TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

DISSERTATION

Governance, Risk & Compliance (GRC) for Information Systems: Towards an Integrated Approach

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der Sozial- und Wirtschaftswissenschaften unter der Leitung von

Privatdoz. Dipl-Ing. Mag.rer.soc.oec. Dr.techn. Edgar Weippl

und

O. Univ.-Prof. Dipl.-Ing. Dr. A Min Tjoa

E188/1
Institut für Softwaretechnik und Interaktive Systeme
Information and Software Engineering Group

eingereicht an der Technischen Universität Wien
bei der Fakultät für Informatik

von

Nicolas Racz

Matrikelnummer: e0727898
Meidlinger Hauptstr. 7/3/25, 1120 Wien
Email: nracz@grc-resource.com

Wien, am 17. Mai 2011

Unterschrift

Kurzfassung

Die Abkürzung „GRC” für Governance, Risk & Compliance hat in den letzten Jahren in Unternehmen stark an Aufmerksamkeit hinzugewonnen. Die primäre Bedeutung des Akronyms – ein Integrationsansatz für die drei GRC-Disziplinen – wurde jedoch bisher von der wissenschaftlichen Forschung ignoriert.

Für die Forschung im Bereich von Informationssystemen ist GRC auf zwei Arten relevant: als „GRC für IT” (IT GRC) und als „IT für GRC” (GRC Software). Die vorliegende Dissertation berücksichtigt beide Szenarien und zeigt die ersten Schritte in Richtung eines integrierten GRC-Ansatzes für Informationssysteme auf. Das primäre Ziel der Arbeit ist die Entwicklung eines Prozessmodels auf hoher Ebene für integrierte GRC im IT-Management. Das sekundäre Ziel ist es, zukünftige GRC-Forschung besser zu ermöglichen, indem Erkenntnisse bezüglich des Status Quo von GRC in Unternehmen bereit gestellt werden und eine wissenschaftliche Basis für GRC-Forschung geschaffen wird. Die Validität der Ergebnisse ist durch die Analyse von GRC in der Praxis, durch die Anwendung etablierter „Best Practice” Frameworks und durch Umfragen unter Experten gesichert.

Zur Erreichung der beiden Ziele ist das Forschungsprojekt in sechs Arbeitspakete (Kapitel 4-9) aufgeteilt. Zuerst gibt eine Publikationsstudie in Kapitel 4 einen Überblick über GRC Forschung, treibende Kräfte und Themen im Rahmen von GRC. Aus existierenden Definitionen und Umfragen wird eine wissenschaftliche Kurzdefinition abgeleitet und in einer Umfrage von GRC-Experten validiert. Basierend auf der Definition wird ein Forschungsrahmen erstellt. In Kapitel 5 werden die Ansichten von Softwareherstellern und Marktforschungsunternehmen anhand einer explorativen Umfrage analysiert. In Kapitel 6 wird der Status Quo von GRC und GRC Softwarenutzung in Großunternehmen anhand einer detaillierten quantitativen Umfrage untersucht. In Kapitel 7 wird das momentane Management von IT GRC in drei Großunternehmen erforscht, um den Fokus auf GRC im Umfeld der Informationstechnologie zu verschieben. Das achte Kapitel vergleicht Frameworks für Enterprise- und IT-Risikomanagement. Im letzten Schritt in Kapitel 9 wird ein Prozessmodell für integriertes IT GRC Management auf hoher Ebene entwickelt.

Die Dissertation leistet mehrere Beiträge zur Informationssystems-Forschung. Erkenntnisse bezüglich GRC-Publikationen und Perspektiven von Softwareherstellern und Marktforschungsunternehmen werden präsentiert. Der Status Quo von GRC, GRC

Software und IT GRC in Großunternehmen wird untersucht. Eine wissenschaftliche Basis für GRC-Forschung wird bereitgestellt. Zahlreiche Möglichkeiten für zukünftige Forschung in diesem Bereich werden vorgeschlagen. Die Redundanz separater IT-Risikomanagement-Frameworks wird identifiziert. Das Prozessmodell für IT GRC erklärt erstmalig die Integration von Governance, Risikomanagement und Compliance über die Prozesse der drei Disziplinen hinweg. Die Ergebnisse dieser Arbeit können von der Forschung verwendet werden, um über integrierte GRC im Allgemeinen und über die Beziehung von GRC zu Informationstechnologie im Speziellen zu lernen. Sie dient zudem zur Navigation in der GRC-Forschung und zur Entdeckung von neuen Forschungsmöglichkeiten.

Schlüsselworte: Governance, Risikomanagement, Compliance, GRC, Integration, Informationstechnologie

Abstract

Governance, Risk & Compliance (GRC) is an important topic in the business and technology world. The dominant notion of the acronym – an integrated approach to the three disciplines of GRC – has so far been ignored by scientific research.

For information systems research, GRC is relevant from the two perspectives of “GRC for IT” (IT GRC) and “IT for GRC” (GRC software). This dissertation considers both views, taking the first steps towards an integrated GRC approach for information systems. The primary goal is the development of a high-level process model for integrated governance, risk, and compliance in information technology management. The secondary goal is to enable future GRC research through provision of insights on the status quo of GRC in business and through creation of a scientific basis for GRC research. The validity of the results is ensured through analysis of GRC in practice, through application of widely used best practice frameworks and through surveys among experts.

To achieve the two goals the research project presented is subdivided into six research chapters. First, a literature review gives an overview of GRC research, of publications and of driving forces and topics within GRC. From existing definitions and surveys a scientific short-definition is derived and validated in a survey among GRC professionals. Based on the definition a frame of reference for research of GRC is constructed. Second, software vendor and market research perspectives on state-of-the-art GRC software are analysed by means of an exploratory survey. Third, the status quo of GRC and GRC software use in large enterprises is examined through a detailed quantitative survey. Fourth, in order to turn towards IT GRC the status quo of IT GRC management in three large enterprises is investigated. Fifth, enterprise and IT risk management frameworks are compared. Sixth and last, a high-level process model for integrated IT GRC management is developed.

The dissertation contributes to information systems research in several ways. Findings on GRC literature, software vendor and market research perspectives are presented. The status quo of GRC, GRC software, and IT GRC in large enterprises is examined. A scientific foundation for GRC research is provided and various possibilities for future research are identified. The redundancy of separate IT risk management frameworks is discovered. The process model for IT GRC for the first time explains the integration of governance, risk management, and compliance across processes of the three disciplines. The work at hand can be used by research to learn about integrated GRC and about its relation to IT, about how to navigate within GRC research, and about GRC research opportunities.

Keywords: governance, risk management, compliance, GRC, integration, information technology

Contents

Index of figures

Index of tables

List of abbreviations

AktG	Aktiengesetz
AS/NZS 4360:2004	Australian Standard / New Zealand Standard for Risk Management
BDSG	Bundesdatenschutzgesetz
BilMoG	Bilanzrechtsmodernisierungsgesetz
BS25999	Business Continuity Management Standard
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CISR	Center for Information Systems Research
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CWC	Chemical Weapons Convention
Directive 2006/43/EC	European Union 9th Council Directive / Directive on Statutory Audit
Directive 95/46/EC	European Union Data Protection Directive
DSG 2000	Bundesgesetz über den Schutz personenbezogener Daten
EBIT	Earnings Before Interest and Taxes
ERM	Enterprise Risk Management
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GRC	Governance, Risk & Compliance
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISO 9001:2008	Quality Management Standard
ISO 31000:2009	Risk management – Principles and Guidelines Standard
ISO/IEC 27000	Information Security Management Systems Standards
ISO/IEC 27001:2005	Standard for Information Security Management Systems Requirements
ISO/IEC 27005:2008	Information Security Risk Management Standard
ISO/IEC 38500:2008	Corporate Governance of Information Technology Standard
IT	Information Technology
ITC	IT Compliance

ITG	IT Governance
ITIL	IT Infrastructure Library
ITRM	IT Risk Management
IT GRC	IT Governance, Risk & Compliance
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
MaRisk	Mindestanforderungen an das Risikomanagement
OCEG	Open Compliance & Ethics Group
OGC	Office of Government Commerce
PCAOB	Public Company Accounting Oversight Board
SEC	United States Securities and Exchange Commission
SOx	Sarbanes-Oxley Act
URÄG	Unternehmensrechtsänderungsgesetz

Chapter 1. Motivation and relevance

The main factors that induced the motivation to carry out this research are explained in the first part of this chapter. In the second part the relevance of the research for business informatics is highlighted.

1.1 Motivation

An integrated approach to the three disciplines of governance, risk management, and compliance was first described in 2004 (PricewaterhouseCoopers, 2004) and is commonly referred to as "GRC". Since then the acronym has rapidly penetrated the world of business and information technology. It has made its way into software labels, service offerings, marketing slides, and department names in global enterprises. GRC came into existence as a response to an "unprecedented series of issues, surprises, and negative events that have increased the focus on the adequacy of organisations' governance, risk, and control activities" (Frigo & Anderson, 2009). Many of these issues and events belong to one of the following three categories:

i. **Governance scandals:** Over the last 15 years many companies suffered from large losses, fraud, and corruption scandals attributed to deficient internal control systems, or in other words, to insufficient corporate governance (Lattemann, 2010). Some examples include:
   - *Enron*: The case of Enron is probably the most infamous scandal of the last decade. For years the large US-American energy company generated fake profits through revenues with special purpose entities owned by Enron itself. Dubious accounting practices resulted in the preparation of fraudulent financial statements (Vinten, 2002; Benston & Hartgraves, 2002). When the whole scheme blew up, Enron went bankrupt in 2001. Right before the bankruptcy, its stock market value amounted to US-$ 60 billion. The Enron scandal also caused the dissolution of Arthur Andersen, back then one of the "big five" auditing firms with approximately 85,000 employees world-wide. Andersen was suspected to have cooperated in the preparation of financial statements, and later on was convicted of obstruction of justice for destroying evidence in the Enron case.

- *WorldCom*: Having come under competitive pressures the telecommunications company used fraudulent accounting practices to bloat its assets by US-$ 11 billion (Special Investigative Committee of the Board of Directors of WorldCom, Inc., 2003). When the fraud was covered up by internal audit and a subsequent investigation of the U.S. Securities and Exchange Commission (SEC) in 2002, WorldCom had to file for bankruptcy. CEO Bernard Ebbers was sentenced to 25 years in prison.
- *Parmalat*: By means of various fake transactions, the Italian food company generated fake sales amounting to a fraud scandal of at least € 8 billion. Empirical evidence seems to confirm shortcomings of Parmalat's monitoring structure and its failure to comply with several corporate governance standards and best practices (Melis, 2004).
- *Siemens*: The giant German-based technology company bribed clients all over the world in a large number of cases to seize deals (Balzi, Deckstein, & Schmitt, 2006). After a law prohibiting payments to clients abroad was introduced in Germany in 1999, Siemens continued the established scheme. They had to pay € 1.2 billion in fines to authorities in several countries, suffered large reputational losses, and several managers were convicted in German courts.
- *Lehman Brothers*: Due to its spectacular collapse the formerly renowned US-American investment bank is now irrevocably associated with the current global financial crisis. In the five years prior to its default in 2008, Lehman Brothers almost tripled its assets from US-$ 260 billion to US-$ 690 billion in 2007, generating earnings of US-$ 4.2 billion (Musura, 2010). But when the subprime market crashed, Lehman Brothers' large investments in that market turned into bad debt (Madhani, 2009). Due to a lack of sound governance, the company had an extremely high leverage ratio (i.e. the total-assets-to-equity ratio), and it borrowed more than 50% of its assets with short-term debt (Musura, 2010). The losses affected its credit-worthiness, preventing it from borrowing more capital. Hence the bank suffered a severe credit crunch that led to its collapse. Eventually Lehman Brothers had to file for bankruptcy in September 2008, leaving behind almost 30,000 employees, and debt of an estimated US-$ 200 billion to countless angry investors (Financial Times Deutschland, 2009).

These and many other scandals are widely attributed to a lack or failure of corporate governance in the respective companies that led to balance sheet manipulations, corruptive behaviour and risky adventures putting the companies' existence at stake (Mardjono, 2005).

ii. **Increased risk:** Risks for globally operating businesses today are immense. Today's world is characterised by unprecedented levels of interconnectedness between all areas of risk, known as systemic risk (World Economic Forum, 2010). The reasons for increasing risks are manifold:

   - *Instability of markets*: The last decade has seen increased turbulence in the economy. The crash of the dot-com bubble in 2001 and the global financial crisis that started in 2007 have demonstrated the instability of markets and of the global financial system (Riaz, 2009). The break-down of markets in countries such as Argentina (default in 2001), Greece, and Ireland (crisis in 2010) has shown that even countries formerly deemed stable may be threatened by defaults.
   - *Globalisation*: Globalisation has increased competitive pressure; new competitors, world-wide supply chains and expansion into global markets introduce a so far unknown degree of complexity and uncertainty for companies world-wide.
   - *Environmental risk*: The eruption of volcano Eyjafjallajøkull in Iceland in April 2010 led to a temporary disruption of international and continental flight transit, leading to huge financial losses for airline companies. The disastrous oil catastrophe caused by BP oil rig Deepwater Horizon in the Gulf of Mexico killed 11 crew members and caused billions of dollars in costs incurred by efforts to stop the oil spill and by reparation demands.
   - *Political risks and terrorism*: The ongoing pressure on corporations to increase revenues and the saturation of markets in developed countries have shifted the focus of growth activities to emerging and developing markets in Asia, South America and Africa. Many of the countries bear higher risk due to their unstable political system. Moreover global terrorism has repeatedly caused business disruptions, especially in the travel and tourism industries.

   These are just some of the many material risks companies face.

iii. **Countless regulations:** Corporate fraud scandals, environmentalism and other factors have triggered the introduction of lots of new high-impact regulations (Lo, 2009; Vinten, 2002). Examples include:

   - *The Sarbanes-Oxley-Act of 2002*: After the Enron disaster the United States issued the Sarbanes-Oxley Act, commonly known as "SOx", in order "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws" (U.S. Congress, 2002). While SOx also defined corporate responsibility for financial reports (section 302), making the CEO and CFO accountable for the correctness of the information provided under the threat of severe punishments, it is especially section 404 that had a giant impact on businesses. Section 404 requires management of all companies listed at U.S. stock markets to assess their internal controls for financial reporting (Kersten & Klett, 2008). The wide-reaching implications of this demand are manifested in the Public Company Accounting Oversight Board (PCAOB) Standard No. 5 (2007). Even though costs to assure SOx compliance have been decreasing from year to year, listed companies still had to invest an average of over US-$ 2 million in 2008 (United States Securities and Exchange Commission, 2009).

- *SOx-like initiatives in other countries*: In the wake of SOx introduction, many other countries issued similar legislations. The European Union published its version colloquially called “EURO-SOx” in 2006, the 8th Council Directive / Directive on statutory audit (2006/43/EC, a revised version of 84/253/EWG from 1984). Transposition into national law at present has meanwhile been finished in almost all member countries. Austria issued the “Unternehmensrechtsänderungsgesetz (URÄG)” in 2009; Germany introduced the “Bilanzrechtsmodernisierungsgesetz (BilMoG)” a year after that. Even though the European version of SOx is not as strict and costly to implement, it has raised awareness for the need of governance and internal control systems (Detecon, 2010). In Asia, a Japanese standard (“J-SOx”) was finalised in 2007 and the Chinese counterpart (“C-SOx”) was enacted in 2009.
- *Basel II and Basel III*: Basel II was introduced to set more risk-oriented capital requirements for banks and financial institutions (Basel Committee on Banking Supervision, 2004). As the regulation proved insufficient in the global financial crisis of 2007, a series of amendments generally referred to as “Basel III” have been made or are currently still discussed.
- *Accounting principles*: Countless national and international standards set requirements for accounting: International Financial Reporting Standards (IFRS), United States Generally Accepted Accounting Principles (US-GAAP), rules of the German Handelsgesetzbuch (HGB) including the “Gesetz zur Kontrolle und Transparenz im Unternehmensbereich” (KonTraG) and BilMoG, the Austrian “Unternehmensgesetzbuch” (UGB) and many more laws and regulations have to be respected by internationally active corporations in accounting and for preparation of financial statements.
- *Privacy regulations*: As information technology spreads into more and more areas of people’s life, data privacy has witnessed increased attention. The European “EU Data Protection Directive” (Directive 95/46/EC), the

German “Bundesdatenschutzgesetz” (BDSG), the Austrian “Bundesgesetz über den Schutz personenbezogener Daten” (DSG 2000), and the American Health Insurance Portability and Accountability (HIPAA) act for healthcare companies are some of the most important regulations for data privacy that companies have to adhere to.

- *Standards for information technology*: IT departments are subject of countless laws, standards and best practices. Apart from privacy regulations there are standards and best practices for IT governance (e.g. ISO 38500:2008, COBIT, ITIL), IT and data security (the ISO 27000 series), business continuity management (e.g. BS25999), quality management (ISO 9001), and many more national and international guidelines.
- *Other regulations*: The picture is completed by embargo and trade control regulations, such as the EU regulations on dual-use items and for combating terrorism, and the Chemical Weapons Convention (CWC), by climate protection and emissions laws, employee safety laws, countless industry-specific regulations (e.g. of the U.S. Food and Drug Administration, or “Mindestanforderungen an das Risikomanagement” (MaRisk) for the financial sector) and many other laws, regulations and standards, the listing of which would fill a book on its own.

