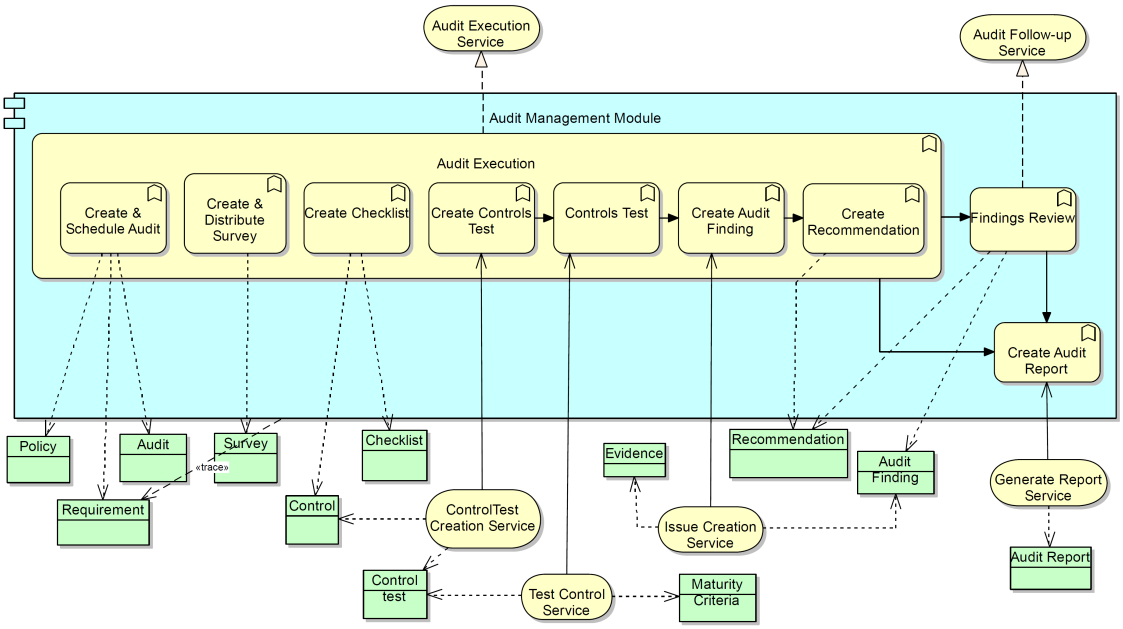

Figure 3.28: Audit Management Module - Application Behaviour Viewpoint

Test controls are created in order to assess controls and report audit findings (issues). At the end of each audit, a report must be created, in this case using the report generation service. Findings that are categorized as unacceptable to the organization must be corrected. The audit follow-up service gives support to the revision of these cases.

To support some of these functions, this application module uses services provided by controls management module, issues management module and reporting and dashboarding module.

3.3.4 Application Cooperation Viewpoint

The application cooperation viewpoint shows the relations between application components. It describes the dependencies in terms of the information flows between them, or the services they offer and use (Iacob *et al.*, 2009). We opted to include only service dependencies in this viewpoint. Sharing of information is described in the application structure viewpoint (see Fig. 3.19 in Sect. 3.3.2).

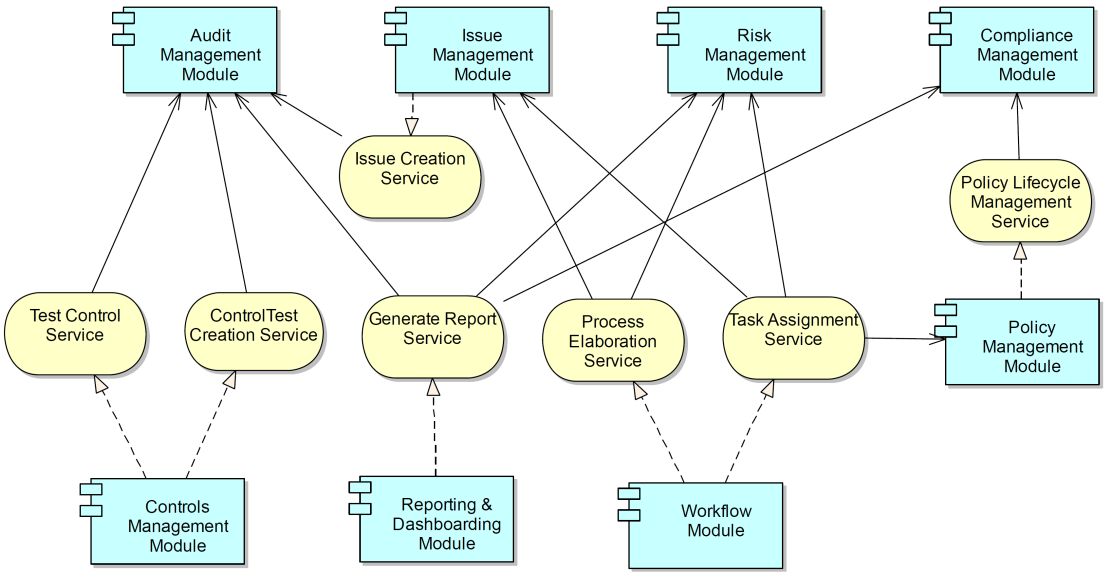

Figure 3.29: Application Cooperation Viewpoint

As stated in the description of each module in the previous section, there are some dependencies between application components. In this viewpoint (Fig. 3.29) those dependencies are more simple to ascertain.

3.4 Summary

Throughout this Section we described the proposed models accomplished in this research: a conceptual model and a reference architecture. The conceptual model was modelled using ad-hoc syntax and the architecture was modelled using several viewpoints based on the TOGAF ADM and the ArchiMate modelling language. The architectural layers accomplished were the business and information system layers. The selected viewpoints portray the authors view and know-how of the domain. A portion of the selected models were scientifically published.

Chapter 4

Evaluation

Evaluating reference models is known to be a major challenge. In this research, the models designed are a conceptual model and an architecture. Reference and conceptual models share common evaluation issues concerning their (re-)usability, testing and analysis (Frank, 1999, 2006). Another issue that difficult the evaluation of these models holds with the factor that reference or conceptual models often describe future domains, hence they cannot be evaluated against a user's perception of reality only (Frank, 2006).

Nonetheless, various frameworks arose to evaluate the quality of reference models. Along this chapter we describe a model quality evaluation framework and the evaluation method, and discuss the obtained results.

4.1 Evaluation Methodology

The evaluation methodology proposed is illustrated in Fig. 4.30.

The evaluation of this research has four main components that feed each other. Interviews with practitioners, scientific publications and participation in the development of GRC software. These three components provide the necessary input to use the data model quality framework (Moody & Shanks, 2003) to evaluate some factors of the constructed artefacts. The factors proposed in the framework are:

- **Completeness** refers to whether the model contains all user requirements;
- **Integrity** definition of business rules or constraints from the user requirements.

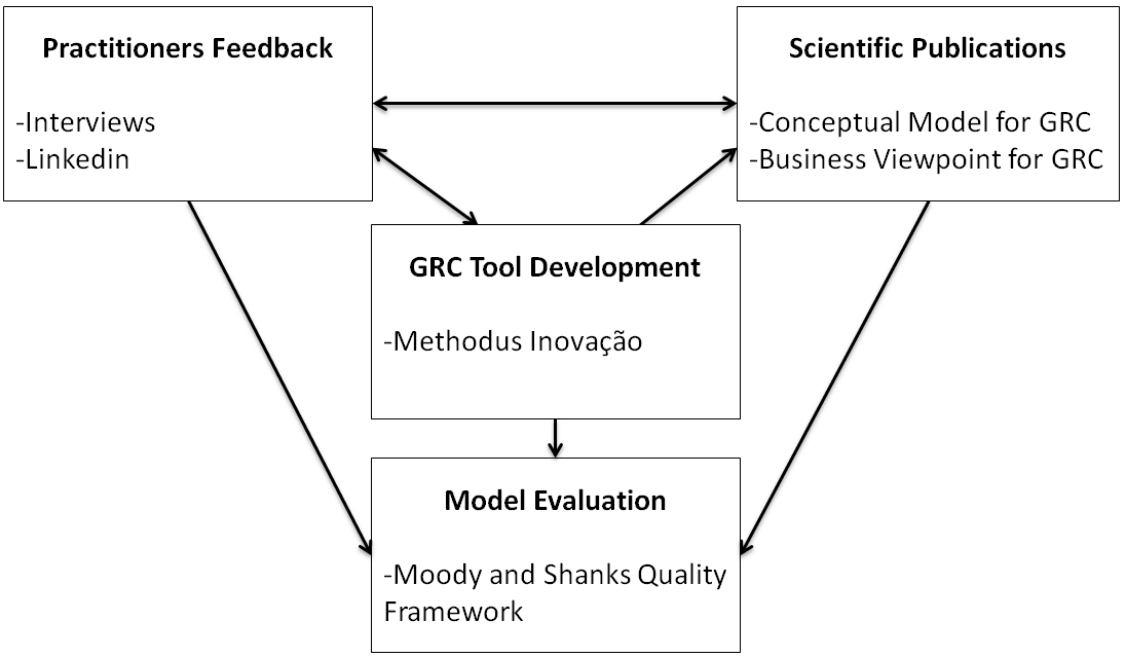

Figure 4.30: Evaluation Methodology

- **Flexibility** is defined as the ease with which the model can reflect changes in requirements without changing the model itself.

- **Understandability** is defined as the ease with which the concepts and structures in the model can be understood;

- **Correctness** is defined as whether the model conform to the rules of the modelling technique (i.e. whether it is a valid model). This includes diagramming conventions, naming rules, definition rules, rules of composition and normalisation;

- **Simplicity** means that the model contains the minimum possible entities and relationships;

- **Integration** is defined as the consistency of the model with the rest of the organisation;

- **Implementability** is defined as the ease with which the model can be implemented within the time, budget and technology constraints of the project;

In the next Section we will discuss the obtained results based on the evaluation methodology described.

4.2 Evaluation

Interviews with practitioners can be divided in three phases. First they supported the identification and validation of the problem and domain. Secondly, they evaluated the scope of the domain through the analysis of the conceptual model. Finally, they evaluated the reference architecture. We used face to face interviews, e-mail exchanges and group discussions in the professional network Linkedin[1]. The majority of comments was made concerning each area individually. The integration between the three areas was well accepted by the discussion participants.

The interviewees and participants occupied diverse job positions. The main areas were: risk, control, audit and security professionals, along with researchers and business directors. Examples of represented companies were: SAP, PT, PwC, Glintt, Instituto de Informática MTSS, Solvay, EDP, APCER, EIC, MAPFRE and Caixa Seguros.

Feedback from these phases allowed to gain more structured knowledge about the domain, and provided the foundations for writing scientific papers. As stated in Sect. 1.2 one of the main objectives of this research was to attain feedback and validation from the scientific community. Lack of scientific guidance was in fact one of the origins of the problem that this research addresses. The scientific publications brought valuable input for further research, feedback and approval (Offermann *et al.*, 2009). It also allowed to obtain more feedback from practitioners. As stated previously, two scientific papers were published: A Conceptual Model for integrated GRC (Vicente & Mira da Silva, 2011b) and A Business Viewpoint for Integrated ITGRC (Vicente & Mira da Silva, 2011a).

Another important component was the participation in the development of a GRC suite with the role of requirement analysts. It allowed to create an instantiation of the reference architecture at the application level. It also brought more connections (i.e. practitioners) from the business environment.

The conjunction of all these aspects, improved the experience and know-how of the authors in this domain, enabling the development of the models that this research proposes. It also provided important feedback to evaluate the same models.

We will now discuss the quality factors from the model quality evaluation framework:

- **Completeness**: Concerning completeness, each case should be treated as a separate case. For some organizations some processes may be missing. However, and since this research focus on the integration of the three disciplines, and not so much in deepening

[1] http://www.linkedin.com/groupItem?view=&gid=121456&type=member&item=40224356&qid=61f2b628-0a1d-40f1-b385-b92b93baaae5 - Most active discussion

each discipline, it is our belief that the reference architecture describes the key integration points between governance, risk and compliance. On the other hand, the model was developed based on well-known validated research. Additionally, the conceptual model used to define the scope of GRC was evaluated in terms of completeness (see Appendix A) and the authors concluded that it was complete.

- **Integrity**: The abstraction of the constructed model does not specifies constraints. Nonetheless, it respects accepted rules in risk management and audits for example. The triggering effect between the processes and application functions follows accepted practices from each discipline.
- **Flexibility**: This factor has paramount importance in reference models. A good reference model must be extensible and evolvable. Given the abstraction of the reference architecture, processes and applications can be easily deepened and adaptable to diversified environments.
- **Understandability**: A key claim from ArchiMate is based on the understandable structure and concepts that it encompasses. For that matter, the use of ArchiMate presents an advantage for modelling architectures. Also, the use of multiple viewpoints clarifies the rationale of the architecture.
- **Correctness**: In the Theoretical Background section (Sect. 2.4.3) we described the elements that have been used in the development of the architecture. We have followed best practices from the ArchiMate specifications to design and relate elements using the viewpoints that better portray the structure and behaviour of the reference architecture. Based on this arguments, we can affirm that the model is valid.
- **Simplicity**: Based on the practitioners opinion none of the entities or relations used on the model were pointed out as unnecessary. Additionally, all the concepts and relations used in the conceptual model were described in the OCEG Capability Model.
- **Integration**: The model presents several viewpoints from different parts of the organization, and successfully relates them at the business and application level. Additionally, the application components were developed taking into account their modularity.
- **Implementability**: One of the claims of this research is to provide a reference concerning processes, applications and information. However, the reference architecture has only been implemented at the application level. The implementability of the processes and their relation with applications was not tested. Nonetheless, the use of reference processes, like COSO ERM and ISO 38500, ensures a certain level of applicability in specific situations.

Another framework could have been used to evaluate the architecture (for example, the conceptual model quality framework (Moody *et al.*, 2003) used in the evaluation of the conceptual model (see Sect. Appendix A) using syntactic, semantic and pragmatic quality factors). However, we chose to use a different framework that encompassed more distinctive factors.

4.3 Discussion

The models developed in this research present a defined level of abstraction. Abstraction, however, does not simply mean to arbitrarily fade out parts of the domain. Instead, abstraction should include hints of how to turn it into a concrete description that applies to a particular case (Frank, 2006). In this research we tried to follow this objective by proposing models and describing rationales that could lead to concrete implementations.

Moreover, the use of some of the few scientific research in this domain showed that scientific research is aligned. Some choices along this research were made taking into account this factor.

Although some of the used sources for this research are directed at the IT GRC scope, we have also been able to verify that IT activities can be supported through a generic reference directed for the GRC scope.

The proposed business process collaboration viewpoint (Fig. 3.15) is good evidence that there is a clear alignment between IT GRC and the overall or enterprise GRC, i.e., the described high level processes can be used enterprise-wide as a reference for GRC activities. Moreover, organizations should employ efforts to generate synergies and alignment between IT GRC, IT strategic goals and business strategy (Damianides, 2005; Jonkers *et al.*, 2004), since the role of IT in GRC is twofold; on the one hand as the main catalyst and, on the other hand, as a part of the organization that can benefit from integrated GRC activities.

Additionally, some criticism can be raised in what concerns the models in terms of their applicability. The application layer was instantiated in a project supported by Methodus Inovação. However, the business layer and its relation with the application layer were not tested in any specific situation.

Another issue that can be pointed out is why to start with a business approach (top-down approach), instead of a technological approach (bottom-up approach, for instance, using a GRC solution available in the market). We can highlight several valid reasons. One reason is based on having more knowledge from the business perspective. Also, by taking a top-down approach, the construction of a complete enterprise architecture is more dynamic and flexible. Furthermore, what is more important in GRC is to determine how to integrate the processes of the three

subjects in order to boost the transparency, organization's health and competitive advantage.

As the design of the architecture moved forward, the importance of the conceptual model in this research raised, since the architecture, yet more concrete, manifested a clear alignment with the concepts and relations of the conceptual model.

The use of the TOGAF ADM also proved to be a good choice, since it provided a good method to design the architecture. The use of ArchiMate combined with the ADM covered a good part of the content metamodel from TOGAF.

Finally, it is noteworthy to recognize that the some models used in this research are part of the information systems knowledge base, thus reinforcing that design research artefacts can and should be employed in order to build new ones (Aier & Gleichauf, 2010).

Chapter 5

Conclusion

More regulations are on the way, along with demanding transparency, accurate information about company operations, robust and comprehensive risk management, regulatory compliance and efficient governance.

Consequently, organizations are seeking to improve their GRC activities, by implementing integrated GRC solutions that provide a holistic view of the organization and help in the automation of activities. Last year (2010), spendings with governance, risk and compliance frameworks rose to $32 billion (Hagerty & Kraus, 2009). After analysing and researching the emerging domain of integrated GRC, the lack of scientific research is alarming and it is holding back improvements in integrated GRC.

In this research we proposed and evaluated two reference models: a conceptual model and a reference architecture. We addressed the problem of this dissertation in two ways. On the one hand, by contributing scientifically to the information systems knowledge base of this domain. On the other hand, using the same knowledge to get and induce know-how into professionals of this domain, thus narrowing the distance between theory and practice (Fitzgerald, 2003). To accomplish this proposal, we used concepts that are familiar to both practitioners and academics - the TOGAF ADM and ArchiMate - in order to break down language barriers that often induce obstacles to progress in some areas (Lang, 2003).

5.1 Future Work

Plenty of research can be performed using this research as basis. Several ideas came from professionals of this domain. For example, assessments in organizations could be performed

using the models proposed by this research. Specifically speaking, the maturity of organizations could be assessed using the reference architecture and the conceptual model.

A fact verified was that many organizations have individual applications and processes to address particular areas (for example, risk management or audit management). The definition of normalized interfaces for the diverse application modules using the normalized systems theory is a path worth to explore. This way organizations could acquire software that followed the right specifications to facilitate integration. The expensive price of all-in-one GRC suites could have some leverage around this topic.

Finally, exploring the detail level of the architecture - mainly at the business level - is a right path to make important improvements in this domain.