Number, complexity and importance of GRC requirements steadily increase, resulting in companies undertaking various efforts to better face risks and to ensure the adherence to laws, regulatory standards and voluntarily imposed obligations (Menzies 2006). At present the multiple compliance and risk endeavours result in silos operating isolated from each other (Fisher, 2007; Volonino, Gessner, & Kermis, 2004) and they lead to a duplication of efforts, redundant solutions, higher cost and increased risk. Several experts argue that a holistic, integrated and strategic approach to GRC can add value and create competitive advantage (Chatterjee & Milam, 2008; PricewaterhouseCoopers, 2004). Consequently enterprises strive to improve the way they structure their GRC programs, trying to consolidate and integrate their separate governance, risk, and compliance activities (OCEG 2007; Caldwell 2008). These efforts are still ongoing, as most companies acknowledge that their GRC activities are not yet fully integrated (OCEG 2007).

In the early days of GRC, PricewaterhouseCoopers (2005) noted: “In itself GRC is not new. As individual issues, governance, risk management and compliance have always been fundamental concerns of business and its leaders. What is new is an emerging perception of GRC as an integrated set of concepts that, when applied holistically within an organisation, can add significant value and provide competitive advantage.” This emerging perception – contrary to the acronym itself – is not well-established. In business as well as in research the awareness of the concept of integrated GRC is rather low. People are struggling to describe the idea behind the term. “Definitions of GRC are as varied as they are fluid” (Leibs, 2007) to a degree that it was even recommended to avoid definitional debates (Dittmar, 2007).

This is partly owed to the lack of scientific research on the integrated approach to GRC; instead software vendors and consultants publish definitions and articles that suit their products and services. We could throw GRC into the corner of buzzing acronyms if market reports and surveys were not attributing a growing importance of GRC in the future (Kahn Consulting, 2008) – and an already strong impact today. In 2008 about 40 billion US-dollars were spent on services, technology and content related to GRC (Rasmussen, 2008). For integrated GRC suites, competitive pressures and the market’s upside potential have triggered market consolidation (Othersen & McClean, 2009; Caldwell, Proctor, & Nicolett, 2010). The German language XING.com group for GRC holds over 1,300 members. The business network LinkedIn lists close to 4,000 GRC professionals. Do they really work in a blurred, intangible domain?

Scientific research finally has to catch up with the GRC developments in the marketplace. This research project is carried out in order to shed light on GRC in general and GRC for information technology in specific. A first scientific examination shall pave the way for future GRC research.

1.2 Relevance for business informatics

We have already seen that GRC is an increasingly important topic in the business world. Moreover it is a hot topic in information technology. In order to cope with the increasing complexity, many companies turn to software to help automate their GRC efforts (Approva, 2007). Specialised solutions can help achieve considerable improvements of GRC operations (Fisher, 2007; Rasmussen, Hand in Hand, 2007). However GRC affects business informatics not only through software; there are GRC aspects in the management of IT as well.

Consequently for information systems research the field of integrated governance, risk, and compliance is interesting from two main perspectives (Teubner & Feller, 2008) as depicted in Figure 1. Firstly as an instrument; how can information systems – especially software applications – support integrated GRC in an organisation’s (business) operations – what is “**IT for GRC**”? And secondly with IT as the subject matter – what is “GRC for IT” or “**IT GRC**” (IT Policy Compliance Group, 2008), i.e. how can integrated GRC be applied to an organisation’s information technology landscape?

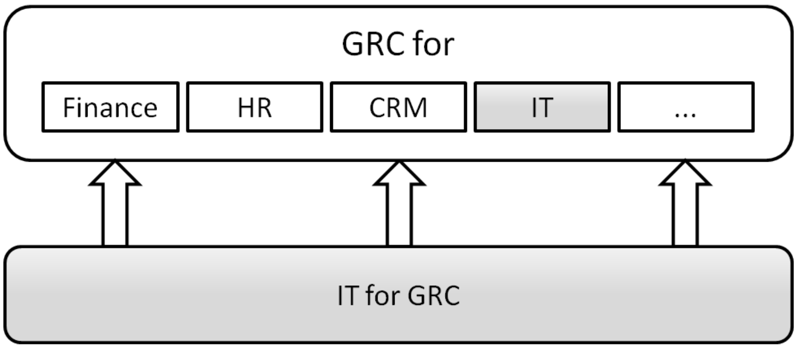


Figure 1: “IT GRC” and “IT for GRC”

The importance of IT in supporting GRC processes is steadily increasing (Jackson, 2007). The relevance of IT for GRC in practice is obvious, due to its market size and the number of software vendors, service providers and customers. Research has yet to analyse integrated GRC software.

As subset of corporate GRC, IT GRC (GRC for IT) is also a topic of high relevance. The three separate disciplines of IT governance (ITG), IT risk management (ITRM) and IT compliance (ITC) are already established topics in research (see chapter Chapter 2). Hence approaches to manage the three disciplines in an integrated manner should be examined by information systems research as well.

Chapter 2. Governance, risk management, and compliance as separate disciplines

Before delving into the peculiarities of GRC the three disciplines that gave the acronym its name should be defined. Moreover the IT counterparts – IT governance (ITG), IT risk management (ITRM), and IT compliance (ITC) – should be introduced. The following section is not meant to fully explain these disciplines, but to establish a basic understanding helpful in following the subsequent research.

2.1 Governance

The English term "governance" can be traced back to the late 14th century, when it was derived from the French word "gouvernance" that was used to describe the body of political leadership. The French term in turn has its roots in the Latin "gubernare" (to direct, rule, guide) and the ancient Greek "kybernan" (to steer) (Harper, 2010). Today governance describes the act or process of governing, i.e. effecting authoritative direction or control (Merriam-Webster, 2010). In business we often encounter the term "corporate governance" for the governance of a corporation. In information technology "IT governance" is a well-established discipline.

2.1.1 Corporate governance

Thus far no single theory adequately explains governance in full (McGinnis, Pumphrey, Trimmer, & Wiggins, 2004). Generally two basic approaches to corporate governance are distinguished (Lattemann, 2010). Firstly, there is the shareholder approach typically found in the Anglo-American world of business, where control is exercised through the capital market by means of the management board ("board model"). Secondly, as often practiced in continental Europe, there is the stakeholder approach, taking into account more stakeholders such as employees by means of supervisory boards and work councils ("separation model"). Hilb (2009) suggests a third model integrating the first two approaches, trying to deliver a comprehensive explanation. The shareholder and the stakeholder approach have recently started to converge, for example through implementation of audit committees for companies in the United States and Great Britain due to the Sarbanes-Oxley Act and the Cadbury Report (The Committee on the Financial Aspects of Corporate Governance, 1992).

The two approaches strongly focus on the various groups that have an interest in an organisation's actions. The best-known definition of corporate governance – and one that is accepted in many countries around the globe – includes a process-oriented dimension in addition. According to the Organisation for Economic Co-Operation and Development (OECD), corporate governance can be understood as "involving a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined" (Organisation for Economic Co-Operation and Development, 2004). Thus corporate governance is composed of structural and process-related elements. As objectives and performance depend on external factors as well, corporate governance deals with internal and external aspects of an organisation (Mallin, 2007). Being aware of this the OECD definition suffices as idea of corporate governance for this research.

2.1.2 IT governance

IT governance is emerging as an important area of enquiry both in research and practice. Academic papers started to use the term in the title of papers only in the late 1990s (Webb, Pollard, & Ridley, 2006). Even though research is broad, focusing both on ITG forms and ITG contingency (Brown & Grant, 2005), professional institutions like ISACA and the Office of Government Commerce (OGC) have an edge on research as far as the acceptance of their ITG perspectives in practice is concerned. IT governance is generally described as a subset and integral component of corporate governance focusing on governance of information technology (OGC, 2007; ISACA, 2009b).

In its nature IT governance parallels corporate governance because it refers to the structural and process-related patterns of authority over IT resources (McGinnis, Pumphrey, Trimmer, & Wiggins, 2004). Previous studies have focused primarily on structural mechanisms of IT governance while neglecting its process mechanisms (Ribbers, Peterson, & Parker, 2002). Lewis and Millar (2009) identified two schools of thought of IT governance; one focuses on decision making and accountability, while the other is primarily concerned with controls and risk management. These schools are two sides of the same coin. We will thus ignore their differing focus.

More important is the distinction between governance and management of IT, especially since some well-known best practice frameworks for IT governance mix up the two disciplines. The Office of Government Commerce (OGC), publisher of the IT Infrastructure Library (ITIL) remarks: “Management and governance are different disciplines. Management deals with making decisions and executing processes. Governance only deals with making sound decisions. It is the framework of decision rights that encourages desired behaviours in the sourcing and the sourced organisation” (OGC, 2007). This framework should ensure “that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.” (OGC, 2007). The “Center for Information Systems Research” (CISR) of the MIT Sloan School of Management also puts the emphasis of ITG on its role as a framework for decision rights and accountability, differentiating five decision domains: IT principles, IT architecture, IT infrastructure strategies, business application needs, and IT investment (Weill & Ross, 2004).

The IT Governance Institute and the Information Systems Audit and Control Association (ISACA) define ITG in their widely implemented framework COBIT as “the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives” (IT Governance Institute, 2007; ISACA, 2009b). According to ISACA IT governance primarily focuses on strategic alignment, value delivery, risk management, resource management and performance management (ISACA, 2009b). Webb et al. (2006) examined twelve definitions of ITG, concluding that the broad reach of ITG is not adequately captured in most definitions. They suggest their own definition, which reads very similar to ISACA’s: „IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management.“ (Webb, Pollard, & Ridley, 2006).

Just like OGC other bodies publish ITG definitions because they try to establish standards or they want to support their frameworks with a concise definition. The standard ISO/IEC 38500:2008, for instance, describes the corporate governance of IT as

> “the system by which the current and future use of IT is directed and controlled. [It] involves evaluating and directing the plans for the use of IT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organisation.” (ISO/IEC 38500:2008, 2008)

The ISO/IEC standard recommends three process steps – evaluate, direct, and monitor – to be applied across six principles: responsibility, strategy, acquisition, performance, conformance, and human behaviour. The framework putting corporate governance in context with business processes is drawn out in Figure 2.

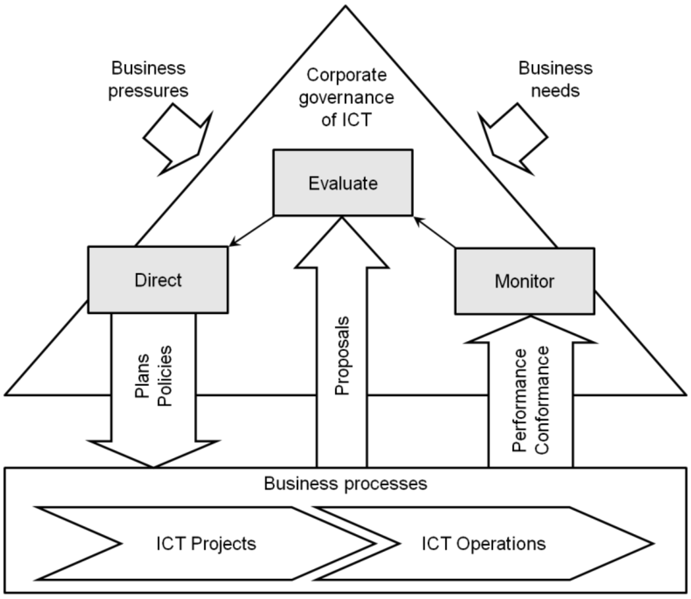


Figure 2: ISO/IEC 38500:2008 model for IT governance

Ohki et al. (2009) recommended adding “reporting to stakeholders” as a fourth process. This definition – the ISO/IEC standard extended by reporting – is the understanding of IT governance shared by the author and applied in this research.

2.2 Risk management

The origin of the term “risk” is uncertain. Some sources attribute it to the non-documented colloquial Latin word “riscare” (to run into danger) (Harper, 2010), while others claim it could be traced to ancient Greek or Arabic words. The meaning of “risk” has recently witnessed a revolution. Since its first appearance around 300 years ago it has always described the possible negative impact of an event. Over the last two decades a new perception of risk as negative or positive deviation of an expected outcome has emerged (DeLoach, 2000). Both risk definitions now co-exist, as there are still risks that can only have a negative impact, such as the risk of default (Prokein, 2008). The term “risk management” only came into existence in the 1960s, even though risk management practices have been used for more than 2,000 years (Bernstein, 1996).

2.2.1 Enterprise risk management

Enterprise risk management (ERM; sometimes also called “corporate risk management”) does not simply stand for the management of risks in enterprises; instead the term constitutes the insight that the various risks of an enterprise are interrelated, and that they have to be managed in an organisation-wide, holistic manner. Due to the benefits of the enterprise-wide approach, companies show a strong interest in accelerating the evolution of ERM as a core business process (Francis & Richards, 2007).

A widely accepted definition of enterprise risk management was published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO). Thus ERM 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives” (COSO, 2004).

Figure 3 highlights the encompassing nature of ERM depicting relevant processes, objectives categories and hierarchy levels.

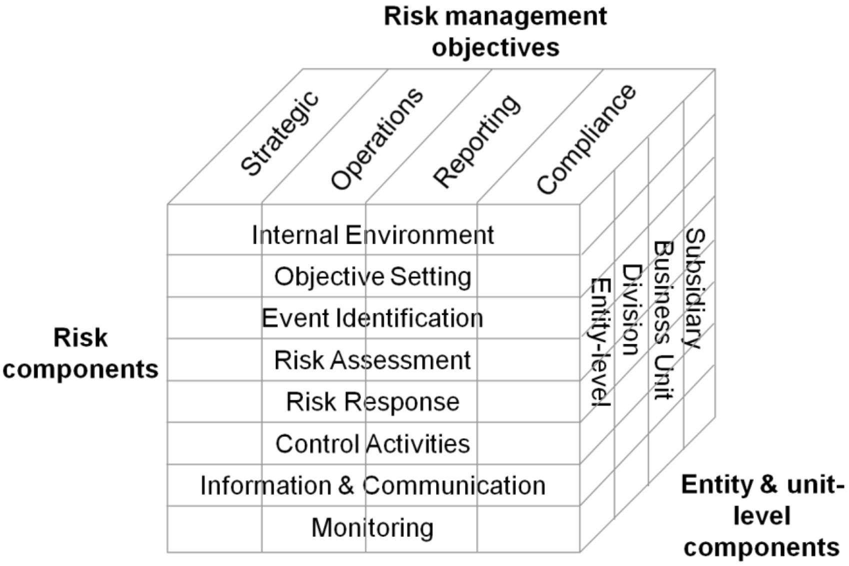


Figure 3: The COSO ERM framework (COSO, 2004)

There is a general agreement on the described goals of ERM in comparison to traditional, siloed risk management: ERM shall enable the holistic identification and control of all risks of an enterprise, the consideration of interdependencies and the integration of risk management into corporate strategy (Albrecht, 1998; Denk & Exner-Merkelt, 2005; Burnaby & Hass, 2009). The COSO definition is therefore adopted in this research. The COSO ERM framework is used in chapters 8 and 9.

2.2.2 IT risk management

IT risk management is the part of enterprise risk management that focuses on information technology risk. IT risk can be understood as “the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise” (ISACA, 2009a).

Historically, ITRM has evolved from IT security management. Hence the most prominent standard for ITRM is still ISO/IEC 27005:2008 (2008) of the ISO/IEC 27000 series that focuses on information security risk management. But IT risk clearly exceeds IT security. Due to the support of business processes through IT, IT risk is inherent in basically every business process. Often IT risk is classified as a subtype of operational risk (Prokein, 2008). ISACA however takes a broader view, arguing that “IT risk is business risk” because IT-related risk influences all other risk categories, such as operational risk, strategic risk, compliance risk, environmental risk and market risk (ISACA, 2009a). There are various classifications of IT risks, for example the distinction of IT risks in infrastructure development and support, operations and maintenance of business process, office level support, software development and outsourcing management (Nadhirah & Khairuddin, 2008). In the end the classification is arbitrary as long as all IT risks are covered.

The typical phases of the ITRM process are similar to those of ERM. In literature they range from four to eight steps, depending on the degree of detail applied (Teuteberg, 2010). ISACA (2009a) differentiates many different processes within the three categories risk governance, risk evaluation, and risk response. Chapter 8 treats this model detail.

2.3 Compliance

The term compliance – the noun to the verb “to comply” – has been in use since the 1600s (Harper, 2010). In business practice in German-speaking countries, the term “compliance” started its conquest only about twenty years ago (Vetter, 2008). A universally accepted definition does not exist; in business science and practice the meaning of “compliance” has only started to take shape after the introduction of the Sarbanes-Oxley Act (Menzies, 2006).