Bibliography

AIER, S. & GLEICHAUF, B. (2010). Applying Design Research Artifacts for Building Design Research Artifacts: A Process Model for Enterprise Architecture Planning. In R. Winter, J.L. Zhao & S. Aier, eds., *Design Science Research in Information Systems and Technology*, vol. 6105 of *LNCS*, 333–348, Springer.

BANHAM, R. (2007). Is GRC ERM? Or Vice Versa? *Treasury & Risk*, 48–50.

BASTOS, A.M., LIMA FILHO, A.D.S. & NERY DE OLIVEIRA, J.F. (2010). Continuous Governance, Risk and Compliance Management. Patent Application, uS 2010/0324952 A1.

BRACHE, A.P. (2001). *How Organizations Work: Taking a Holistic Approach to Enterprise Health*. Wiley.

BROCKE, J.V. & BUDDENDICK, C. (2006). Reusable Conceptual Models - Requirements Based on the Design Science Research Paradigm. In *First International Conference on Design Science Research in Information Systems and Technology*.

CHATTERJEE, A. & MILAM, D. (2008). Gaining Competitive Advantage from Compliance and Risk Management. In D. Pantaleo & N. Pal, eds., *From Strategy to Execution*, 167–183, Springer Berlin Heidelberg.

COSO (2004). Enterprise Risk Management - Integrated Framework. www.coso.org.

DAMERI, R.P. (2009). Improving the benefits of it compliance using enterprise management information systems. *Information Systems Journal*, **12**, 27 – 38.

DAMIANIDES, M. (2005). Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. *IS Management*, **22**, 77–85.

EL KHARBILI, M., STEIN, S., MARKOVIC, I. & PULVERMÜLLER, E. (2008). Towards a Framework for Semantic Business Process Compliance Management. In *The Impact of Governance, Risk, and Compliance on Information Systems (GRCIS)*, vol. 339 of *CEUR Workshop Proceedings*, 1–15, Montpellier, France.

FITZGERALD, B. (2003). Introduction to the special series of papers on, Informing each other: Bridging the gap between Researcher and Practitioners. *Informing Science*, **6**, 13–19.

FRANK, U. (1999). 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 (AMCIS99)*, 695–698, Association for Information Systems, Milwaukee.

FRANK, U. (2006). Evaluation of Reference Models. In P. Fettke & P. Loos, eds., *Reference Modeling for Business Systems Analysis*, 118–140, Idea Group.

FRIGO, M.L. & ANDERSON, R.J. (2009). A Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*.

GERICKE, A., FILL, H.G., KARAGIANNIS, D. & WINTER, R. (2009). Situational Method Engineering for Governance, Risk and Compliance Information Systems. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, DESRIST '09, 24:1–24:12, ACM, New York, NY, USA.

GILL, S. & PURUSHOTTAM, U. (2008). Integrated GRC - Is your Organization Ready to Move? In *Governance, Risk and Compliance*, 37–46, SETLabs Briefings.

GODELLAWATTA, G. (2009). Compliance after the global crisis. *Association of Professional Bankers SRI Lanka*.

HAGERTY, J. & KRAUS, B. (2009). GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency. http://www.oversightsystems.com/pdf/whitepapers/AMR-GRC-in-2010.pdf.

HALTTUNEN, V. (2004). Using Reference Architectures in Enterprise Modelling. Tech. rep., Information Technology Research Institute.

HEVNER, A.R., MARCH, S.T., PARK, J. & RAM, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, **28**, 75–106.

IACOB, M.E., JONKERS, H., LANKHORST, H.M. & PROPER, E. (2009). ArchiMate 1.0 Specification. Tech. rep., The Open Group.

IEEE (2000). IEEE Recommended Practice for Architectural Description of Software-Intensive Systems. *October*, i–23.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, (2009). The Risk IT Framework - Principles - Process Details - Management Guidelines - Maturity Models.

ISO19011 (2002). Guidelines for quality and/or environmental management systems auditing.

ISO31000 (2009). Risk management - Principles and guidelines.

ISO/IEC38500 (2008). Corporate governance of information technology.

JONKERS, H., LANKHORST, M., BUUREN, R.V., BONSANGUE, M. & TORRE, L.V.D. (2004). Concepts for Modeling Enterprise Architectures. *International Journal of Cooperative Information Systems*, **13**, 257–287.

JONKERS, H., PROPER, E. & TURNER, M. (2009). TOGAF™ 9 and ArchiMate® 1.0.

LANG, M. (2003). Communicating Academic Research Findings to IS Professionals: An Analysis of Problems. *Informing Science*, **6**, 21–29.

LANKHORST, M. & VAN DRUNEN, H. (2007). Combining TOGAF and ArchiMate. www.via-nova-architectura.org.

LLANAJ, G. (2010). Meeting the Challenges of Governance, Risk and Compliance. http://www.sas.com/reg/wp/corp/9137.

MCCUAIG, B. (2010). Building a Business Case For Governance, Risk and Compliance (GRC). http://paisley.thomsonreuters.com.

MITCHELL, S.L. (2007). GRC360: A Framework to help Organisations drive Principled Performance. *International Journal of Disclosure and Governance*, **4**, 279–296.

MOERDLER, M.L., BOSWELL, C.S., DATSKOVSKY, G., SWAMINATHAN, M., DIEBOLD, B.R., DING, Y. & BENTON, J.D. (2009). System and Method for Governance, Risk, and Compliance Management. Patent Application, uS 2009/0319312 A1.

MOODY, D.L. & SHANKS, G.G. (2003). Improving the Quality of Data Models: Empirical Validation of a Quality Management Framework. *Inf. Syst.*, **28**, 619–650.

MOODY, D.L., SINDRE, G., BRASETHVIK, T. & SØLVBERG, A. (2003). 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 '03, 295–305, IEEE Computer Society, Washington, DC, USA.

NAMIRI, K. & STOJANOVIC, N. (2007). A Formal Approach for Internal Controls Compliance in Business Processes. In *Business Process Modeling, Development and Support 2007. 8th Workshop on BPMDS in Conjunction with CAiSE 2007*, 1–9.

OCEG (2009). GRC Capability Model. http://www.oceg.com.

OFFERMANN, P., LEVINA, O., SCHÖNHERR, M. & BUB, U. (2009). Outline of a design science research process. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, DESRIST '09, 7:1–7:11, ACM, New York, NY, USA.

ÖSTERLE, H., BECKER, J., FRANK, U., HESS, T., KARAGIANNIS, D., KRCMAR, H., LOOS, P., MERTENS, P., OBERWEIS, A. & SINZ, E.J. (2011). Memorandum on Design-Oriented Information Systems Research. *EJIS*, **20**, 7–10.

PMI (2004). *A Guide To The Project Management Body Of Knowledge (PMBOK Guides)*. Project Management Institute.

PRICEWATERHOUSECOOPERS (2004). 8th Annual Global CEO Survey. http://www.grc-resource.com/resources/pwc_8th_ceo_survey.pdf.

RACZ, N., PANITZ, J., AMBERG, M., WEIPPL, E. & SEUFERT, A. (2010a). Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises. In *Proceedings of the 21st Australasian Conference on Information Systems (ACIS)*, Brisbane, Australia.

RACZ, N., SEUFERT, A. & WEIPPL, E. (2010b). A Process Model for Integrated IT Governance, Risk, and Compliance Management. In *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*, 155–170, Riga, Latvia.

RACZ, N., WEIPPL, E. & SEUFERT, A. (2010c). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In B.D. Decker & I. Schaumüller-Bichl, eds., *Communications and Multimedia Security*, vol. 6109 of *LNCS*, 106–117, Springer.

RACZ, N., WEIPPL, E. & SEUFERT, A. (2011). Governance, risk & compliance (grc) software - an exploratory study of software vendor and market research perspectives. In *HICSS*, 1–10, IEEE Computer Society.

RASMUSSEN, M. (2010a). Achieve GRC Value: Efficient Business Process and Application Monitoring. http://www.corp-integrity.com/grc-fundamentals/achieve-grc-value-efficient-business-process-and-application-monitoring.

RASMUSSEN, M. (2010b). Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise. http://www.corp-integrity.com/wp-content/uploads/2010/12/2010-11-Collaborative-Accountability-in-Policy.pdf.

RASMUSSEN, M. (2010c). GRC Reference Architecture: Understanding the Landscape of GRC Software. http://www.corp-integrity.com/grc-fundamentals/grc-reference-architecture-making-sense-of-the-grc-technology-landscape.

RASMUSSEN, M. (2011). GRC 2011: Gripes & Directions. http://www.corp-integrity.com/compliance/grc-2011-gripes-directions.

RATH, M. & SPONHOLZ, R. (2009). *IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen*. Schmidt.

SCHELP, J. & WINTER, R. (2009). Language communities in enterprise architecture research. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, DESRIST '09, 23:1–23:10, ACM.

SCHERMANN, M., BÖHMANN, T. & KRCMAR, H. (2009). Explicating Design Theories with Conceptual Models: Towards a Theoretical Role of Reference Models. In J. Becker, H. Krcmar & B. Niehaves, eds., *Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik*, 175–194, Physica-Verlag HD.

SCHON, D.A. (1983). *The Reflective practitioner: How Professionals Think in Action*. Basic Books, New York.