Compliance has two principal meanings. It either describes the act or process of complying, or the state of conformity in fulfilling requirements (Merriam-Webster, 2010). Rath & Sponholz (2009) call the first meaning the “action-oriented” dimension and the second meaning the “normative-legal” dimension of compliance. They further identify a third, “proof-oriented” dimension that describes processes carried out to provide a proof of compliance (such as an audit). Whenever compliance is used in this research all three dimensions are referred to. The requirements companies adhere to can be laws and regulations, which is the narrow definition of compliance, but also contractual obligations and internal policies, according to the broad definition of compliance (Moeller, 2007).

As with corporate/IT governance and enterprise/IT risk management, the discipline of corporate compliance refers to all types of compliance in an enterprise, with IT compliance being a part of corporate compliance. ITC – the compliance of IT – should not be confused with IT solutions that enable compliance – compliance through IT – for instance through automation of compliance processes (Sackmann, 2008).

2.3.1 Corporate compliance

According to the German codex for corporate governance, the board has to assure that regulations and internal policies are adhered to by all entities of the enterprise, which is defined as “compliance” (Regierungskommission DCGK, 2010). Menzies (2006) defines corporate compliance as an organisation-wide, integrative approach to efficiently and effectively fulfil stakeholder requirements.

Hauschka (2007) gives a comprehensive overview of corporate compliance from a legal perspective. The standard measure taken to assure compliance is the establishment of an internal control system (Menzies, 2004) as required by several standards, such as §82 AktG and §11 GmbHG in Austria, KontraG in Germany (Deutscher Bundestag, 1998) and SOx in the United States of America (U.S. Congress, 2002). Such an internal control system is designed to provide reasonable assurance regarding the achievement of objectives like effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations (COSO, 1992). The main components of such a system are the control environment (describing the tone at the top and control consciousness of employees, among other things), risk assessment, control activities, information and communication of control measures and issues, and monitoring of controls and the control process (COSO, 1992). The effectiveness of the internal control systems is examined through frequent internal and external audits.

2.3.2 IT compliance

There is no generally accepted definition of IT compliance in research. ITC can be viewed narrowly as the adherence to laws, or more broadly as the adherence to any kind of mandatory or voluntary requirements for information technology (Klotz & Dorn, 2008). ITC comprises compliance of all IT operations of an organisation, even if they are outsourced (Mossanen, 2010). Especially in its broad meaning ITC does not only have a preventive role; it further helps optimise processes and it can even add value to create competitive advantage of and through IT (Böhm, Goeken, & Johannsen, 2009; Böhm, 2008).

Most of the regulations mentioned in chapter 4 are either specifically directed towards IT, such as data privacy legislation, or they affect business processes supported by IT, thus also bearing relevance for IT departments. For instance the 8th EU Directive, even though it aims at the business process of financial reporting, requires the implementation of an internal control system, integration of financial reporting software, secure data and document transmission, centralised data storage and the use of an IT governance framework (Liegl, 2009). The risk and binding character of rules increases from internal rules over external frameworks (standards and best practices) and contractual obligations to legal obligations that are mandatory and thus generally carry a high risk of non-compliance (Klotz & Dorn, 2008).

From a process perspective ITC, same as corporate compliance, consists of four main process steps Figure 4.

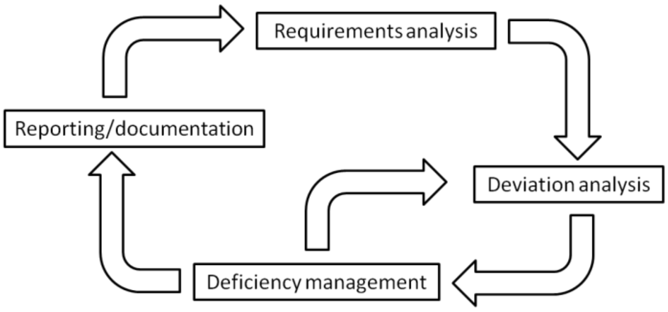


Figure 4: The IT compliance process (Rath & Sponholz, 2009)

At the start an organisation-specific analysis of requirements – be it from laws, regulations, contracts, and external or internal standards – is carried out. Second is the analysis of possible deviations of the adherence to these requirements, often done by internal or external auditors. Where deviations are discovered and the organisation decides that the requirement should be complied with, deficiency management improves the status quo. Deviation analysis and deficiency management are carried out in a loop, as new implementations have to be checked for their effectiveness. Relevant actions and results of the first three steps are documented and reported to stakeholders. The ITC process model will be used later in this research in chapter 9.

2.4 Summary

Obviously the topics IT governance, IT risk management, and IT compliance as well as their corporate counterparts have been treated in various ways in research and in practice. The definitions selected for application in the research at hand are not exclusively valid, but they support broad concepts of the disciplines and thus reduce the risk of framing the field of research too narrowly.

Chapter 3. Research goals and methodology

Having established a basic understanding of governance, risk management, and compliance when separately defined, we can now turn to the actual research carried out on GRC integration. In this chapter the research goals, the used methodologies and the rigour applied are explained.

3.1 Research goals

This research project pursues two principal goals.

> *Primary goal of this research is the development of a comprehensive high-level process model for integrated governance, risk, and compliance in information technology management.*
>
> *The secondary goal, indispensable to reach the primary goal, is to enable future GRC research through creation of a scientific basis and through provision of insights on the status quo of GRC in business.*

3.2 Research methodology

In order to reach these goals the research project is subdivided into six research chapters (chapters 4 to 9 in this document) – each one defined to assure control over the progress of the work. Due to the lack of scientific research the groundwork activities to create an understanding of GRC and of the GRC status quo in the industry make up the majority of the project. The results from these studies directly and indirectly influenced the primary goal, the creation of the process model. Table 1 gives an overview of the defined research chapters, their description and the methodology applied.

Table 1: Research chapters

Chapter	Description	Methodology
4	GRC definition and frame of reference for research	Literature review; survey for validation of definition
5	GRC software as seen by software vendors and market research	Explorative study combining a survey and document analysis
6	Status quo of GRC and GRC software use in the industry	Quantitative survey among large enterprises
7	Status quo of IT GRC management in the industry	Case studies in selected large enterprises
8	Analysis of the relation of enterprise risk management and IT risk management	Theoretical study through comparison of best practice frameworks
9	Process model for integrated IT GRC management	Descriptive combination of best practice frameworks

At the start of the research project a literature review is carried out in order to derive a scientific working definition of GRC. Based on the GRC definition a frame of reference for research of GRC is constructed (chapter 4).

In order to understand the status quo of GRC in the industry, three studies (chapters 5 to 7) are conducted. Firstly, state-of-the-art GRC software is examined through a survey among GRC software vendors and a comparison with market research frameworks. Secondly, a survey among GRC personnel in large enterprises identifies the status quo of GRC and of GRC software use. Thirdly, a case study of IT GRC processes in selected companies identifies the status quo of IT GRC and potentials for integration.

Due to the observed core role of risk management within GRC and to enable integration of general GRC and IT GRC, ERM is compared to ITRM. The comparison shows in how far process models of the two disciplines are congruent (chapter 8).

The results of all five previous chapters are then used in the construction of a reference process model for IT GRC management (chapter 9).

Figure 5 depicts the basic research structure. Chapter 4 sets the frame for all subsequent research chapters. The results of chapters 5 to 8 are incorporated in chapter 9.

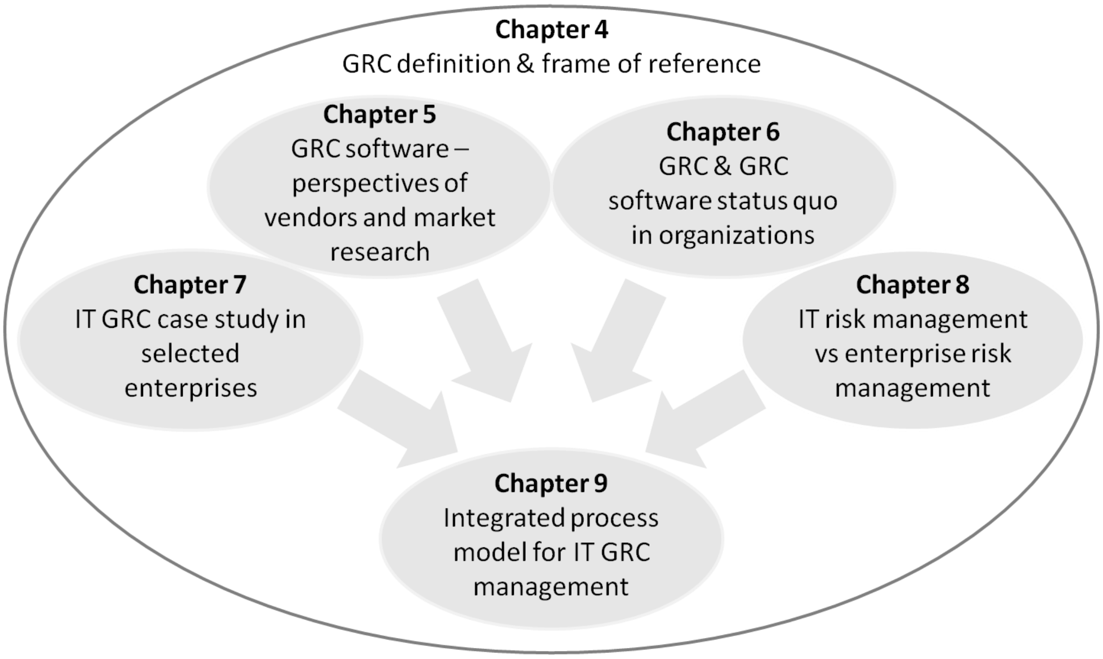

Chapter 4
GRC definition & frame of reference
Chapter 5
GRC software – perspectives of vendors and market research
Chapter 6
GRC & GRC software status quo in organizations
Chapter 7
IT GRC case study in selected enterprises
Chapter 8
IT risk management vs enterprise risk management
Chapter 9
Integrated process model for IT GRC management

Figure 5: Research methodology in chapter 4

For each chapter a specific methodology is used that best helps reach the goals of the respective chapter. The methodologies applied range from literature reviews, validation surveys, quantitative surveys and detailed qualitative case studies to inductive, conceptual framework developments. Details of the employed methodologies are presented in the respective chapters.

3.3 Scientific rigour

Information systems research can and should be both relevant and rigorous (Applegate, 1999). The rigour of the applied methodology has to be proven (Hevner, March, Park, & Ram, 2004). By the time this document was finished, all six research chapters were already published at peer-reviewed conferences. The acceptance of the results can be interpreted as a confirmation of the strict rigour applied. An overview of the conferences is given in Table 2.

Table 2: Conferences of published chapters

Chapter	Conference
4	11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz. Springer.
5	44th Hawaii International Conference on System Sciences, HICSS 2011. IEEE.
6	21st Australasian Conference on Information Systems, ACIS 2010, Brisbane. AIS.
7	2011 International Workshop on IT GRC, ITGRC 2011, Washington D.C., IEEE.
8	Informatik 2010, Leipzig. GI.
9	Ninth International Baltic Conference, Baltic DB&IS 2010, Riga. IOS Press.

Thorough selection of survey participants, careful data collection, transparent data analysis, and the construction of new theories and models based on prior insights are just some of the features of this work that should ensure scientific rigour.

Chapter 4. Literature review, GRC definition and frame of reference

Standing at the start of the research project we have to realise that there is hardly any scientific research on GRC as an integrated approach to build on. Thus we have to start from the scratch, reviewing existing literature – the rare scientific and the predominant non-scientific publications – in order to develop a frame of reference that supports GRC research in general and the creation of reference models (such as the process model in chapter 9) for integrated GRC in specific, according to the process model for an empirically grounded reference model construction (Ahlemann & Gastl, 2007). The frame construction goes hand in hand with the development of a single-phrase definition of GRC. Both items may be used as a starting point by researchers when approaching the topic in a structured, scientific manner. The following section will help to shed light on what we talk about when we talk about GRC. After all we do not forever want to treat GRC “like a large black box: a mysterious container full of improved processes and software for automation” (Broady & Roland, 2008).

4.1 Research methodology

The methodology applied in this chapter consists of four stages, as depicted in Figure 6.

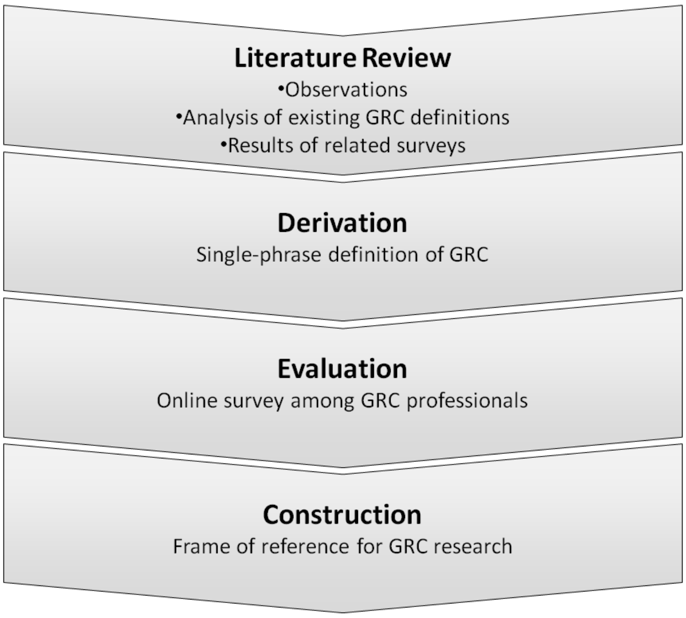
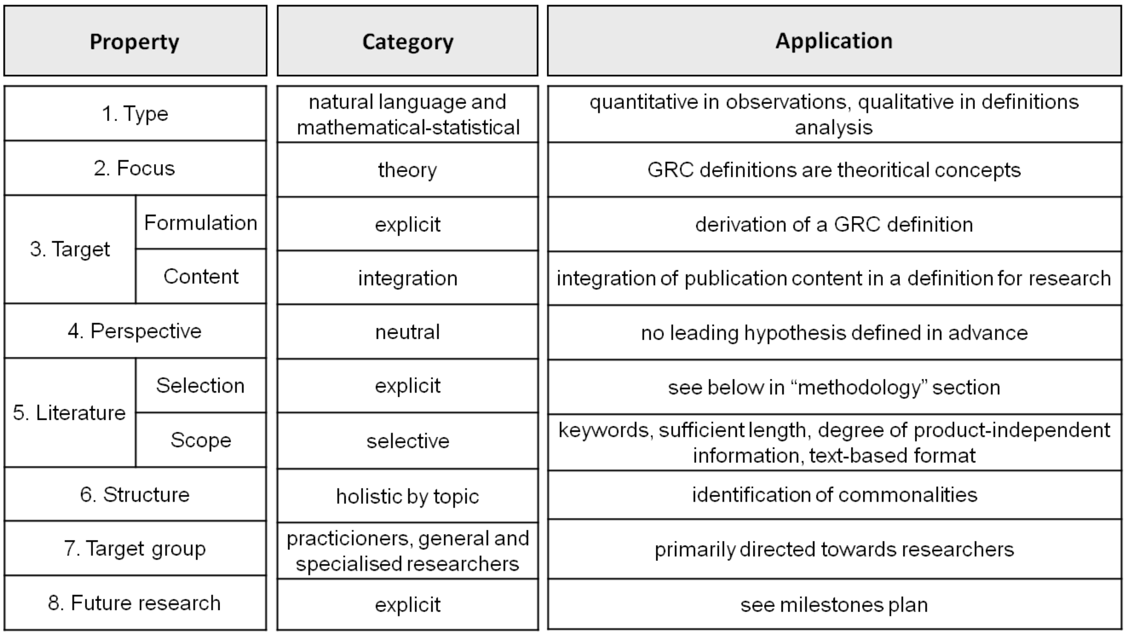

Literature Review
•Observations
•Analysis of existing GRC definitions
•Results of related surveys
Derivation
Single-phrase definition of GRC
Evaluation
Online survey among GRC professionals
Construction
Frame of reference for GRC research

Figure 6: Research methodology in chapter 4

The first stage is a review of GRC publications following the classifications of Fettke (2006) for reviews in business informatics. Its properties are as follows:



Property		Category	Application
1. Type		natural language and mathematical-statistical	quantitative in observations, qualitative in definitions analysis
2. Focus		theory	GRC definitions are theoritical concepts
3. Target	Formulation	explicit	derivation of a GRC definition
	Content	integration	integration of publication content in a definition for research
4. Perspective		neutral	no leading hypothesis defined in advance
5. Literature	Selection	explicit	see below in “methodology” section
	Scope	selective	keywords, sufficient length, degree of product-independent information, text-based format
6. Structure		holistic by topic	identification of commonalities
7. Target group		practicioners, general and specialised researchers	primarily directed towards researchers
8. Future research		explicit	see milestones plan

Figure 7: Literature review properties (Fettke, 2006)

Immediately striking a reader of GRC-related publications is the massive number of topics mentioned. Numerous methodologies such as business rules management, business process management, or enterprise content management are as present as processes such as auditing, planning and control. Seen as separate topics, corporate governance, risk management and compliance alone are vast areas impossible to grasp in a single literature review. Since we want to identify the meaning of GRC as a whole and not that of its fragments alone, we restrict the review to publications that explicitly mention all three topics as in “governance, risk (management) and compliance” or “GRC”.