SCHUMM, D., LEYMANN, F., MA, Z., SCHEIBLER, T. & STRAUCH, S. (2010). Integrating Compliance into Business Processes: Process Fragments as Reusable Compliance Controls. In Schumann/Kolbe/Breitner/Frerichs, ed., *Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI'10), Göttingen, Germany, February 23-25, 2010*, 2125–2137, Universitätsverlag Göttingen, Göttingen.

SHANKS, G., TANSLEY, E. & WEBER, R. (2003). Using Ontology to Validate Conceptual Models. *Commun. ACM*, **46**, 85–89.

SHEN, W., CAMARINHA-MATOS, L. & AFSARMANESH, H. (2006). Towards a Reference Model for Collaborative Networked Organizations. In *Information Technology For Balanced Manufacturing Systems*, vol. 220 of *IFIP International Federation for Information Processing*, 193–202, Springer Boston.

SIMON, H.A. (1996). *The Sciences of the Artificial - 3rd Edition*. The MIT Press, 3rd edn.

SOFTWARE ENGINEERING INSTITUTE, (2010). Capability Maturity Model Integration for Development. Version 1.3.

SUMNER BLOUNT DIRECTOR, (2009). The Policy Lifecycle. http://www.thecomplianceauthority.com/the-policy-lifecycle.php.

TAKEDA, H., VEERKAMP, P., TOMIYAMA, T. & YOSHIKAWA, H. (1990). Modeling Design Processes. *AI Mag.*, **11**, 37–48.

TARANTINO, A. (2008). *Governance, Risk and Compliance Handbook : Technology, Finance, Environmental and International Guidance and Best Practices*. John Wiley & Sons, Hoboken, N.J.

THE OPEN GROUP (2009). TOGAF 9 - The Open Group Architecture Framework Version 9.

VAISHNAVI, V.K. & KUECHLER, W. (2008). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*. Auerbach Publications, Boca Raton, FL, USA, 1st edn.

VICENTE, P. & MIRA DA SILVA, M. (2011a). A Business Viewpoint for integrated IT Governance, Risk and Compliance. In *Proceedings of the 1st International Workshop on IT GRC held in Conjunction with the 7th World Congress on Services (SERVICES 2011)*, IEEE, Washington.

VICENTE, P. & MIRA DA SILVA, M. (2011b). A Conceptual Model for Integrated Governance, Risk and Compliance. In H. Mouratidis & C. Rolland, eds., *23rd International Conference on Advanced Information Systems Engineering*, vol. 6741 of *LNCS*, 199–213, CAiSE'11, Springer, London.

WAGNER, S. & DITTMAR, L. (2006). The Unexpected Benefits of Sarbanes-Oxley. *Harvard Business Review*.

ZACHMAN, J.A. (1987). A framework for information systems architecture. *IBM Syst. J.*, **26**, 276–292.

Appendix A

Scientific Publications

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).

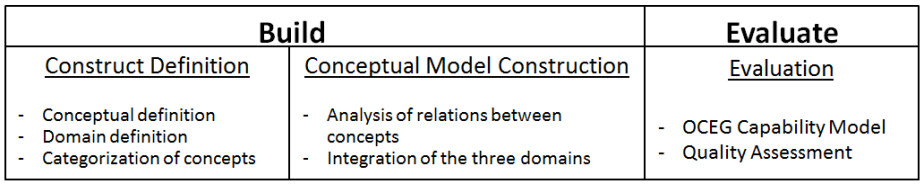

Fig. 1. Research Methodology

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

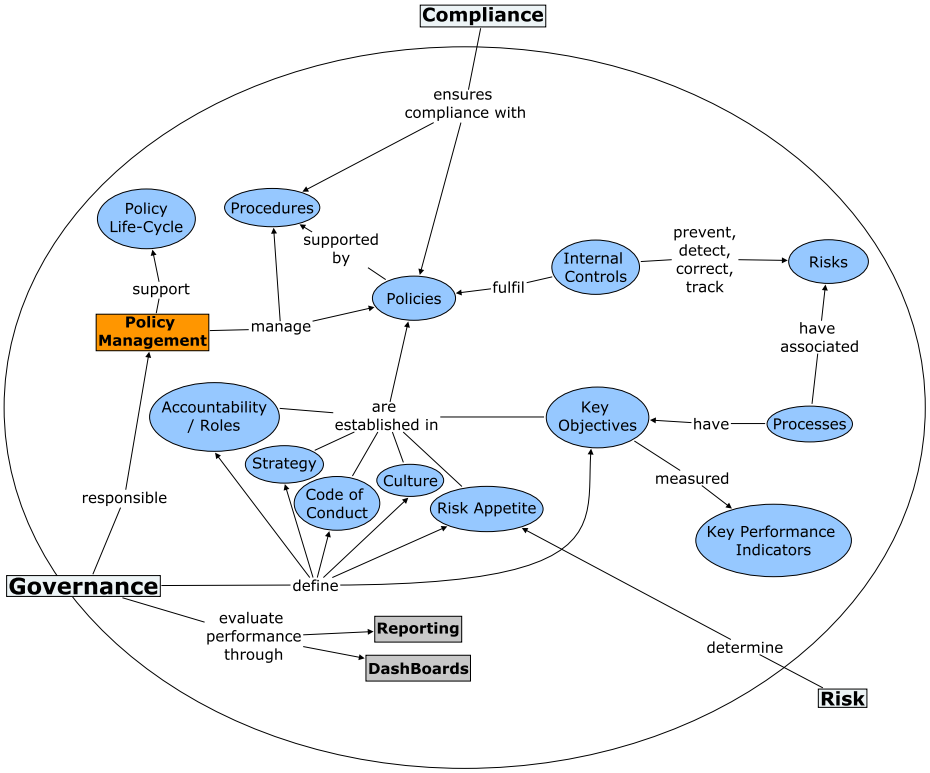

Fig. 2. Conceptual Model for Governance

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

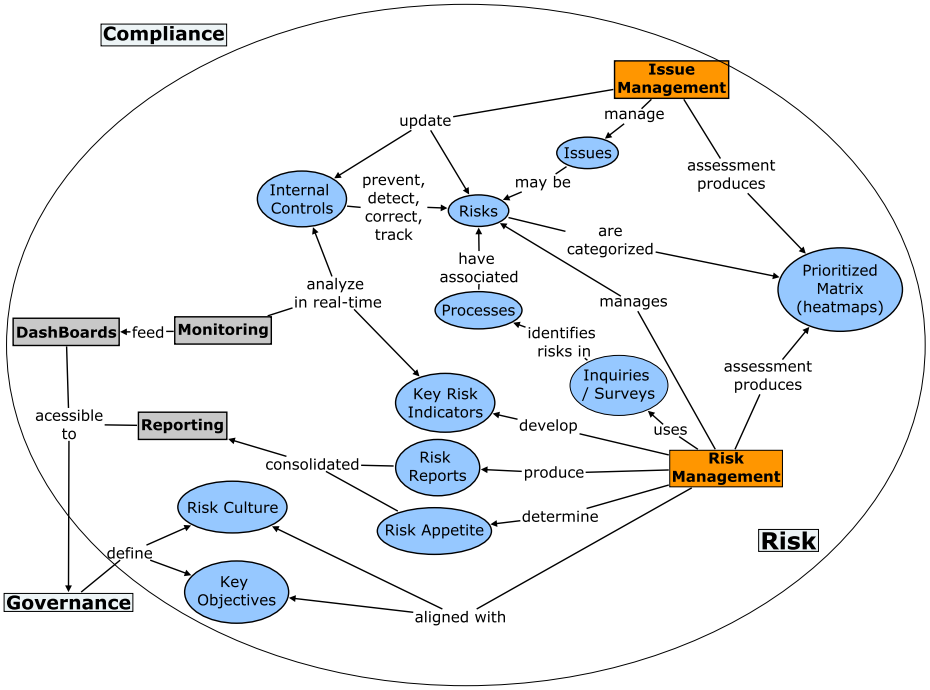

Fig. 3. Conceptual Model for Risk Management

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

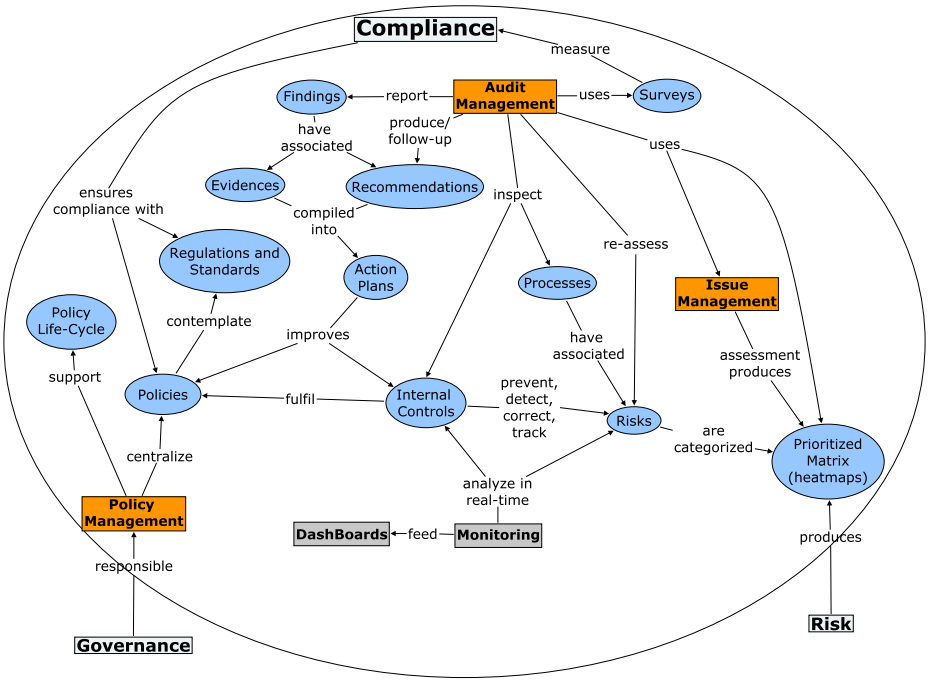

Fig. 4. Conceptual Model for Compliance

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.

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.

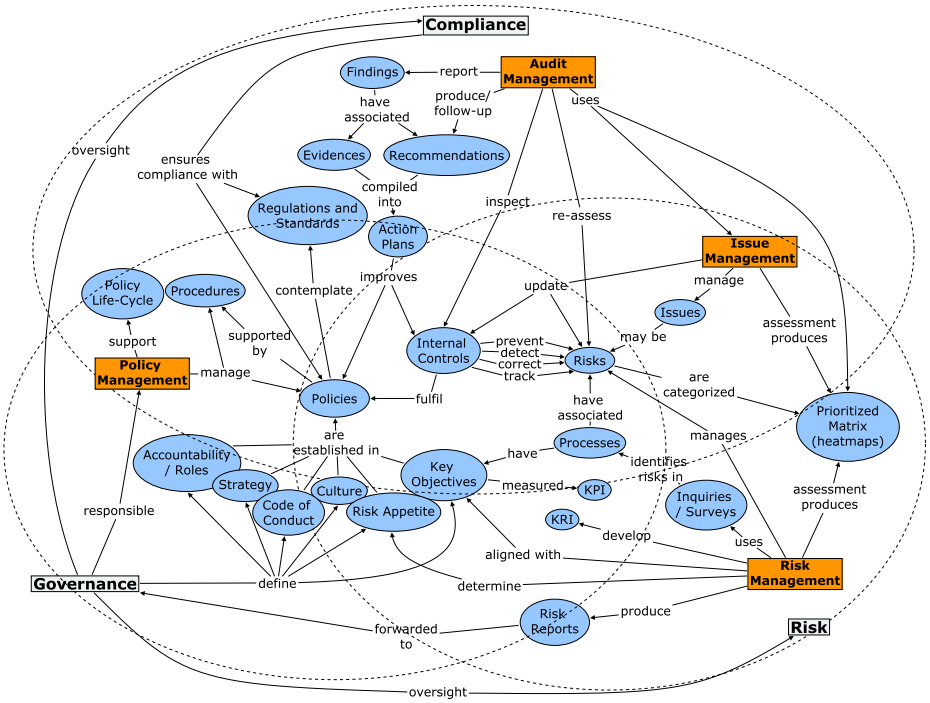

Fig. 5. Integrated GRC Conceptual Model

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).

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].

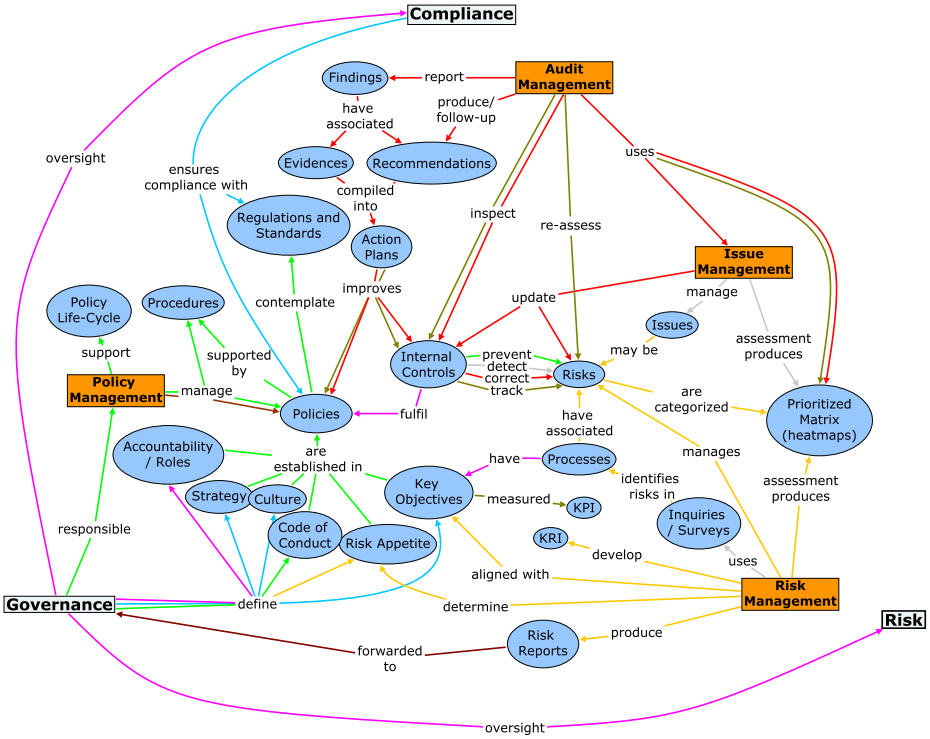

Fig. 6. Mapping between the Reference Model and the OCEG Capability Model

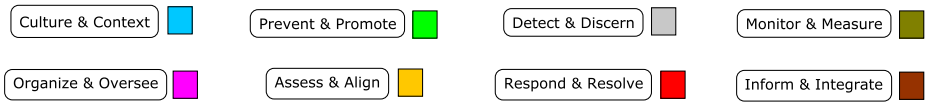

Fig. 7. GRC Capability Model Components

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].

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

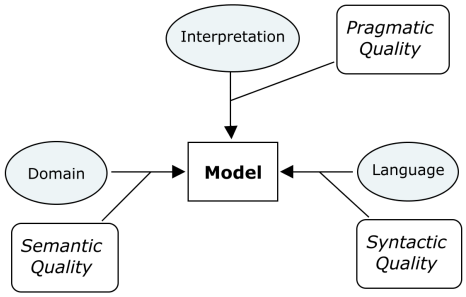

Fig. 8. Conceptual Model Quality Framework - adapted from [19]

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/pwc8thceosurvey.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.blogspot.com/2010/02/defining-policy-management-lifecycle.html
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/documents/AchieveGRCValue-EfficientBusinessProcessandApplicationMonitoring.pdf

A Business Viewpoint for Integrated IT 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*—Due to increasing requirements, standards and tight oversight from governments, along with the immediate need to effectively manage the increasing business and operational risks inherent to competing in a complex global market, integrated Governance, Risk and Compliance (GRC) is becoming one of the most important business requirements for organizations. In particular, IT requirements, standards and best practices play a crucial role in IT organizations/departments. The lack of guidance in this domain, namely scientific research, results in unaided attempts to improve efficiency and effectiveness in organizations.**

In this paper we propose a business architecture that describes the integration of the main processes for IT Governance, IT Risk Management and IT Compliance (IT GRC). Based on a process model for IT GRC and a conceptual model for GRC, we use ArchiMate to model the behavioural, structural and informational structure of the business viewpoint - business processes, roles and business objects respectively. To end with, we discuss the final result and draw some conclusions about the constructed artifact.

***Keywords*-governance; risk; compliance; business viewpoint; integrated; IT GRC**

I. INTRODUCTION

The business environment has been experiencing an unprecedented series of issues, surprises, and negative events that have increased the focus on the adequacy of organizations Governance, Risk and Compliance (GRC) activities [1].

Over the last few decades, many corporate disasters impacted business unfavourably and rudely forced governments to act (e.g., LTCM, Enron, Sub-prime, Societe General, WorldCom, etc.) [2]. Widespread damage caused by these disasters eroded the trust government and people had in corporations, and resulted in the enactment of multiple regulations like Basel II, Sarbanes-Oxley Act (SOX), Anti-Money Laundering (AML), etc. [2], [3]. Additionally, with the financial crisis fresh on the regulators mind, boards are impelled not only to review their GRC activities, in accordance to the law, but also to better understand how to transform their GRC activities from a burden to an advantage [4].

If performed right, integrating GRC activities will undoubtedly improve both the effectiveness and efficiency of many internal functions of organizations. To assist this mission, IT is comprehensive: On the one hand as the main catalyst and, on the other hand, as a part of the organization that can benefit from integrated GRC activities.

Nowadays, best practices, frameworks and standards such as ITIL, COBIT and ISO/IEC 27001, represent a distinctive factor in the market. Although is difficult to demonstrate that they leverage competitive advantage [5], ultimately it leads to value creation [6]. For example, COBIT implementation can help in the implementation of SOX used in conjunction with COSO-ERM [6], [7]. This advantage consists in frameworks and methodologies that point out optimum approaches to address business and IT needs. As in the overall GRC, having IT processes, risks and controls interconnected with IT activities results in enhanced performance, improved processes and internal controls, decision making, tracking and monitoring risks, etc. [8]. In other words, it is irrelevant whether we are talking about IT GRC or enterprise GRC. What organizations need is a holistic, enterprise-wide and systematic approach to governance, risk and compliance resulting in a deeper understanding of what is going on in a business.