Publications were found using the search engines of WISO, EBSCO, ACM, IEEE Xplore, SpringerLink, Emerald, Google, the Vienna University of Technology’s and Ludwigshafen University of Applied Sciences’ libraries, and through manual browsing on relevant websites (see Appendix A – List of manually processed websites). From the findings only those results were chosen that fulfil the three criteria of sufficient length, sufficient degree of product-independent information and text-based format. Eventually 107 sources published between 2004 and 2009 made it to the final list (Appendix B – List of 107 publications from literature review). They were analysed using mathematical-statistical and natural-language methods. The exact methodology applied is case-specific for each observation. It is therefore presented later in this document together with the respective observations.

In a second stage the observations, the analysis of existing definitions and the results of two related surveys are used in the derivation of a single-phrase working definition of integrated GRC.

In a third stage an anonymous online survey is conducted to evaluate and improve the working definition. We posted the survey in GRC expert groups of the business networks XING and LinkedIn. Eventually 131 GRC professionals took part. They responded to four questions:

i. a rating of the definition on a scale from 10 (best) to 1 (worst) with the option to refuse a ranking if they felt that a single-phrase definition of GRC generally would not make sense;
ii. an optional free text comment to provide feedback;
iii. the type of organisation the respondent is working for; and
iv. the respondent’s GRC focus.

The participants constitute a cross-section of GRC professionals (see Figure 8). 42% work in GRC consulting, 18% for GRC software vendors, 16% focus on GRC in their own organisation, 11% are auditors and 5% each work for research institutions or as freelancers. 3% work for other types of organisations.

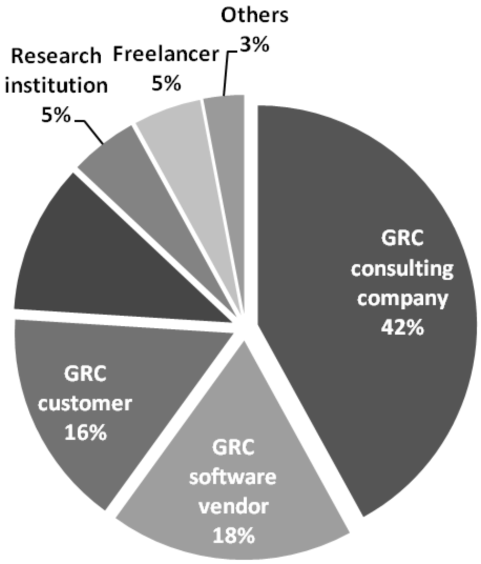


Figure 8: GRC definition validation survey participants, by employer

Participants' primary interests in GRC are GRC processes without technology focus (29%) followed by GRC technology (26%), compliance (19%), risk management (18%), and corporate governance (4%). The remaining 5% do not primarily focus on any of these topics.

The fourth stage of the research project is the construction of a frame of reference for research of integrated GRC based on the short-definition. Following the process model for empirically grounded reference model construction (Ahlemann & Gastl, 2007), the frame is a condensed high-level abstraction of future reference models created to support navigation within the problem domain of GRC. As proposed by Schlagheck (2000) the frame of reference is developed early on in the research helping to scope GRC modelling and other research projects, to identify single model elements and to guarantee completeness.

4.2 Literature review results

The results of the literature review – key observations, the analysis of definitions and prior surveys – are described in the following.

4.2.1 Literature review – key observations

O1: There is basically no scientific research on GRC as an integrated concept.

While lots of research exists on the "G", the "R", and the "C" as separate topics, the potential integration moves under the radar of scientific research. Of the 107 sources identified a mere two deserve the label "research paper" (Mitchell, 2007b; Tapscott, 2006). Both publications only provide short definitions of governance, risk management and compliance separately. O1 demonstrates the lack of research participation in GRC.

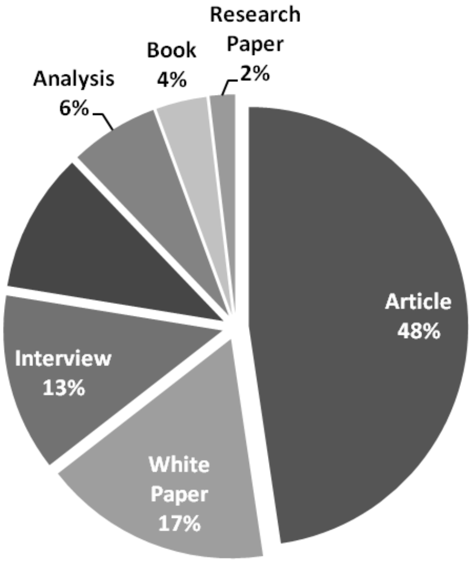


Figure 9: GRC publications by type

O2: Software vendors, analysts and consultancies are the main GRC publishers.

We categorised our sources by authorship, distinguishing software vendors, analysts, consultancies, scientific research personnel and independent experts. Co-authorship was applied in four cases. For interviews only the role of the interviewee was considered. The review shows that GRC software vendors are the most active group providing GRC publications (40), closely followed by analysts (34) and consultancies (31). Together these three parties participated in 94% of the selected GRC publications. GRC is obviously dominated and driven by the business community.

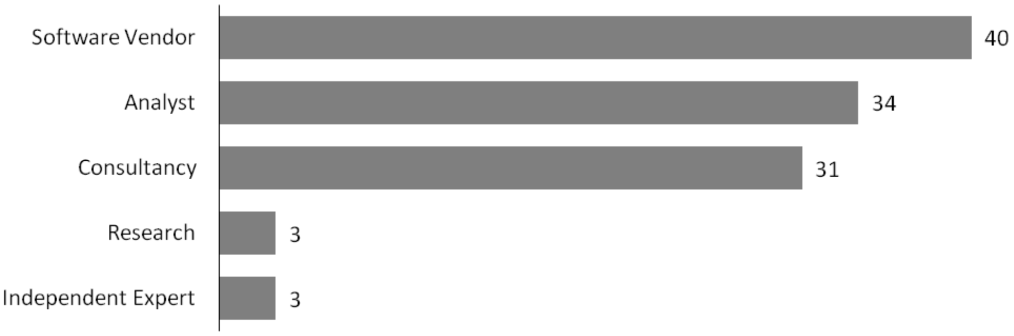


Figure 10: Authorship by number of publications

O3: Software technology is the prevailing primary topic.

When publications are dominated by software vendors followed by consultancies that help implementing technologies, it is not surprising that software technology is the prevailing topic in these works. 57 publications (53%) primarily treat technology. This finding underlines the importance of technology as an enabler of GRC.

O4: Regulatory compliance is the main driver of GRC, challenged by risk management.

We listed all reasons explicitly named as GRC drivers in publications. 43 out of 107 publications do not mention any GRC drivers. Of the remaining 64, 25 (39%) consider the increasing number of regulations to drive GRC. 18 (28%) name increased risk, 10 (16%) the potential for cost reductions, 8 (12.5%) mention the increased complexity of business due to market dynamics, globalisation and other factors. According to a study of AMR Research, risk management is about to surpass compliance as top GRC priority. “No longer just a U.S.-centric concern tied to compliance with 2002's Sarbanes-Oxley Act and other specific regulations, GRC has evolved into a set of practices to manage and mitigate the full array of risks organisations face” (Kelly, 2008). Comparing the drivers mentioned in 2007 and in 2008, we found that our review did not significantly support the AMR findings. References to risk as a driver hardly changed (23.5% in 2007; 24% in 2008), while the emphasis of regulations declined from 41% to 34%.

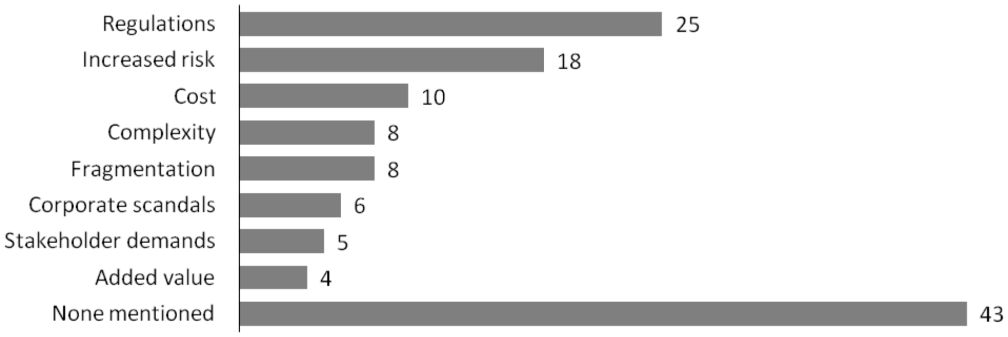


Figure 11: GRC drivers by number of publications

O5: ERM is an important methodology within GRC.

Inspired by the article “Is ERM GRC? Or Vice Versa?” (Banham, 2007) we wanted to find out how often enterprise risk management (ERM) or its synonyms were mentioned in GRC publications. References to ordinary risk management were not accounted for. 58 publications (54%) mentioned ERM. The enterprise-wide perspective of risk seems to go hand-in-hand with GRC.

O6: GRC is closely linked to Sarbanes-Oxley.

Undoubtedly the regulation causing the biggest impact on enterprises since the turn of the millennium, the Sarbanes-Oxley Act of 2002 (SOx) seems to go hand in hand with the idea of GRC. Arguably SOx is the main reason GRC came into existence, as exploding costs of compliance inspired clients, consultants and software vendors to think of remedies. Our research shows that SOx is mentioned in 74% of GRC publications. Considering that 47% of all publications were articles, many of them of moderate length, the result strongly supports the hypothesis that SOx and GRC are closely linked.

4.2.2 Literature review – GRC definitions

One in three of the analysed publications offer a GRC definition. Two thirds of these definitions explain what is understood by GRC as an integrated concept. The remaining third disregards that the total might be more than the sum of its parts and confines itself to defining the three terms of governance, risk management and compliance separately.

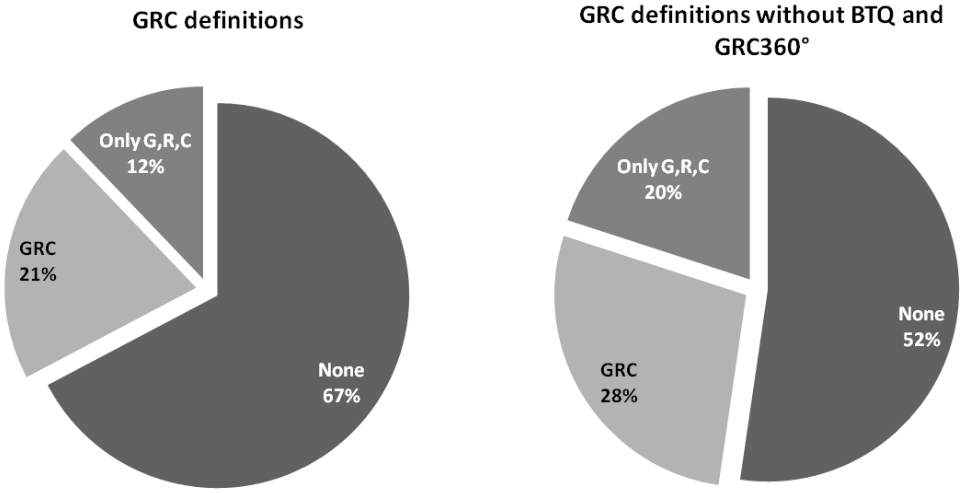


Figure 12: GRC definitions in publications

Omitting the two journals steadily publishing GRC articles directed towards readers familiar with the term – “Business Trends Quarterly” (BTQ) and “GRC360°” – the percentage of GRC definitions rises to almost fifty percent. References to definitions made before are basically nonexistent; sometimes several different definitions are provided by a single organisation.

A separate definition of the three terms of governance, risk management and compliance is made in 12% of the publications and in 20% when leaving away BTQ and GRC360°. The exact meaning of the topics themselves is a study of its own and cannot be discussed in this document. According to Mitchell (2007a) it might not even be purposeful: “To be clear, there are substantially more processes than governance, risk and compliance playing critical roles in GRC. But 13-letter acronyms rarely catch on.” Still some of the authors follow the “G,R,C approach” in their definitions (Hoffmann, 2007; Switzer, 2007; Curran, 2007). However the larger percentage of comprehensive GRC definitions in publications lets us conclude that the idea of an integrated concept is more widely supported. GRC is more than an umbrella term for governance, risk and compliance.

Looking at definitions of the integrated concept, some authors hold a technology-oriented view. Banham(2007) cites a consultant stating that in contrast to ERM “GRC is more a technology platform for illuminating governance and compliance risk. It’s useful to think about GRC in terms of an IT platform. [...] The technology helps you centralize and organize your policies, procedures, documentation requirements, risk assessment analyses and other content [for] dashboard reporting.”

On the contrary KPMG (2008) insists that “[GRC] is more than a software solution; it is a strategic discipline. GRC is a continuous process that is embedded into the culture of an organisation and governs how management identifies and protects against relevant risks, monitors and evaluates the effectiveness of internal controls, and responds and improves operations based on learned insights.” This view of GRC as an enterprise-wide management concept is supported by several authors (PricewaterhouseCoopers, 2005; Economist Intelligence Unit, 2008; Wechsler, 2008). Corporate Integrity (2007) goes as far as calling GRC a “philosophy of business” that “permeates the organisation: its oversight, its processes, its culture.” Mitchell (2007b) speaks of “principled performance”, which is picked up by Hovis (2007): “Integrated GRC is a cross-functional and extended enterprise capability that, when implemented, creates ‘principled performance.’ An integrated GRC effort is a transforming initiative, affecting how the enterprise will function both in its strategic orientation and in its operational focus.”

The Open Compliance & Ethics Group (OCEG, 2009) published an exhaustive definition that was reviewed by professionals from a variety of organisations: “GRC is a system of people, processes and technology that enables an organisation to understand and prioritize stakeholder expectations; set business objectives congruent with values and risks; achieve objectives while optimizing risk profile and protecting value; operate within legal, contractual, internal, social and ethical boundaries; provide relevant, reliable and timely information to appropriate stakeholders; and enable the measurement of the performance and effectiveness of the system.”

Switzer (2007) emphasises integration: “We like to use the three letter term ‘G-r-C’ as a symbol for the need to integrate these efforts with each other and within business operations.” Process-oriented perspectives emphasising improvements through integrated GRC are taken by Vemuri (Vemuri, 2008) and Frigo & Anderson (2009), who describe GRC as a set of “initiatives [...] which look across [...] risk and control functions holistically and seek to enhance their efficiency and effectiveness.”

From these definitions we concluded that

i. GRC is an integrated, holistic management concept for the topics involved
ii. technology is a key – but GRC is more than just technology, and
iii. integrated GRC is supposed to improve the performance of processes.

4.2.3 Literature review – previous surveys on the understanding of GRC

The opinion of GRC professionals has previously been identified by two surveys. The first survey of over 400 organisations led to the following result: "The vast majority of respondents (75%) view GRC as 'a coordinated program involving people, processes and technology.' More than half (54%) viewed GRC as a valuable concept, representing the future of how GRC concepts will be addressed. Almost all respondents view GRC as a process rather than a product or a fad (only 3%) [...]." (Kahn Consulting, 2008). This shows a more deliberate idea of GRC than the results gathered by Approva (2007) one year earlier. In this survey, 87.1% of over 200 respondents consider GRC a "term used to describe a group of internal policies & processes designed to manage risk", while hardly anybody opted that GRC was "just another acronym" (3.3%), the "name of a software category" (2.4%) or the "name of a functional department in my company" (3.3%). Only 3.8% of respondents were unfamiliar with the term.

4.3 Derivation and evaluation of a GRC working definition

The multitude of GRC definitions makes it difficult to find a consensus; to a certain extent the definitions overlap, but some treat aspects that are disregarded in others. For our definition the 75% majority of the Kahn survey claiming that people, processes and technology are involved was taken as a starting point. Furthermore the concept of "integrated" GRC, after ruling out the fragmented approach above, was followed. Incorporating the observations and the three conclusions drawn from the definitions analysis – the integrated, holistic management concept, technology being a key (but not the only one), and GRC being supposed to improve the performance of processes – we derived the following preliminary single-phrase definition:

> GRC is an integrated, holistic approach to corporate governance, risk and compliance ensuring that an organisation acts in accordance with its self-imposed rules, its risk appetite and external regulations through the alignment of strategy, processes, technology and people, thereby leveraging synergies and driving performance.

The survey conducted in order to validate and improve the definition brought about interesting results. Only three out of 131 respondents opted to answer "no rating – I think there should not be a one-sentence definition of GRC". The other 128 participants attributed the definition an average of 7.5 on a 10-point-scale. 78% rated it 7 or higher. Only 12% chose a rating of four or lower – the same percentage of respondents that supported the definition unconditionally, awarding a ten point rating.