How can this be achieved? The ideal perspective is to identify, integrate and optimize processes and activities that are common and related across the GRC domain. To accomplish this, breaking silos and "interface" definition are needed within the organization. What are the processes of GRC, and what business information is exchanged?

Does Information Systems research play a role in this matter? In the authors' opinion, yes. Scientific research techniques and methodologies can help define and describe artifacts in a specific and independent manner. However, and according to Fitzgerald [9], the gap between researchers and professionals may be an obstacle to progress in this area. Breaking down language barriers is paramount to obtain results that are both useful to researchers and professionals [10]. To try to overcome this barrier, in this paper we will use a modelling language - ArchiMate - since it presents itself as an independent, complete and comprehensible modelling language used to better describe architectures to the organization's stakeholders.

In this specific case, a business reference architecture can help organizations develop and optimise their information management systems, that may be more suitable than standard GRC solutions [11]. Also, the effort to implement and design an in-house complete enterprise architecture that

supports GRC processes, is, nowadays, the most suitable and supported approach to integrated GRC [12].

The concept of architecture is defined as: ”The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution“ [13]. Architecture is positioned between business and IT [14], and in the GRC domain, the gap between business and IT is a major concern, since vendors are very focused on standard technological solutions and business knowledge is fragmented and inconsistent [15], [16]. Having this said, a complete architecture definition is paramount to align and serve both business and IT.

In this research paper the authors propose a part of a business architecture: a business viewpoint. The main goal is to describe a business viewpoint that clearly shows the integration points between governance, risk and compliance, thus providing more hints, or references, concerning the articulation of the three subjects. Another, and more secondary goal, is to verify the alignment between IT GRC and the overall GRC by using research from both areas' knowledge base.

II. Theoretical Background

In this section we gather and present all the scientific resources used throughout this research, starting with a reference for conducting GRC research, followed by the models and modelling language used to construct the final artifact.

A. Frame of Reference for GRC Research

As the concept of integrated GRC started reaching the scientific community, a very important step was made by Racz *et al.* [17], when they proposed the first scientific GRC definition in 2010. The definition 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.*"

This definition was translated into a frame of reference for GRC research comprising three core subjects (governance, risk and compliance), four components (strategy, processes, technology and people) and rules (risk appetite, internal policies and external regulations). Given the young age of scientific research around this topic, the definition and the frame of reference is indeed very helpful to better address research in GRC in an organized and coherent manner.

As we will unveil in the next sections, this paper specifically addresses processes and people components.

B. Process Model for IT GRC

The first process model for IT GRC [18] (see Fig. 1) was proposed through the analysis and combination of three references that address GRC as a separate topic: a process model from the ISO/IEC 38500:2008 for IT governance [19]; the COSO ERM framework for risk management [20]; and a generic model for IT compliance.

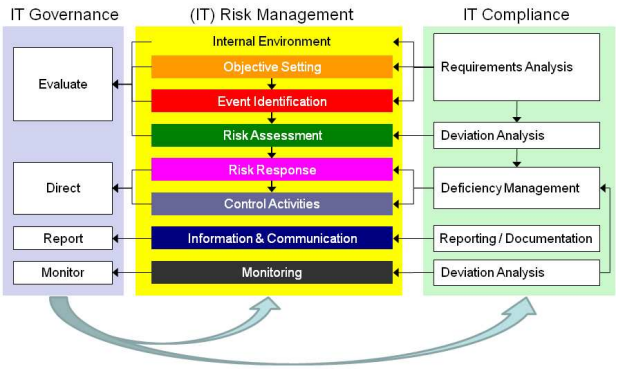

Figure 1. Process model for IT GRC [18]

Although the process model is directed at IT, the authors claim that the selection of the three references was made by taking into account the relation between IT GRC and the overall GRC.

In our opinion this process model brings added value to GRC research, since it untangles some high-level relations between governance, risk and compliance. However, it is not clear about the meaning of the relations between the components of the model. The authors also state that the process model is untested in terms of its applicability and that the selection of different references would be plausible.

C. Conceptual Model for GRC

With the objective of clearing out the real scope of GRC, Vicente and Silva [21] proposed a conceptualization of the domain (see Fig. 2). Following the approach of the process model of the previous section, the conceptual model was built by analysing each discipline individually and then merging the three scopes of governance, risk and compliance. This approach, also called *building blocks* [22] - a design research pattern - consists in dividing a "complex research problem into smaller problems that can form the building blocks for solving the original problem".

The conceptual model in Fig. 2 represents a high-level model, describing points of integration between governance, risk and compliance, through the identification of common concepts. Unlike the process model in the previous section, the relations between concepts are explicit and provide some hints as to the overall GRC behaviour. Additionally, the conceptual model is not specific for IT GRC.

However, the conceptual model was not fully evaluated, namely in terms of pragmatic quality. Moreover, it was

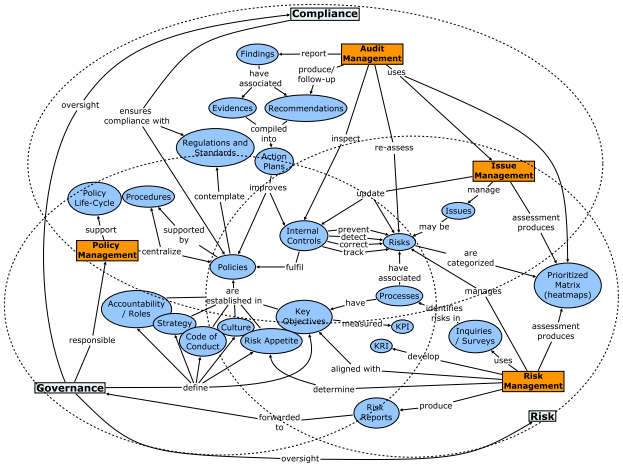

Figure 2. Conceptual model for GRC [21]

evaluated using only one reference - the GRC capability model from the Open Compliance & Ethics Group (OCEG) [23]. Although the GRC capability model, also known as *redbook*, is the most complete reference in the GRC domain, additional evaluation using other references could have been performed.

D. Archimate

ArchiMate is an open and independent enterprise architecture modelling language. It was developed in the Netherlands, in 2004, by a consortium led by the *Telematica Instituut* which allows the modelling of organizational architectures and recently became part of the Open Group.

ArchiMate presents a set of clear concepts and relations in architecture and offers a simple and uniform structure for describing the content of these domains [24]. Enterprise architecture is an important instrument in designing an enterprise-wide integration. ArchiMate supports a layered modelling approach essentially divided into three layers: business, application and technology architecture. Every entity in each level is categorized according to three aspects: structure, information and behaviour [25]. In this research paper we will focus on the business layer.

According to ArchiMate's business layer metamodel [25], we have selected (see Fig. 3) active and passive structures (roles/actors and business objects, respectively) and behaviour elements(business processes). Processes and business objects will be used to model the business viewpoint, whereas roles and actors will be describe separately, as we will explain in Sect. IV *C*.

A brief description of the proposed elements follows.

Business Process: A unit of internal behaviour or collection of causally related units of internal behaviour intended to produce a defined set of products and services.

Business Object: A unit of information of relevance from a business perspective.

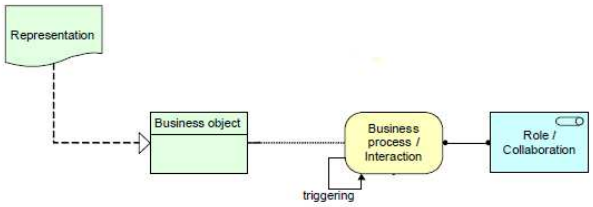

Figure 3. ArchiMate selected concepts

Business Role: An organizational entity that is capable of performing behaviour.

ArchiMate is a good alternative to UML, because it is more understandable, less complex and does support integration and alignment between the three layers through various viewpoints. The notion of viewpoint is not new. A viewpoint establishes the conventions by which a view is created, depicted and analysed, and determines the languages to be used to describe it [26]. In this research, we focus on the business process viewpoint, since it comprises and relates the majority of elements of the artifacts chosen for this research - processes and objects.

III. Research Methodology

The methodology applied in this research paper is divided into three stages (see Fig. 4).

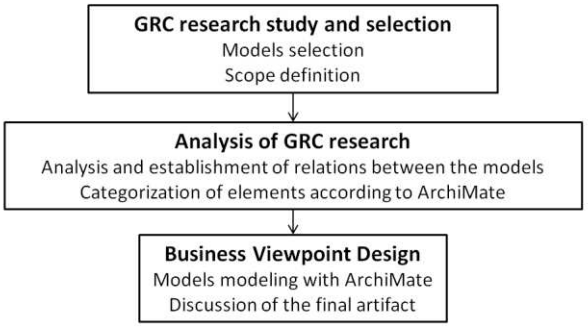

Figure 4. Research Methodology

In the first stage we selected and analysed recent research in GRC. Using only artifacts from the information systems knowledge base [27], we chose the most suitable and applicable ones for this research; a process model for IT GRC and a conceptual model for GRC. In order to avoid biased results, this selection had into account that each model was developed independently.