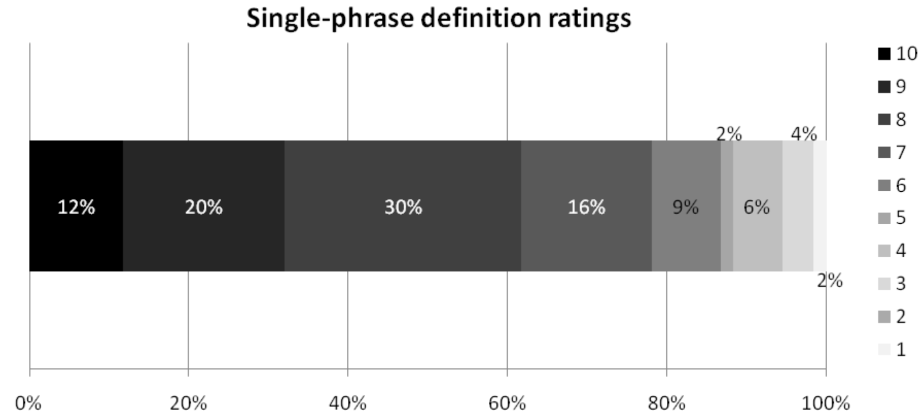


Figure 13: Distribution of ratings of the single-phrase GRC definition

We interpret the result as a strong backing of our definition. Still we looked at the 74 comments provided by participants in order to introduce minor improvements. 18 respondents criticised that the definition was overly long and complex. 13 and 8 respondents, respectively, did not like the wording "leveraging synergies" or "driving performance". We replaced the terms with "improving efficiency and effectiveness", which includes the use of synergies and improved performance but is more general. "Self-imposed rules" was criticised as being clumsy; we replaced it with "internal policies". Several respondents asked for ethics to be included as companies such as Enron and Worldcom were fully compliant but still went bankrupt due to unethical actions. "Corporate" was replaced with "organisation-wide" as the former could imply a restriction of GRC to the C-level of a company. Lastly we moved "risk appetite" in front of "internal policies and external regulations" because participants felt the definition was too compliance-centric. The final definition is as follows:

> *GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation 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.*

4.4 Construction of a frame of reference for research of integrated GRC

The definition was incorporated into a high-level frame of reference highlighting the key elements that should be examined when researching the integrated GRC concept.

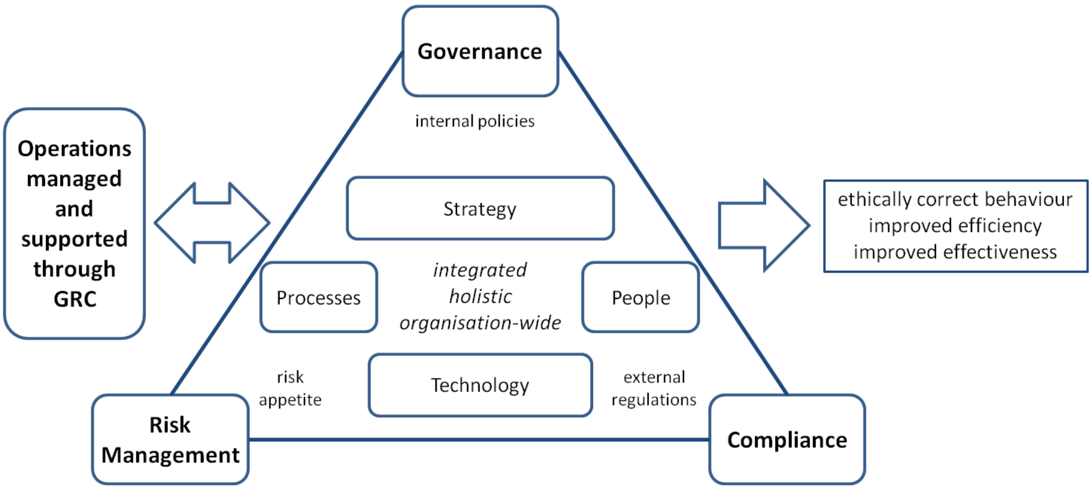


Figure 14: Frame of reference for research of integrated GRC

Governance, Risk Management and Compliance are the core subjects of GRC. Each of the subjects consists of the four basic components of GRC: strategy, processes, technology and people. The organisation's risk appetite, its internal policies and external regulations constitute the rules of GRC. The subjects, their components and rules are now to be merged in an integrated, holistic and organisation-wide (the three main characteristics of GRC) manner – aligned with the (business) operations that are managed and supported through GRC. In applying this approach, organisations long to achieve the objectives of GRC: ethically correct behaviour, and improved efficiency and effectiveness of any of the elements involved.

Of course the components strategy, processes, people and technology are not exclusive to GRC. All operations of an organisation are constituted by these components. For the procure-to-pay cycle, for example, there is a strategy that sets and controls targets; there are the process steps from procurement to payment, and procurement staff as well as transactional and information systems enabling the cycle. GRC supports the management and the execution of these operations; e.g. through governance specifications for the handling of goods, segregation of duties across the procure-to-pay processes, or technology to monitor risks in the supply chain.

As mentioned before for information systems research GRC processes that support the information technology operations of an organisation are of special interest (Teubner &

Feller, 2008). These GRC processes are commonly referred to as “IT GRC” (IT Policy Compliance Group, 2008).

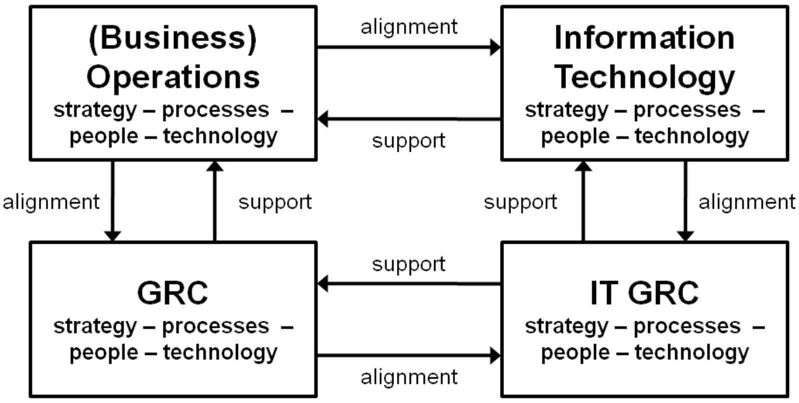

(Business) Operations
strategy – processes – people – technology
Information Technology
strategy – processes – people – technology
GRC
strategy – processes – people – technology
IT GRC
strategy – processes – people – technology
alignment
support
alignment
support
support
alignment
support
alignment

Figure 15: GRC and IT GRC in the business and IT context

IT GRC deals primarily with issues of information security, IT compliance, IT and data governance, IT risk management and IT revision (Rath & Sponholz, 2009). It is aligned with the overall GRC activities, the IT operations and indirectly with the organisation’s (business) operations.

A universal analysis of GRC would have to consider all the components of the two figures above. Analysis – the separation of a whole into its component parts – helps a researcher to focus on certain aspects. For example a research project could be restricted to examining IT GRC technology, such as IT security software and systems monitoring tools. A more comprehensive project might include the whole of IT GRC and its integration with the IT components. A researcher who does not want to dive into the depths of technology might focus on the integration of GRC processes with a specific business process. Sometimes it is difficult to draw a clear line between the four boxes in Figure 15; there are even intentional overlaps. For instance in most cases GRC technology is information technology. Depending on the perspective of the researcher, classifications can be made as it suits the research project best. For scoping it is just important that relevant components are not left away.

Once the components in scope have been chosen, the same can be done for the rules that are to be considered. The rules of GRC are basically defined by compliance requirements, the risk management process and the organisation’s governance codices. No matter if they are stated in regulations, internal policies or target agreements, in the end they are all normative or restrictive instructions that may potentially be represented and used in an integrated manner. The large number of rules might require a researcher to focus on certain rules and leave others away (e.g. include the COBIT framework but ignore ISO 27001). In any case it should be examined in how far the GRC characteristics (integrated, holistic, and organisation-wide) are present in the subject of research.

Eventually GRC research should investigate the impact of integrated GRC in their models or subjects of research; is there an improvement in the objectives of ethically correct behaviour, efficiency and effectiveness? Effects may arise in any of the GRC subjects, all operations, IT, GRC and IT-GRC subcomponents, and in the handling of the GRC rules.

A short example will help to understand how this frame of reference supports scoping and approaching a GRC research project. Assuming a researcher wants to examine an organisation's GRC approach and its effects on the procure-to-pay cycle, excluding IT GRC. The researcher needs to consider the following points:

- Is the organisation's approach to governance, risk management and compliance integrated, holistic and organisation-wide across the four components of strategy, processes, people and technology?
- What does the procure-to-pay cycle look like across the four components?
- Which rules affect the procure-to-pay cycle? Which of these rules need to be considered in the research project? Does the organisation treat these rules in an integrated, holistic and organisation-wide manner?
- Do the GRC specific components interact with their "general" counterparts? E.g. does the GRC strategy influence the setting of targets for the order-to-cash cycle? Are automated controls implemented in the order-to-cash application and are they linked to GRC systems?
- Are the objectives of GRC realised? Is adherence to the rules in the order-to-cash cycle efficiently and effectively ensured? Are there side effects such as improved efficiency and effectiveness of the procure-to-pay performance (e.g. lower cost, improved goods quality)? Is non-ethical behaviour prevented?

Naturally these questions may be complemented by specific questions relevant to the respective research project. Orientation along the frame of reference helps to create a high-level process model to structure the research.

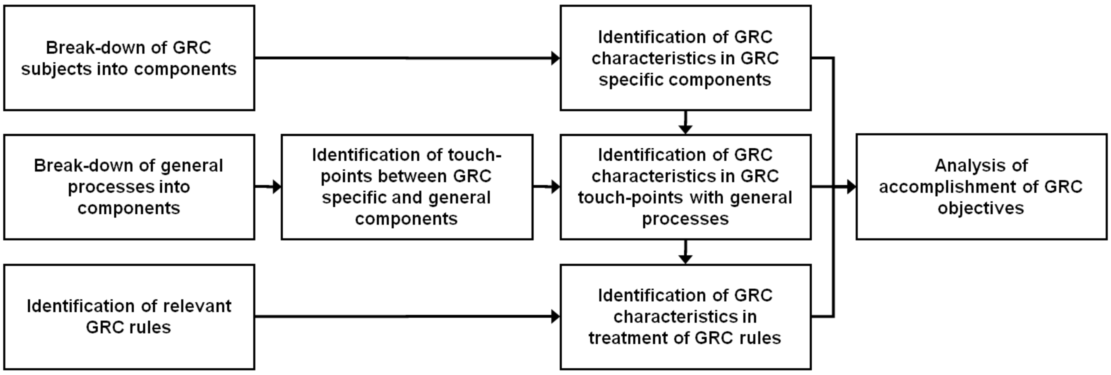

Break-down of GRC subjects into components
Identification of GRC characteristics in GRC specific components
Break-down of general processes into components
Identification of touch-points between GRC specific and general components
Identification of GRC characteristics in GRC touch-points with general processes
Analysis of accomplishment of GRC objectives
Identification of relevant GRC rules
Identification of GRC characteristics in treatment of GRC rules

Figure 16: Exemplary process model for integrated GRC research

4.5 Discussion

Admittedly, putting the complexity of GRC into a single phrase is provocative. One sentence cannot catch all inherent notions. However, in contrast to other definitions, the definition presented here considers the commonalities and the focus of the whole of prior publications and research on GRC. So far it is the only definition that has been derived in an empirical, scientific manner. Moreover it has experienced GRC professionals' acceptance as shown by the survey. Thus compared to prior definitions it should be more representative for the whole spectrum of GRC.

Of course the approach to derive a definition by means of a literature review has certain disadvantages. Some sources were of rather poor quality. The publishing groups have a business interest, which questions the objectivity of their articles. We assume that the large number of publications reviewed largely makes up for this disadvantage. Another approach could have been to conduct structured interviews with GRC experts. The effort however would have been incomparably higher if an objective result not dominated by a small number of opinions was to be achieved. In addition we doubt that the quality would have been significantly higher; the statements given in interviews would not have had a scientific foundation either.

The frame of reference naturally only displays a high-level abstraction of GRC. It does not visualize the massive complexity of GRC, but it is not meant to do that. As long as it helps researchers to gain a quick first understanding of integrated GRC in order to structure their research, it fulfils its purpose.

The contribution of this first research chapter consists of three aspects. Firstly, for the first time GRC publications have been reviewed; the lack of research on GRC is now obvious. Secondly, for the first time a GRC definition has been derived rigorously in a scientific manner and it has been validated by GRC professionals, thus proving its relevance. Thirdly, a frame of reference has been constructed that may be used for GRC reference modelling or other research of integrated GRC. The knowledge base of the information systems research framework (Hevner, March, Park, & Ram, 2004) has been extended (while the use of our results is not restricted to IS research, of course). If the complexity of GRC has so far been a barrier holding off research, we hope that we have lowered this barrier.

4.6 Conclusion

The analysis at hand clearly shows that integrated GRC is a widespread topic that has not yet been adequately researched. We can see what happens to a topic that lacks a common forum for communication of professionals as research could offer. The information provided publicly remains at a high level; understandably neither software companies nor consultancies want to give away their knowledge for free. Different products and marketing efforts have created a domain consisting of lots of shared buzzwords but missing clarity. The myriad of perceptions of GRC harms the development of a rising topic. At least there is a consensus on a few key points regarding GRC which we included in our results. Our definition and the frame of reference are a first step towards a more active role of research in integrated GRC. We encourage other researchers to build on our results and to use the definition and the frame of reference in their own research of GRC, as we did in the following sections.

Chapter 5. GRC software as seen by software vendors and market research

Software vendors' perspective on GRC is a driving force in today's GRC domain with a strong impact on the public perception of the topic (Racz, Weippl, & Seufert, 2010a). Our literature review showed that the term GRC is primarily promoted by software vendors, as the authorship of 40 out of 107 reviewed publications could be attributed to one of the many technology providers (Figure 10). At present research lags behind the industry. Scientific recommendations for the architecture or functionality of GRC software have not been made, and the functionality involved in integrated GRC suites has not yet been scientifically identified. An analysis of what the GRC software industry puts under the umbrella of "GRC" could provide a good starting point for the research of GRC technology.

This part of the research project is carried out in order to answer two questions:

i. *What is state-of-the-art GRC software from the viewpoint of software vendors, market analysts and other organisations in the industry specializing on GRC?*

ii. *What are the implications of the software industry's perspectives for scientific research?*

5.1 Research methodology

A methodology consisting of four stages was designed to answer these two questions (see Figure 17).

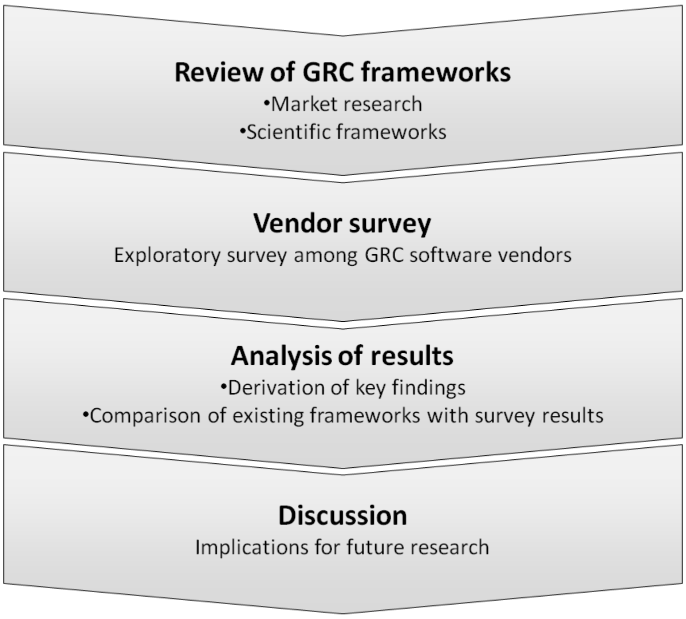

Review of GRC frameworks
•Market research
•Scientific frameworks
Vendor survey
Exploratory survey among GRC software vendors
Analysis of results
•Derivation of key findings
•Comparison of existing frameworks with survey results
Discussion
Implications for future research

Figure 17: Research methodology for chapter 5

First we review existing scientific and market research containing GRC software classifications and frameworks. Section three provides an overview of the sources identified.

In a second step we conduct a survey among vendors of GRC software suites. The survey was limited to ten questions in order to increase the probability of participation. The questions were developed drawing on our understanding of GRC gained in chapter 4, thus building on the GRC short-definition (Racz, Weippl, & Seufert, 2010a). The questions can be subsumed under three main categories: two questions about the vendors' understanding of GRC in general, five questions about the vendors' present GRC software portfolio, and three questions about the vendors' future GRC software portfolio. The whole questionnaire is displayed in Appendix C – GRC vendor survey questionnaire.

For selection of respondents we wanted to focus on providers of "integrated GRC management suites", i.e. vendors that try to offer solutions covering as many aspects of governance, risk, and compliance management as possible. Vendors of point solutions such as pure risk management software were not in scope. Therefore we based our selection on the vendor list of the 2008 Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Management (Caldwell & Eid, 2008) and added further vendors that claimed to provide integrated GRC solutions. The resulting 27 companies were contacted through email and asked for participation several times. Eventually eight vendors returned answers, a response rate of 30%. One set of answers had to be disregarded because its quality was insufficient. The participants taken into consideration were CA, IDS Scheer, MetricStream, Protiviti, SAP, and Wolters Kluwer, and Paisley (which was meanwhile acquired by Thomson Reuters).

The answers sent to us were prepared by heads of product development or portfolio managers from marketing. Where responses were unclear we contacted the vendors again and clarified the issues. Depending on the nature of the topic, answers were processed in different ways in order to find common or distinguishing elements (see Table 3).

Table 3: Survey evaluation methods

Questions	Evaluation Method
Q1: GRC definition	Decomposition of GRC short-definition into twelve components; comparison of congruence with vendor answers; calculation of percentage of congruence;
Q2: GRC and ERM	Qualitative analysis
Q3,4: GRC portfolio	Standardization of wording; identification and exclusion of non-functional features following the classification of Roman (1984); statistical analysis of functionality mentioned; resulted in 35 different functional capabilities, not counting regulation- or methodology-specific modules (e.g. ISO9000 or Six Sigma); statistical analysis
Q5: Unique selling point	Answers not used in this research
Q6: Customer benefits	Standardization of wording; statistical analysis
Q7: Centralization	Qualitative analysis
Q8,9,10: Future trends	Qualitative analysis

In the third stage we bring together the results from the survey with a deeper analysis of the existing frameworks identified in the first step in order to see in how far the views on GRC software of software vendors are congruent with those of market research and other organisations. We identify eight key findings that are the primary result of our research. Figure 18 gives an overview of the research structure, depicting which findings (F1...F8) were derived from which answers to the survey questions (Q1...Q10) and from the analysis of existing models. The findings are described in section 5.3.

In the fourth stage the implications of the findings for scientific research are discussed. They are presented in section 5.4.

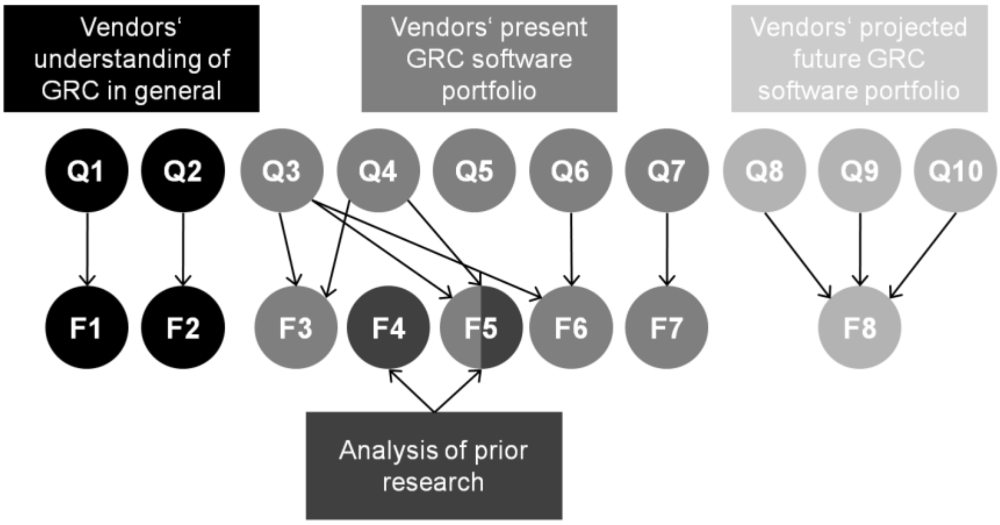

Vendors‘ understanding of GRC in general
Vendors‘ present GRC software portfolio
Vendors‘ projected future GRC software portfolio
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
F1
F2
F3
F4
F5
F6
F7
F8
Analysis of prior research

Figure 18: Derivation of research findings from survey and existing frameworks

5.2 Review of existing GRC classifications and frameworks

So far research on GRC software has only been carried out as typical technology market research by Gartner Research, Forrester Research and AMR Research, and by the Open Ethics and Compliance Group (OCEG) that provides a framework for GRC information technology.

Gartner defined a “Comparison Model for the GRC Marketplace” (Proctor, Caldwell, & Eid, 2008). It is applied in the yearly composition of the “Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms” that evaluates and ranks vendors’ GRC portfolios. Gartner identifies four primary functions of enterprise-wide governance, risk, and compliance platforms: audit management, compliance management, risk management, and policy management (Caldwell & Eid, 2008; Caldwell, Eid, & Casper, 2009).

A similar study is regularly provided by Forrester Research as “The Forrester Wave: Enterprise Governance, Risk and Compliance Platforms” (McClean, 2009). The functional categories of GRC platforms as identified by Forrester are policy and procedure management, risk and control management, event and loss management, and GRC management and analytics. Furthermore Forrester considers “technical functionality” in the areas of content management, process management and project management, but the category also includes non-functional criteria such as scalability, usability, configurability, flexibility and ability to integrate.

AMR Research published a GRC framework in 2008. Through a mix of general research and vendor evaluation they developed a GRC taxonomy consisting of three categories: GRC management software, GRC execution capabilities and GRC applications that “address specific business processes as identified by regulatory agencies across the globe or industry-led consortia that may or may not incorporate specific GRC management and/or execution components" (Hagerty, Verma, & Gaughan, 2008). GRC management applications comprise risk and control frameworks (e.g. policies), risk management software, dashboards and reporting, as well as initiative-specific content. Access controls and identity management products, business process controls, audit testing tools and data security products are part of the GRC execution category. GRC applications are a myriad of products managing specific issues (e.g. environmental health and safety, global trade management or IT risk management). The category is not defined in more detail.

Since AMR only publishes vendor profiles one-by-one, they can adapt their framework in a flexible manner for each vendor analysis, while Gartner and Forrester are forced to confine the GRC platform more strictly. As AMR Research was acquired by Gartner in 2009, it is not sure if its current framework will remain in use.

The same market research companies also provide high-level research of GRC software portfolios in general, e.g. "The Enterprise Governance, Risk and Compliance Platform Defined" by Gartner (Caldwell, 2008) or "The GRC Technology Puzzle: Getting All The Pieces To Fit" by Forrester (McClean, McNabb, & Dill, 2009). An older framework for GRC software has been provided by Rasmussen for Forrester Research (Rasmussen, 2007). It consists of four levels. The lowest layer is the supporting technology infrastructure software. Financial risk software and operational risk and control software constitute the second level. The third level consists of the GRC platform, including policies, procedures and controls, risk and control assessment, risk analytics and loss, events and investigations management. Enterprise risk management dashboards on the fourth level complete the framework. On request however Rasmussen stated that this model is now deprecated.

The market research models are useful for the purpose of ranking products of a clear-cut, delimited hypothetical market, but they aggregate functionality on a level that is too high to enable deeper analysis for scientific research purposes without access to internal methodology documentation. The results of software vendor rankings differ depending on which research company's framework and methodology is used, underlining the differing composition and priorities of the models applied. Without further ado it is not possible to say if one of the frameworks is more or less valid than the others. Being deprived of the research companies' documentation, scientific research can only determine the common and distinguishing elements of the various frameworks.

A more exhaustive and detailed classification of GRC software is provided by the non-profit organisation "Open Compliance and Ethics Group" (OCEG) in its "GRC-IT Blueprint" (OCEG, 2009). OCEG lists 72 GRC software applications, which they call "technology modules". These are mapped to one of three "technology levels" as well as to one of nine "technology arenas". The technology levels are (software) infrastructure, business applications, and GRC specific applications. The nine technology arenas consist of corporate governance, assurance and audit management, business intelligence, business process management, enterprise content management, enterprise resource management, human resources management, security management and risk management.

The OCEG model is more detailed than the market research frameworks. Also professionals from various organisations were involved in its creation. However it shares some deficits with the market research frameworks. They all lack transparency and their scientific validity is not verifiable as the methodology that led to their construction has not been published. Moreover as the frameworks are not openly accessible their application is restricted to a small community of users that is able and willing to pay for the reports. The different GRC perspectives presented inhibit the development of a common understanding of integrated GRC software suites and their components.

Despite these shortcomings the frameworks could theoretically still be useful for research as a basis for a first identification of GRC software. The whole of the functionality mentioned could give an indication about components possibly enabling integrated GRC; common elements might indicate a higher importance of certain functionality over other components. So far an identification of the frameworks’ common elements has not been conducted. Therefore in this research the existing frameworks were compared and in addition matched against the software vendors’ perspectives on GRC as provided through our survey.

5.3 Analysis of results

The following section describes the eight main findings of this research chapter in detail.

5.3.1 F1: Software vendors share a common basis in their understanding of GRC

In order to ensure comparability of survey answers it was important to see if participants followed the idea of integrated GRC as we see it to a sufficient extent. For this purpose we matched the vendor definitions against the as of today sole scientifically derived short-definition of GRC (Racz, Weippl, & Seufert, 2010a): “GRC is an [integrated, holistic] approach to [organisation-wide] governance, risk and compliance ensuring that an organisation [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].”

At average 58% of the definition’s twelve components (marked in square brackets) were matched in vendors’ definitions, with a standard deviation of 14,4%. The largest congruence was found to be 75%, the smallest 42%. The median of 58% matches the average exactly. The aspects most rarely included were people (once), ethics and efficiency (twice each). Integration was mentioned explicitly by all vendors but one, who mentioned it implicitly. The integrated approach to GRC is the key prerequisite to enable a comparison of the participants’ answers.

The congruence of vendors’ GRC definition with the definition applied in this research is sufficiently high to allow for a purposeful analysis. Vendors are sharing a common basis in their definition of the term GRC.

5.3.2 F2: Software vendors see the relation of GRC and ERM in two different ways

The relation of GRC and Enterprise Risk Management (ERM) has been discussed briefly by Banham (Banham, 2007), who concluded that there were different perceptions. Our survey identified two distinct viewpoints of the GRC-ERM-relation. Either ERM and all of its components (such as risk identification, risk assessment, risk monitoring, etc) are considered a part of GRC (P1 in Figure 19); or ERM and GRC are perceived as interconnected, partially overlapping methodologies that share certain processes and technologies enabling these processes (P2). Consequently in the first case processes exclusive to ERM are classified as being part of GRC, whereas the second perspective puts them outside the GRC domain.

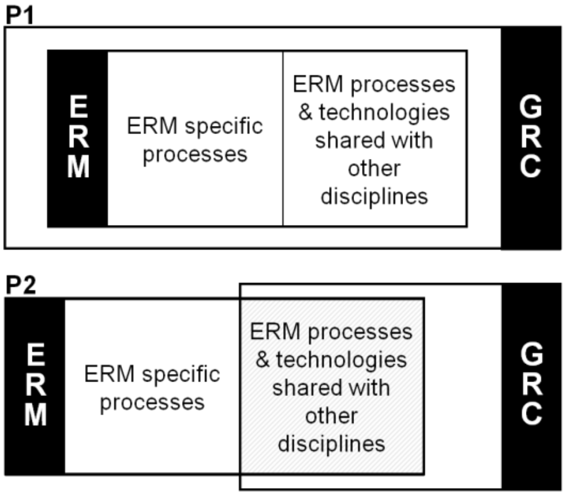

P1
ERM
ERM specific processes
ERM processes & technologies shared with other disciplines
GRC
P2
ERM
ERM specific processes
ERM processes & technologies shared with other disciplines
GRC

Figure 19: The two perceptions of the GRC-ERM relation

In our survey four companies supported the first perspective, while three stated that ERM and GRC only shared a number of common elements. For vendor CA, for instance, GRC is the unification of ERM and compliance. Protiviti notes that definition-wise GRC and ERM are very similar, but market practices show the actual difference: They claim that GRC typically encompasses a broader spectrum of activities associated with managing an organisation while ERM has tended to be more focused on a subset of activities and processes to manage risks within an organisation.

5.3.3 F3: Vendors' perceptions of GRC functionality are diverse

Vendors have different perspectives on which functionality should be delivered by GRC software. We asked vendors to list the functional capabilities of their GRC portfolios. The answers were harmonized as different wording was often used to describe the same or strongly overlapping functionality, e.g. risk management and enterprise risk management, or event management, issue management and incident management. We built groups of overlapping and synonymous functionalities where possible.

Harmonization resulted in a list of 35 high-level functionalities. Only 13 were named by more than one vendor. They are listed in Table 4.

Table 4: GRC software functionality named by more than one vendor

Function	**# times mentioned**
Risk management (RM, ERM)	7
Policy management	7
Audit management	7
Reporting / dashboards / analytics	7
Case / issue / event / remediation / loss management	6
Operational risk management	5
Compliance management	5
Controls testing and management	4
Financial controls	3
Surveys	3
Workflow management	3
Corporate governance	2
IT audits and compliance	2

The vendor mentioning the fewest components came up with seven items. For one vendor we counted 15 items even after harmonization. The average vendor listed 11.86

different GRC capabilities (median: 12) with a standard deviation of 2.67 items. At average each capability was named in 2.37 out of the seven answers with a standard deviation of 2.16. Consequently there is a rather low degree of congruence. Vendors share a common core of GRC capabilities, but apart from the core the GRC functionality offered is very vendor specific.

22 capabilities were only mentioned once each: program and project management, corporate social responsibility, training management, quality management, non-conformance management, supplier quality management, GRC management, configuration management, document management, role-based security, risk and control assurance, IT governance, IT GRC, supply chain risk and compliance management, global trade management, environmental services, testing and documentation, sign-off management, mapping of policies, risks and controls with processes and hierarchies, internal control system definition, documentation and publication, and fraud detection.

Certainly many of these capabilities are delivered by other vendors as well, but they are not part of their GRC core functionality and thus were not mentioned. Moreover some capabilities, such as sign-off management, may be part of another vendor's compliance management module and were therefore not separately listed.

5.3.4 F4: The scope of existing GRC software frameworks varies strongly

In order to compare the three frameworks from technology market research as described above, they were mapped and classified using the AMR categorization of GRC management, execution, and application software. To a large extent the components described in the frameworks overlap (Table 5).

Table 5: Comparison of market research GRC frameworks

	AMR	Forrester	Gartner
GRC management	Risk and control framework	Policy and procedure management	Policy management Compliance management
	Risk management software	Risk and control management	Risk management
	Dashboards and reporting	GRC management and analytics	
	(non-functional: Initiative-specific content)	Event and loss management	
GRC execution	Access controls	Parts of the “technical functionality” category, but no focus of the framework	
	Identity management		
	Business process controls		
	Audit testing		Audit management
	Data security		
GRC application	Applications for specific areas		

The functional classification of Forrester and Gartner focuses on GRC **management** capabilities. This confinement makes sense in two ways. Firstly, it helps draw clear lines between GRC solutions and other product lines such as business intelligence or enterprise content management that support GRC but also other disciplines (even though the GRC analytics included by Forrester represent an exception). Secondly, assuming an integrated GRC process the management functions are the capabilities most likely to be integrated on a single platform, or even in a single application, in order to deliver a central management tool providing an overview of GRC activities.

The scope of the AMR classification is wider than that of Gartner and Forrester, especially in the GRC execution and application categories, thus going beyond GRC management capabilities.

The OCEG GRC-IT Blueprint with its 72 technology modules is even more comprehensive and granular, to an extent that a one-to-one mapping to the market research classifications is not convenient. The OCEG category “GRC specific applications” covers many of the GRC management capabilities as identified by market research. This category consists of 30 modules covering compliance and governance, different types of controls, risk management and audit applications, and further modules such as accountability management, crisis management, discovery, helpline and hotline, legal matter management and more.

The main difference between the OCEG model and the three market research models is the list of 24 business applications that includes basically all applications somehow relevant for GRC, such as knowledge management, customer relationship management, budget and finance management, and project portfolio management. The OCEG infrastructure category contains some of the GRC execution capabilities of the AMR model – access control, identity management and data security products – but not audit tools and business process controls, which for OCEG are GRC specific applications. Other infrastructure functionality such as system logs management and physical security is OCEG specific, as it is not mentioned in the market research models.

In summary it can be stated that while certain elements (GRC management and audit management) exist in all frameworks, the scope of the four frameworks analyzed varies strongly.

5.3.5 F5: Vendors' understanding of GRC software functionality differs from existing frameworks

The 35 GRC software modules overall and the 11.86 functionalities average named by vendors are a lot more than listed by technology research companies. Consequently the GRC scope of most vendors clearly surpasses the scope outlined in the technology market research reports. The common ground of vendors and market research are the GRC management capabilities and audit management.

Compared to the OCEG GRC-IT Blueprint with its 72 technology modules, vendors' portfolios are much more delimited in scope. The deviation exists for several reasons.