The reuse of models is a featured topic in design science research. The design "by reuse" process is based on existing models from the knowledge base. In more detail, reuse is conducted by taking parts of one or more original models, adapting and extending them in the resulting artifact [28].

After this selection a deeper analysis was required. In the second stage, both models were studied and a link between their elements was made. Also at this stage, and according to ArchiMate business layer meta-model, the elements were categorized into business objects, processes and roles.

Finally, the part of the business architecture was designed using the viewpoints that best portray the relations between elements.

IV. Business Viewpoint

Business architecture provides a multifaceted view of the organization's key components. It bridges the gap between an organizations's strategic business intent and real-world capabilities comprising processes, behaviour and information dimensions [29].

As stated in Sect. II *D*, the business viewpoint will be developed using the ArchiMate modelling language.

In order to start the construction of the viewpoint, we will convert the models that support this research to the chosen modelling language, ArchiMate.

A. Using ArchiMate to model the process model for IT GRC

The model presents one type of concept and three types of relations (see Fig. 5). The dashed rectangular boxes - IT Governance, (IT) Risk Management and (IT) Compliance - show a group relation. The grouping relationship indicates that objects belong together based on some common characteristic [25]. The elements inside the grouping relationship represent high-level processes and are the same as the process model for IT GRC (see Fig 1).

The filled arrows between processes indicate a trigger event, i.e., the flows between processes. The dashed relations with a tag *flow* represent the exchange of information amongst processes.

B. Merging the Conceptual Model for GRC

Through the analysis of the conceptual model (Fig. 2) and the process model (Fig. 1) a business process viewpoint was built, composed by processes and objects - represented between the grouping relationships.

The *flow* relations presented in Fig. 5 were replaced with business objects retrieved from the conceptual model (see Fig. 6).

We will now describe the logic of the constructed artifact.

Business process viewpoint analysis: Starting with the Evaluate process of IT Governance, the conceptual model establishes as the responsibility of governance, the definition of strategy, culture, risk appetite, key objectives and policies. This clearly indicates how the organization is controlled and evaluated.

Based on these concepts, the first processes of risk management have all the information needed to establish the internal environment and objectives (Internal Environment and Objective Setting). The COSO ERM [20] describes

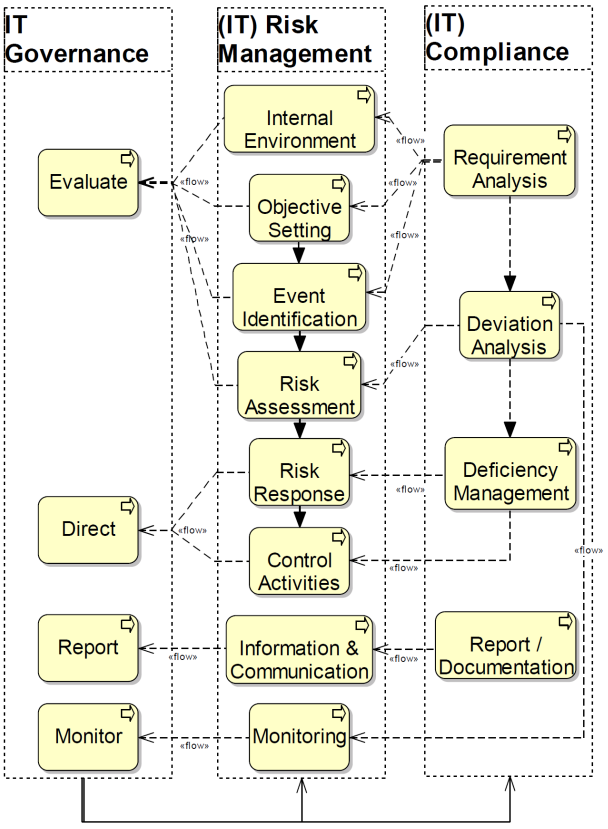

Figure 5. Process model for IT GRC [18] modeled with Archimate

internal environment as the establishment of the entity's risk culture, ethics and risk appetite. Additionally, key objectives, risk appetite and the strategy established are requirements to properly identify events that should be aligned with the organization's concerns. These events, that have already occurred (issues) or may occur (risks), can be identified using self-assessment techniques through surveys. Compliance management must gather and convert all the external (regulations, laws, standards) and internal (internal policies and procedures) obligations into policies, in order to complete the requirement analysis process.

Once the requirement analysis is complete, the deviation analysis can be performed through audits or self-assessments. Also, the already identified issues and risks (events) should be marked for review. This is where the risk assessment process is important: to prioritize risks in terms of its impact, probability and velocity.

From the risk assessment and deviation analysis, a response to the risks and findings produced by the audit teams must be conducted (Deficiency management). Action plans and risk response strategies are produced, resulting in the improvement of internal controls that play an essential role to prevent, detect, correct and track risks, and that, as a result, fulfil the control goals that need to be established

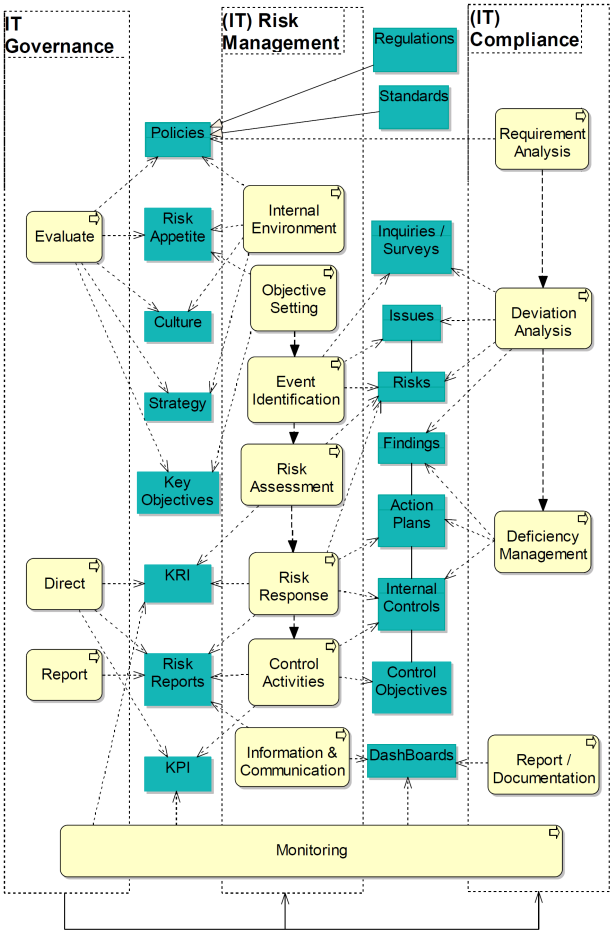

Figure 6. Business Process Viewpoint

(control activities).

The processes described represent activities and measures taken to minimize the impact of risks and issues, as well as, to enhance internal controls and, thus, processes, while increasing the level of compliance and decreasing the risk exposure of the organization.

Additionally, and along the previously mentioned processes, governance manages the outputs from risk and compliance processes, namely indicators - Key Risk Indicators (KRI) and Key Performance Indicators (KPI) - among others - and risk and compliance reports that transmit the current organization-wide status of residual risks, controls, policies and compliance levels. The analysis and exchange of information across the levels of the organization is supported by reporting and monitoring processes that provide reliable and real-time information through dashboards and reports.

In the business process viewpoint presented in Fig. 6, we extended the monitoring process to governance, risk and compliance, since it is present in all three sub-domains.

After this description, it can be stated that both models complete each other, leading to a business process viewpoint comprising the processes and the business objects used between them. On the one hand, this demystifies the relations of the process model and, on the other hand, it organizes and provides more structure to both models.

C. Actors and Roles

Breaking down silos means new structure in organizations. This leads to new roles, enhanced processes, common vocabulary and approach [30]. Actors and its roles are paramount to correctly perform GRC activities, but everyone needs to know what to do, and when. This can be facilitated using workflow systems with static and dynamic processes and tasks to help collaborators perform their duties [21]. Once again, IT plays a crucial role not only in the efficiency and effectiveness of GRC activities, but also in information quality and reduced errors.

ArchiMate defines active elements as the organisation structure, and a business actor is defined as an organizational entity capable of (actively) performing behaviour . Most notably, the actor role is also used to denote who performs, or is assigned, to (one or more) business roles. Examples of business actors are humans, departments, and business units.

To describe roles and actors for this business layer, the authors chose not to represent them with ArchiMate and include them into a viewpoint. The main reason for this choice lies in the fact that the elements that constitute the architectural layer are too abstract to define precise roles and link them to processes. As a matter in fact, the processes and objects presented in Fig. 1 are so high-level that the most likely outcome would be too much roles assigned to several processes (and vice versa). Also, insight concerning actors and roles is not presented in the models used to conduct this research. Nevertheless, the correct definition of roles in organizations is very important, because actors are the main enablers of processes.