Partly this is owed to the fact that the nine infrastructure technology modules identified by OCEG are hardly mentioned by the participants of our survey (IT operations management, physical security, enterprise architecture standards or configuration and change management, among others); apart from access controls, vendors do not seem to refer to this functionality as being delivered by GRC software.

Another reason is granularity; a vendor application can comprise more than one OCEG technology module while carrying only a single name; for instance "Operational Risk Management" in the vendor's understanding may already include the separate OCEG module "Risk Analytics". "Operational Assurance & Audit", "Information Technology Audit" and "Audit Analytics" may be subsumed under "Audit Management", etc.

Furthermore, some of the items in the OCEG business applications category are simply not considered to be "GRC" by vendors. Capabilities for transaction management, corporate performance management, email management or customer relationship management are actually offered by some vendors, but were not included in the survey answers. However this does not apply to all the OCEG business applications; vendors count loss management, learning & training management, document management and other modules towards their GRC portfolio. However apart from loss management and dashboards, none of these OCEG business applications was mentioned by more than one vendor.

With “news feeds”, OCEG also lists content, which we do not consider in this part of our study; with “helpline”, “hotline/whistleblower” and “physical security” it includes items that are generally not software applications in the first place.

It can be concluded that vendors at average have a broader definition and portfolio of GRC software than technology market research companies, but a more confined perspective than that described by OCEG. Vendors’ understanding of GRC software functionality therefore differs from existing frameworks.

5.3.6 F6: Vendors agree on the benefits delivered through integrated GRC suites to a large extent

Respondents were asked for the top five benefits their customers normally gain when employing their GRC solution. Of course the answers might be marketing-driven and they might not reflect the actual outcomes of GRC implementations, but they still show which benefits customers are trying to achieve, as these benefits are explicitly addressed by vendors.

The wording of the answers strongly varied, but the gist of the statements was in most cases found to belong to one of four categories: better transparency (6x), increased efficiency (6x), improved risk management (5x), and reduced costs (5x). Other benefits mentioned included streamlining the organisation through centralization (2x), alignment (2x), competitive advantage (1x) and increased agility (1x). Sometimes two benefits listed by a vendor could be attributed to the same category, hence the reduction of the number of references in sum from 35 to 28.

The result implies that the promoted customer benefits of GRC are universal, being mentioned by most of the vendors. The benefits seem to be relatively tool independent, lying in the nature of the integrated GRC approach and in commonalities of the GRC platforms.

5.3.7 Technology architectures of vendors mainly differ in their degree of integration

The technology architecture descriptions we received varied strongly in detail. Still the information provided was sufficiently comparable to conclude that – programming languages and other implementation details left aside – the main technological difference between vendors' architectures is the degree of integration. Integration aspects are found on six levels.

i. Technology infrastructure: Is the GRC software open to many platforms and can it share resources, also with other product lines? Are there hardware or database restrictions? Does complexity of the technology infrastructure increase when more GRC modules of a vendor are added because they have differing technology infrastructure requirements?
ii. Data model and data store: Are GRC modules sharing a data model wherever it makes sense? Is structured and unstructured data (documents, comments) combined and saved in a single data store?
iii. Integration with ERP systems and other relevant non-GRC software: How easily can GRC applications integrate data from other systems? Can they directly influence the process flow in these systems, for instance through direct application and execution of rules provided by GRC?
iv. Coherent reporting: Do the tools enable GRC reporting together with reporting of conventional performance data?
v. Front-end environment: Does the user experience a single environment for the various GRC applications (single sign-on, joint presentation in a portal or the like)?
vi. Front-end look and feel: Are navigation and user interface elements reasonably harmonized across GRC tools?

The integration possibilities might be one of the key enablers of GRC benefits through reduction of costs and human resources, through shortened process cycle times and improved data and process quality.

5.3.8 F8: Five key trends influence GRC technology in the near future

Based on the survey answers five key trends were identified that, according to vendors, influence the future development of GRC technology.

i. Integration of GRC with business processes: As SAP states, "GRC is not an external, 'end of process' or check the box activity, and must be integrated into the performance of a business process in order for companies to receive the greater value of GRC." Integration of GRC with business processes supports the trends towards continuous monitoring and involvement of more and more people in GRC activities (PricewaterhouseCoopers, 2007; Coderre, 2005). IDS Scheer also focuses on the aspect of business process driven GRC.

ii. Integration of GRC with performance management: Understood as a closed-loop model for managing the planning, monitoring and controlling of business processes and their performance within BPM (Martin & Nussdorfer, 2005), it is obvious that performance management will gradually be merged with GRC as a result of the integration of GRC with business processes. The key link between performance management and GRC is risk. Business risks will be considered in the planning process; they need to be monitored; and key risk indicators complement key performance indicators when deciding about control measures.

iii. Continued integration of GRC software on a single technology platform: With specialist vendors enhancing their portfolio to cover more GRC functionality on the one hand, and ERP vendors and consultancies penetrating into the market on the other hand, GRC includes a myriad of software components. Market consolidation is still in its early stages. Efforts to provide more coherent, integrated platforms are ongoing.

iv. Centralization of GRC-relevant information: The precedent trend of reducing technological complexity supports another trend: bringing together GRC-relevant information. Data warehouses historically have struggled to integrate unstructured data. Risk management is mostly carried out as a function separated from performance management, resulting in data silos. Enterprise-wide consistent document management in many companies still has not been realized. GRC-relevant information from all included activities needs to be merged, the different types of data need to be connected, and the whole needs to be presented in a seamless manner. According to CA, for example, the centralization of risk and compliance information is important in order to eliminate redundancies.

v. Improved analytics and reporting: In general vendors seem unsatisfied with current reporting and analytics solutions. Owed to the complexity of merging applications that have been managed separately so far, reporting silos still exist and analytics do not dig as deep and work as efficiently as desired. Thomson Reuters states that consistent reporting across the various disciplines of GRC should be a decisive feature of an integrated GRC suite.

5.4 Discussion and implications for research

The survey response rate of 30% is considered to be high, given that answering the survey must have taken several hours judging from the length of the responses. The high degree of participation shows the interest of vendors both to promote their own perspective on GRC and to learn more about the viewpoints of competitors.

Of course there are points of critique that can be brought forward against the research methodology applied. The questionnaire design with open answers enables vendors to elaborate on their GRC perspective, but it also introduces inaccuracy through different wording and foci. Vendors try to promote their products and therefore tend to highlight strengths and disregard weaknesses of their tools. We still decided to leave the questions open-ended so that vendors would not be confined to a frame that might inhibit gaining a full understanding of GRC as seen by the software industry.

Another issue is that the analysis of the answers might not always have been accurate because resource restrictions inhibited a deeper analysis of certain issues, for example in how far vendors' policy management applications offer the same functionality. However as the survey was conducted to gain a general idea of GRC software, and not to derive an exact technology reference model in the first place, keeping the analysis at a high level does not harm the research.

Lastly the findings represent a momentary snapshot of state-of-the-art software that will change over time. The young GRC market is in an early phase of consolidation. Recent market activity includes the acquisition of Paisley through Thomson Reuters and of Archer Technologies through EMC. The spectrum of GRC tools is still immense. One of the ideas behind integrated GRC is to reduce complexity in processes, but the merger of more and more products in GRC suites and the integration of acquired products are going to increase complexity of the technology applied. Vendors make progress with product integration on the integration levels described above. Some vendors have come far on this path because they rely on a GRC platform that has been built from the scratch, while others have more complex technology architectures due to integration challenges of diverse tools. But even vendors with advanced integration between the three disciplines face another integration challenge while GRC moves closer towards business process execution.

Aware of the possible deficits of the research at hand, what are the implications of the eight findings to scientific GRC research in general?

In the case of F2, we recommend the first perspective, with ERM being completely contained in GRC, to be adopted by GRC researchers. Otherwise they run the risk of excluding processes that bear potential for integration with other disciplines within GRC today or in the future.

F3, F4 and F5 show that the various vendors, market research companies and OCEG all have different perspectives on GRC. The common basis that vendors share in their GRC definitions (F1) has hardly led to a shared perspective on GRC functionality. F3 and F4 demonstrate that at least GRC management (risk and policy/compliance management) as well as audit management and reporting are counted towards GRC software functionality by the large majority of the organisations considered in this research.

We continue to deem the analysis of the status quo of GRC software as useful in order to identify gaps, to learn from errors made in the past, and to understand GRC requirements. However GRC technology research in general should not be based on the analysis of a single vendor's GRC portfolio or a single framework. Even the small common core of the portfolios and frameworks does not provide a firm basis to be applied in scoping GRC research; it may merely help prioritize the functionality to be examined. The same can be said about F6, F7 and F8 – they may help draw the attention of researchers towards a specific set of benefits, integration possibilities and future developments, but research should not be restricted to the results of these findings.

In addition to the findings certain elements of existing perspectives could also be used as theoretical impetus, such as the AMR distinction of GRC management and GRC execution software applied in F4 that gives an apparently reasonable recommendation for segmentation of GRC software functionality. However any concepts taken over have to be scientifically validated before being applied in research.

Apart from heterogeneity another shortcoming of the existing portfolios and frameworks underlines the cautious approach that research should take when using them. The GRC software products on the market have to be sold today; therefore they have to integrate with customer landscapes. The market research frameworks are also bound to be applicable as of now, otherwise they would not sell. Thus the creators of software and market research depend on the revenue generated through their products. Consequently both software and frameworks heavily depend on the status quo in organisations. However a new, integrated approach to GRC might require change on a larger scale, on strategic, organisational, process and technology levels. New information technology concepts might have to be applied.

To sum it up, research of GRC software should follow one of the "classic" procedures of software engineering (Ludewig & Lichter, 2006). It should start with the identification of current and foreseeable future GRC requirements. Then GRC process models to cover these requirements in an integrated manner should be developed. Finally research should derive software functionality and an adequate architecture enabling the execution of the recommended GRC processes, considering state-of-the-art and newly suggested technology from practice and research. Current GRC software does not provide a shortcut in this process.

This part of the research followed the requirements of the information systems research framework (Hevner, March, Park, & Ram, 2004). We identified that when developing and building theories and artefacts for GRC technology, research should not rely heavily on technology present in the environment. In Chapter 5 further eight key findings were derived that help researchers understand and approach the GRC domain, GRC software and GRC frameworks. Originality is given as for the first time technology market research frameworks were compared. Also for the first time scientific research compared the high-level functionality of state-of-the-art GRC software products to each other and to market research. A first consideration of these tools and models in the early phases of GRC research was indispensable as contemporary GRC software is used by many organisations world-wide; the frameworks of market research and OCEG are also widely used to facilitate buying decisions and to help understand and manage GRC.

5.5 Conclusion

The research of chapter 5 was carried out in order to find out about state-of-the-art GRC software and its implications on scientific research. As has been shown an understanding of software vendors’ GRC products and of existing GRC models can provide valuable insights, but due to the different perspectives on GRC in the industry future research should not be based purely on such an analysis. We recommend constructing reference models for integrated GRC software based on scientifically applied software engineering. For our share we will focus on GRC management processes for information technology operations, providing a process model based on the understanding of GRC gained by now and enhanced in the next chapters.

Chapter 6. GRC status quo and software use in large enterprises

GRC can be integrated horizontally (the integration of the three disciplines with each other) and vertically (the integration of GRC with business processes, as described by zur Muehlen & Rosemann (2005), for instance). ”Integration” as used in the following refers to horizontal integration. In this chapter we strive to identify the status quo of horizontal GRC and GRC software in large enterprises in order to discover future research opportunities in general and insights for this research project in specific.

6.1 Prior research

GRC frameworks from market research, OCEG and some other authors have already been mentioned above (chapter 4 & 5). In addition, during preparation of this chapter we discovered research of Marekfia and Nissen (2009), who suggest a conceptual reference framework for strategic GRC management. However their model is purely conceptual and neither do they relate their model to integrated GRC software, nor did they validate the concepts. Evidently prior research has already suggested reference models for GRC processes and it has evaluated GRC software from a functional point of view (chapter 5). However the deployment and use of integrated GRC software have not been examined so far. The research done for chapter 6 shall partially close this gap, answering the research question: *How are integrated GRC and GRC software perceived and applied in large enterprises?*

6.2 Research methodology

The methodology applied in this chapter is organised in four phases: survey design, survey execution, survey analysis and a discussion recommending actions for research (Figure 20).

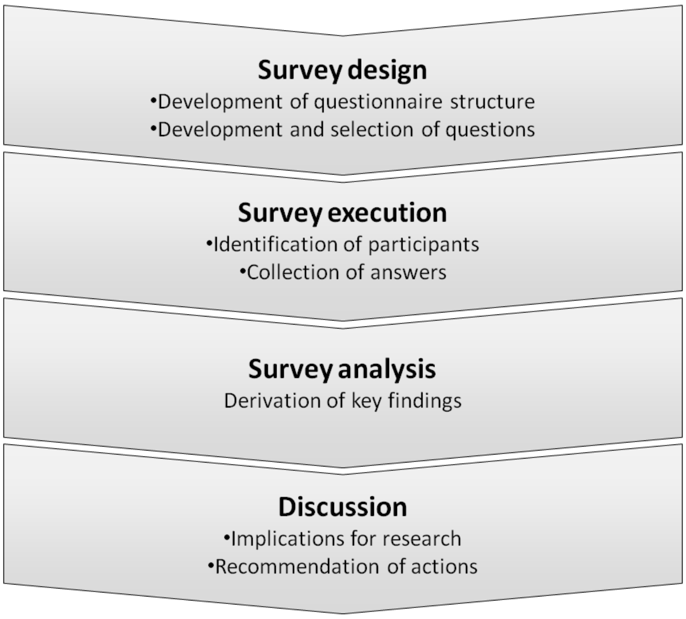

Survey design
•Development of questionnaire structure
•Development and selection of questions
Survey execution
•Identification of participants
•Collection of answers
Survey analysis
Derivation of key findings
Discussion
•Implications for research
•Recommendation of actions

Figure 20: Research methodology in chapter 6

In the survey design phase we first agreed on a common understanding of GRC, relying on the definition cited above (Racz, Weippl, & Seufert, 2010a). With this basic understanding of GRC and also respecting insights and deficits of prior GRC research described in the section above we started to develop questionnaire items that could help answer the research question and close the identified gap.

The survey was targeted towards professionals based in German-speaking countries but working for globally operating companies. The companies underlie GRC requirements from all important markets world-wide, such as the United States, the European Union, Australia and emerging Asian markets. The results should therefore be representative for all globally active enterprises, no matter where they are headquartered.

The questionnaire was subdivided into five groups. The first group of the relevant subset contained general questions concerning the respondent’s company size and field of business. Group two analysed the relation of the three disciplines and the integrated management of GRC. Statements about GRC software platforms had to be evaluated in group three. The fourth and fifth group aimed at pointing out benefits or disadvantages of GRC in general and GRC software. The subset of questions and statements used for the research at hand was spread across the five groups as shown in Table 6.

Table 6: Questionnaire Structure

Group	Topic	Questions (Q) & Statements (S) used in this research
1	Respondent's organisation	Q1, Q2
2	Status of integrated management of GRC	S1 to S5
3	GRC software platforms	S6 to S12
4	Benefits and disadvantages of GRC	S13 to S17
5	Benefits and disadvantages of GRC software	S18 to S26

The items of the questionnaire (apart from those in group 1) were set up as Likert scales. Respondents had to provide their views on prepared statements, the options reaching from "strongly agree" over "agree", "neutral" and "disagree" to "strongly disagree". Likert Scales are the most commonly used scaling method in empirical studies, as they are easy to construct and they facilitate the operationalisation of results (Schnell, Hill, & Esser, 1999).

Originally questions for each group were randomly suggested by the researchers. Schnell et al. (1999) point out that no formal approach exists to discover questionnaire items. Nevertheless, going forward they suggest specific rules and regulations that must be adhered to in order to develop high quality items. The researchers followed the given suggestions. A total of 30 questions were included in a draft version of the survey. Statements were formulated in a way that from case to case agreement or disagreement had to be expressed by respondents to disclose a positive attitude. Thereby biases due to constant agreement to items without reading them were softened.

An online version of the draft questionnaire was subsequently created using the survey tool "EFS Survey Uni Park". A pre-test was carried out in order to ensure validity, clarity and a correct understanding of the questions and statements. Five pre-test participants provided their feedback. Questionnaire items were revised or eliminated based on the pre-test results. Two questions and 26 statements remained in the final version of the questionnaire.

The survey execution phase started with the identification of potential participants by means of a review of recent GRC publications, through recommendation of other experts and through utilising social and professional networks. In order to qualify for participation people had to hold positions mainly concerned with governance, risk management and compliance. The identified professionals were contacted and asked for participation in the survey either personally or through posts in interest groups of GRC practitioners. 151 professionals indicated that they were interested in participation. The questionnaire was placed online where it was available for an entire month from January 11 until February

11, 2010. The link to the questionnaire was sent to the identified participants via email. In total 99 of the initially contacted 151 participants completed the questionnaire, resulting in a response rate of 65.6%.