Having this said there are some examples of actors, roles and categories that can be pointed out, based on some literature review [2], [30]:

- Leadership and champions
- Oversight personnel
  - Board of Directors
- Strategic personnel
  - C-suite - Chief Information Officer, Chief Compliance Officer, Chief Audit Executive, Chief Financial Officer, Chief Risk Officer, Chief Operations Officer.
  - Information Systems and System owners
  - Process owners
- Operational personnel
  - Key-users
  - Governance, risk, audit, controls, legal and compliance managers.

This categorization was made according to Mitchel [30] and reinforces that GRC involves individuals at all levels. Although this division is not very enlightening, it must be noted that this division does indeed make sense, since on the one hand, the operational personnel is more linked to processes and objects shared between risk management and compliance and, on the other hand, strategic and oversight personnel are more related with governance.

V. Discussion

Given the nature of both models used in this research, the business viewpoint still represents a high level approach to GRC. Moreover, this research does not go any further on pointing out how the constructed artifact can be accomplished in a specific situation. Nevertheless, the junction of the process and conceptual model bring added value to research in GRC, since it gathers more clues concerning the integration of GRC.

Although the title of this research is directed at IT GRC scope, we have used a non-IT specific conceptual model and a process that was built to the IT GRC scope but that has an obvious relation to the overall GRC. The proposed business viewpoint is good evidence that there is a clear alignment between IT GRC and the overall or enterprise GRC, i.e., the described high level processes can be used enterprise-wide as a reference for GRC activities. Moreover, organizations should employ efforts to generate synergies and alignment between IT GRC, IT strategic goals and business strategy [31], [32].

Additionally, some criticism can be raised in what concerns the models in terms of their individual applicability. As a favourable point, the junction of the two models provides a more structured approach to the process and conceptual model. Moreover, the positive combination of the models confirms the quality and validity of both and shows that GRC research is also aligned.

Another issue that can be pointed out is why to start with a business approach (top-down approach), instead of a technological approach (bottom-up approach, for instance, using a GRC solution available in the market). We can highlight several valid reasons. One reason is based on having more knowledge from the business perspective. Also, by taking a top-down approach, the construction of a complete enterprise architecture is more dynamic and flexible. Furthermore, what is more important in GRC is to determine how to integrate the processes of the three subjects in order to boost the transparency, organization's health and competitive advantage.

Finally, it is noteworthy to recognize that both models and the frame of reference used are part of the information systems knowledge base, thus reinforcing that design research artifacts can and should be employed in order to build new ones [33].

VI. Future Research

In future research the next steps will be to complement a business architecture using more elements that might be missing, given the high-level nature of the artifacts used. Additionally, the remaining architectural layers will be designed for a complete enterprise architecture, namely information systems and technology architecture. Also, the use of ArchiMate viewpoints can help in the designing process, since it comprises viewpoints that help in the alignment of all architecture layers [25].

VII. Conclusion

In this research paper we developed and discussed a business viewpoint for IT GRC by joining two high-level models for integrated GRC - a process model for IT GRC and a conceptual model for GRC. The models complete each other very well, resulting in a better, more complete and more structured artifact.

The research at hand does not only increments the information systems research knowledge base, but also uses recent references from the knowledge base itself.

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] M. L. Frigo and R. J. Anderson, "A Strategic Framework for Governance, Risk, and Compliance," *Strategic Finance*, 2009.

[2] A. Tarantino, *Governance, Risk and Compliance Handbook : Technology, Finance, Environmental and International Guidance and Best Practices*. John Wiley & Sons, Hoboken, N.J., 2008. [Online]. Available: http://www.loc.gov/catdir/enhancements/fy0745/2007038100-t.html

[3] S. Gill and U. Purushottam, "Integrated GRC - Is your Organization Ready to Move?" in *Governance, Risk and Compliance*. SETLabs Briefings, 2008, pp. 37–46.

[4] S. Wagner and L. Dittmar, "The Unexpected Benefits of Sarbanes-Oxley," *Harvard Business Review*, April 2006.

[5] P. C. B. de Oliveira, N. F. da Silva, and M. M. da Silva, "A process for estimating the value of itil implementations," in *Conference on Enterprise Information Systems (CENTERIS 2009)*. Springer-Verlag, October 2009.

[6] G. Hardy, "Using it governance and cobit to deliver value with it and respond to legal, regulatory and compliance challenges," *Information Security Technical Report*, vol. 11, no. 1, pp. 55 – 61, 2006.

[7] C. Magnusson, "Corporate governance, internal control and compliance," September 2007.

[8] G. Llanaj, "Meeting the Challenges of Governance, Risk and Compliance," http://www.sas.com/reg/wp/corp/9137, 2010.

[9] B. Fitzgerald, "Introduction to the special series of papers on, informing each other: Bridging the gap between researcher and practitioners," *Informing Science*, vol. 6, pp. 13–19, 2003.

[10] M. Lang, "Communicating academic research findings to is professionals: An analysis of problems," *Informing Science*, vol. 6, pp. 21–29, 2003.

[11] R. P. Dameri, "Improving the benefits of it compliance using enterprise management information systems," *Information Systems Journal*, vol. 12, no. 1, pp. 27 – 38, 2009.

[12] N. Racz, J. Panitz, M. Amberg, E. Weippl, and A. Seufert, "Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises," in *Proceedings of the 21st Australasian Conference on Information Systems (ACIS)*, 2010, vortrag: ACIS 2010, Brisbane, Australia; 2010-12-01 – 2010-12-03.

[13] "Ieee recommended practice for architectural description of software-intensive systems," *October*, no. IEEE Std-1471-2000, pp. i–23, 2000.

[14] J. Schelp and R. Winter, "Language communities in enterprise architecture research," in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, ser. DESRIST '09. ACM, 2009, pp. 23:1–23:10.

[15] J. Hagerty and B. Kraus, "GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency," November 2009.

[16] M. Rasmussen, "GRC 2011: Gripes & Directions," January 2011. [Online]. Available: http://www.corpintegrity.com/compliance/grc-2011-gripes-directions

[17] N. Racz, E. Weippl, and A. Seufert, "A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)," in *Communications and Multimedia Security*, ser. Lecture Notes in Computer Science, B. D. Decker and I. Schaumüller-Bichl, Eds., vol. 6109. Springer, 2010, pp. 106–117.

[18] N. Racz, A. Seufert, and E. Weippl, "A process model for integrated it governance, risk, and compliance management," in *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*, 2010, pp. 155–170, vortrag: Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), Riga, Latvia; 2010-07-05 – 2010-07-07.

[19] *ISO/IEC 38500:2008 - Corporate governance of information technology*, ISO/IEC Std.

[20] COSO, "Enterprise Risk Management - Integrated Framework," www.coso.org, September 2004.

[21] P. Vicente and M. M. da Silva, "A Conceptual Model for Integrated Governance, Risk and Compliance," in *International Conference on Advanced Information Systems Engineering*, CAiSE. Springer, June 2011.

[22] V. K. Vaishnavi and W. Kuechler, *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*, 1st ed. Boca Raton, FL, USA: Auerbach Publications, 2008.

[23] OCEG, "GRC Capability Model," http://www.oceg.com, 2009.

[24] ArchiMate, "Why ArchiMate?" [Online]. Available: http://www.archimate.org/en/about_archimate/

[25] M.-E. Iacob, H. Jonkers, H. M. Lankhorst, and E. Proper, "ArchiMate 1.0 Specification," The Open Group, Tech. Rep., 2009.

[26] H. A. Proper, A. A. Verrijn-stuart, and S. Hoppenbrouwers, "Towards utility-based selection of architecture-modelling concepts," in *Proceedings of the Second AsiaPacific Conference on Conceptual Modelling (APCCM2005*. Australian Computer Society, 2004, pp. 25–36.

[27] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–106, 2004.

[28] J. V. Brocke and C. Buddendick, "Reusable conceptual models requirements based on the design science research paradigm," in *First International Conference on Design Science Research in Information Systems and Technology*, 2006.

[29] P. J. Wolfenden and D. E. Welch, "Business architecture: A holistic approach to defining the organization necessary to deliver a strategy." *Knowledge & Process Management*, vol. 7, no. 2, pp. 97 – 106, 2000.

[30] S. L. Mitchell, "GRC360: A Framework to help Organisations drive Principled Performance," *International Journal of Disclosure and Governance*, vol. 4, no. 4, pp. 279–296, November 2007. [Online]. Available: http://dx.doi.org/10.1057/palgrave.jdg.2050066

[31] M. Damianides, "Sarbanes-oxley and it governance: New guidance on it control and compliance," *IS Management*, vol. 22, no. 1, pp. 77–85, 2005.

[32] H. Jonkers, M. Lankhorst, R. V. Buuren, M. Bonsangue, and L. V. D. Torre, "Concepts for modeling enterprise architectures," *International Journal of Cooperative Information Systems*, vol. 13, pp. 257–287, 2004.

[33] S. Aier and B. Gleichauf, "Applying design research artifacts for building design research artifacts: A process model for enterprise architecture planning," in *DESRIST*, ser. Lecture Notes in Computer Science, R. Winter, J. L. Zhao, and S. Aier, Eds., vol. 6105. Springer, 2010, pp. 333–348.