In the survey analysis phase the results were examined and reviewed in depth. Out of the 99 respondents 48 stated that they worked for large organisations with over 10,000 employees; only the answers of these 48 participants were considered in the research at hand, as otherwise the heterogeneous characteristics of organisations with different sizes would have harmed comparability of the answers, and because this research generally focuses on GRC in large enterprises. A complete list of the statements and answers per Likert category in percent is attached in Appendix D – Results from survey among large organisations. The results were used to derive five key findings (KF). Each finding was based on a distinct set of answers (see Table 7). The key findings are described in the results section.

Table 7: Derivation of key findings

Key findings	**Statements (S) used**
KF1	S1, S2, S3, S6
KF2	S13, S14, S15, S16, S17
KF3	S6, S7, S8, S9, S10, S11
KF4	S12, S18, S19, S20, S21, S22, S23, S24
KF5	S4, S5, S25, S26

Finally, in the fourth phase the key findings are discussed and recommendations for research actions to follow up on the findings are given.

6.3 Results

6.3.1 Key finding 1

KF1: Efforts to integrate the three disciplines governance, risk management, and compliance with each other are more advanced on the organisational than on the process or information technology level, as many organisations are undetermined concerning the importance of an integrated GRC strategy.

The frame of reference for GRC research in chapter 4 suggests examining GRC integration within and across four components: strategy, processes, people (the organisational structure) and technology (Racz, Weippl, & Seufert, 2010a). From a strategic viewpoint the integrated approach to GRC is only supported by slightly more than a third of organisations. While 37% of organisations attach importance to integrate GRC activities and while only 21% do not, a large number of organisations (42%) is undetermined concerning the importance of GRC. Thus many organisations have not yet bought into the integrated GRC concept.

On the process level less than a third of organisations integrate GRC activities instead of keeping them in silos (27%). As far as the technology level is concerned, only 29% have implemented integrated activities on a uniform, comprehensive IT platform. The organisational integration is more advanced: 44% of organisations already have a central department that is responsible for GRC activities. On the road from separate disciplines to an integrated GRC approach it seems that first the structural organisation is changed before the process organisation is amended hand-in-hand with changes in the IT implementation of GRC processes. Only five out of 27 organisations have integrated GRC processes or platforms without having a central GRC department.

Of the 18 organisations that attribute importance to GRC, 61% have a central GRC department; 56% have integrated GRC processes, 50% an integrated IT platform for GRC. This shows that even in the organisations that are deeming GRC integration important, there is still a lot of potential – the integration of GRC is ongoing.

6.3.2 Key finding 2

KF2: Integrated GRC is deemed useful, as it acts as a link between strategic objectives and daily operations, and as it improves risk management and even creates competitive advantage.

The benefits of integrated GRC have so far not been proven by scientific research. Business cases have not yet been created, and theoretical models are rather vague about the supposed benefits, describing them only at a high level. Ethically correct behaviour, and improved efficiency and effectiveness of all components involved in GRC (Racz, Weippl, & Seufert, 2010a) or stakeholder satisfaction and potential benefits (Marekfia & Nissen, 2009) are very general categories hardly useful for analysis.

Asked if the efforts of integrated GRC approaches outweighed the benefits, only four percent of respondents agreed, while 58% disagreed and 15% disagreed strongly. Benefits are achieved because GRC links strategic objectives and daily operations, said 61% of participants; better transparency in risk management is enabled (57%) and the integrated approach helps prevent risks (75%). 81% of participants even stated that GRC can create competitive advantage by means of improved risk management. The link of GRC and competitive advantage is supported by (Amberg & Mossanen, 2008) from a compliance viewpoint. They point out that companies adhering to rules and regulations and thus being among the high performers in GRC are attributed a more positive image by their customers, resulting in better customer retention and higher sales.

6.3.3 Key finding 3

KF3: Nearly half of organisations uses software labelled "GRC"; in-house developments are preferred over standard solutions.

46% of the organisations in our survey have deployed GRC software that covers multiple governance, risk and compliance aspects. Only 29% state that all GRC activities are consolidated in a single software platform, however.

Such integrated GRC suites are offered by a variety of vendors such as CA, IDS Scheer, Metric Stream, Oracle, Protiviti, SAP, Thomson Reuters and Wolters Kluwer. They vary in the functionality offered as well as in their degree of integration on the technology infrastructure and data levels, on the front-end, in reporting and with enterprise resource planning systems (Racz, Weippl, & Seufert, Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives, 2011). The heterogeneity might be attributed to the fact that there are few well known standards to refer to (Dameri, 2009). Only 14% or 7 organisations in the survey have deployed such a standard solution, while 40% rely on in-house developments. Three companies (6%) use both at the same time. 73% of organisations still use a separate compliance application, and 64% use separate risk management solutions.

Of the 29% (14) of respondents say all GRC activities are covered by a uniform software platform, 4 use a standard solution; 5 use an in-house developed solution; 2 use both types of solutions that somehow seem to be integrated nonetheless. The remaining two respondents were unsure about the origin of their organisation's software platform.

Altogether our survey draws a fragmented picture of GRC software landscapes. Most companies use several solutions at the same time, partially integrated and partially stand-alone, generic and tailor-made.

6.3.4 Key finding 4

KF4: The application of integrated GRC software helps leverage the benefits of integrated GRC.

When asked about the benefits of GRC software, respondents can be divided into two groups: those who are convinced of its benefits, and those who do not feel capable to judge if GRC helps leverage the benefits of integrated GRC. Only 4% see GRC software as a pure cost factor, but 52% cannot say if investing in GRC software pays off. Nobody agrees that the application of GRC software is useless and 58% are sure that it is not, but 42% cannot say.

The majority of respondents states that an integrated platform brings improvements in risk management (71%) and compliance (63%). In the eyes of the respondents GRC software helps connect formerly siloed activities. 52% state that GRC software offers an organisation-wide view of GRC processes (12% disagree), 54% think it helps highlight the interrelations of risks across the enterprise, and 46% say it integrates risk management and compliance through showing the relations of risks and regulations (46% “neutral”).

Of the 19 companies using in-house developed GRC software, 47% are convinced that their GRC implementation pays off (42% cannot tell, 11% disagree). 79% agree that they see improvements in risk management (16% disagree), 74% agree that there are improvements in compliance (5% disagree). 68% agree that GRC software offers an organisation-wide view of GRC processes (16% disagree). 79% say it helps see interrelations of risks (11% disagree), 58% say it connects risks and regulations (16% disagree).

Of the 7 companies using standard solutions for GRC, 71% are convinced that their GRC implementation pays off (29% cannot tell). 100% agree that they see improvements in risk management, 100% agree that there are improvements in compliance. 86% agree that GRC software offers an organisation-wide view of GRC processes (one company disagrees). 86% say it helps see interrelations of risks (one company does not know), 71% say it connects risks and regulations (one company disagrees, one does not know).

Thus it seems that enterprises that have deployed standard solutions are more satisfied with their GRC software than companies that have chosen the do-it-yourself approach.

6.3.5 Key finding 5

KF5: Integrated GRC reports are in use, but reports generated through existing solutions are not considered adequate.

40% of the organisations that participated in the survey deliver integrated GRC reports to management. Software is a key in delivering these reports. 58% of respondents agree that GRC software helps automate documentation and reporting, while only 14% disagree. However 57% state that the reports generated through the GRC software solutions are not sufficient. Only 10% of organisations with integrated GRC reports confirm that the reports provided to management are adequate in content, clearness and quality.

29% of the respondents from companies that use standard GRC software agree that it does not provide sufficient reporting functionality. 43% are neutral about the standard solutions’ reporting. On the other hand, also 60% of the organisations that use custom tailored software solutions for GRC management agree that the reporting function does not fully fit their needs (21% neutral).

Within GRC, reporting and monitoring are not only a one-way activity with data from operations being collected and aggregated and then sent to management. The results of GRC monitoring are used in a closed loop and thereby influence planning activities in 59% of organisations. However, half of these organisations agree that their current reporting is not sufficient to be used as a basis for planning. Due to the unavailability of comprehensive GRC reporting tools, these companies are nevertheless building future plans on whatever data is available. A broader and integrated GRC reporting would thus be beneficial to these organisations. GRC monitoring and reporting can also serve to identify areas for process improvements. This underlines the need for an appropriate workflow that ensures adequate action on basis of reported data. Furthermore transparency on GRC status, findings and follow-up can be ensured. The widely accepted balanced scorecard concept could form the basis of such an integrated GRC reporting as recommended by Panitz et al. (2010).

6.3.6 Summary of key findings

Figure 21 shows a graphical summary of the five key findings that were derived from our research. These should result in a set of actions for researchers. Recommended actions will be discussed in the following.

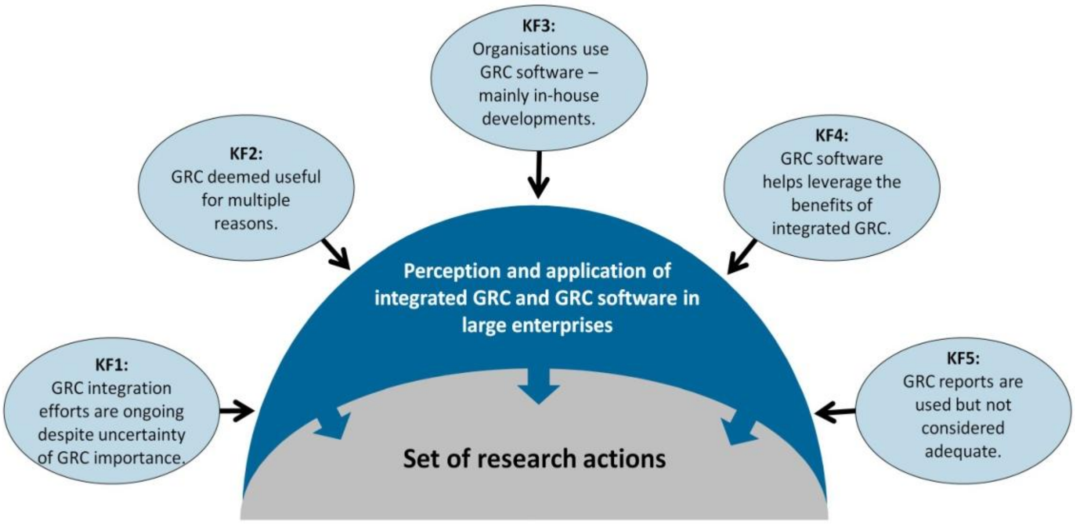

KF3:
Organisations use GRC software – mainly in-house developments.
KF2:
GRC deemed useful for multiple reasons.
KF4:
GRC software helps leverage the benefits of integrated GRC.
Perception and application of integrated GRC and GRC software in large enterprises
KF1:
GRC integration efforts are ongoing despite uncertainty of GRC importance.
KF5:
GRC reports are used but not considered adequate.
Set of research actions

Figure 21: Overview of the five key findings

6.4 Discussion

To follow up on the findings we can recommend a set of actions for research.

6.4.1 Action for KF1: Identify potentials for GRC integration

KF1 has shown that the status quo of GRC integration is unevenly distributed across the four levels of strategy, processes, the organisational structure and technology. Large enterprises are not sure about the importance of an integrated GRC strategy. First actions are focused on the adaption of the organisational structure. Research should identify how organisational amendments such as the consolidation of responsibilities, the creation of competence centres and centralised GRC departments can support the integration of GRC activities. Likewise research should focus on the integration of GRC processes in different areas (like Racz et al. (2010b)) and on integration potential offered through GRC software.

6.4.2 Action for KF2: Examine benefits of integrated GRC in more detail

Our finding has only provided a superficial first impression of how GRC benefits are perceived in large enterprises. The results should be followed up through case studies examining GRC processes before and after integration. Several questions need to be answered. Can the integration of GRC activities help decrease costs? Do risk and compliance management show improved efficiency and effectiveness? Does the integration have a positive impact on financial results or on the market value of enterprises? How do the results relate to the benefits mentioned in theoretical models?

6.4.3 Action for KF3: Highlight the deficiencies of standard GRC software solutions

Our survey has shown that in-house developments are preferred over standard solutions for integrated GRC software. Possible explanations should be examined. For instance there could be functional differences between insufficient standard solutions and in-house developments. But companies could also have been driven by cost considerations when opting for the “make it” approach. Maybe standard solutions were insufficient when the “buy or make” decision was made, but meanwhile they have evolved and deficiencies have been eliminated. If still existent the deficiencies represent a research gap that needs to be identified before developing GRC reference models or implementations in information systems research.

6.4.4 Action for KF4: Find out how GRC software can help leverage benefits of integrated GRC

Research should examine the influence of GRC software on the benefits of integrated GRC identified in beforehand (see action for KF2). Do integrated GRC platforms enable more efficient auditing? Can licensing and administration costs be saved through moving from a siloed landscape to a holistic single-vendor-solution? Maybe process cycle times in risk and compliance management are reduced through the application of software solutions. According to a survey among GRC vendors, the benefits delivered through integrated GRC suites are mainly increased transparency and efficiency, improved risk management and reduced costs. Do these benefits really exist, or are they marketing inventions? The main enabler of leveraging benefits could be a common data store, or harmonised GRC processes embedded into an integrated application, or automated controls, for example. A means of achieving the benefits could also be the complete integration of GRC software with the business process software landscape, for instance with enterprise resource planning (ERP) systems, as foreseen by Müller and Terzidis (2008); the authors claim that until then today’s “supervenient” systems – separate GRC solutions that need to be adapted whenever changes in the ERP environment are implemented – will remain in place.

6.4.5 Action for KF5: Create a reference model for integrated GRC reporting

Finally the fifth key finding draws out the need for an integrated reporting of GRC activities. The primary purpose of central GRC reporting is to automate much of the work associated with the documentation and reporting of GRC management (Caldwell, 2008). Current reporting solutions however are not sufficient and do not provide a comprehensive overview of the GRC status, results and subsequent actions. A single source GRC reporting is required that reduces the number of reports the people in charge of GRC receive, thus providing more transparency to GRC management (Dawson 2008). Research should provide answers to various questions. Could existing reporting tools and concepts be adapted for a comprehensive GRC reporting? What should a recipient focused GRC reporting look like? Which major key performance indicators must be included? Which additional workflows and processes are deemed necessary? How could reporting be used in GRC benchmarking? What additional benefits could be achieved through the central availability of GRC data? The answers to all these questions should be used in the creation of a reference model for integrated GRC reporting that describes the processes, contents, technology and organisational roles involved. The path from single manually composed reports in spreadsheets towards integrated compliance dashboards and scorecards should be highlighted. To ensure a company-wide and comprehensive GRC reporting, a solution should be described that can be integrated into standard as well as into custom developed GRC software. It should allow for a single source and an integrated GRC reporting and in addition comprise a comprehensive workflow that covers remediation as well as risk mitigation activities. In the area of GRC reporting there is room for extensive future research.

6.4.6 Summary of actions for research

Figure 22 summarises the recommended actions for research.

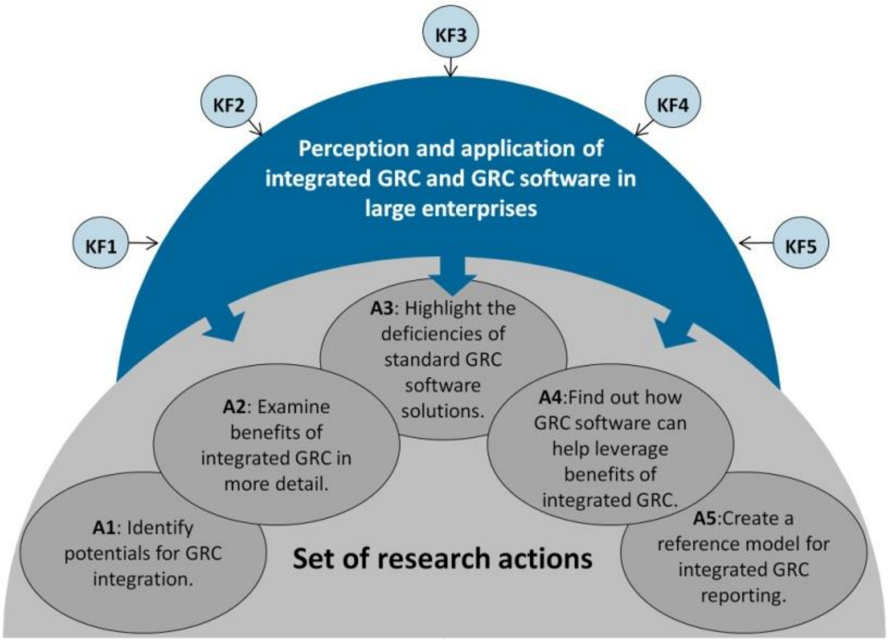

KF3
KF2
KF4
Perception and application of integrated GRC and GRC software in large enterprises
KF1
KF5
A3: Highlight the deficiencies of standard GRC software solutions.
A2: Examine benefits of integrated GRC in more detail.
A4:Find out how GRC software can help leverage benefits of integrated GRC.
A1: Identify potentials for GRC integration.
Set of research actions
A5:Create a reference model for integrated GRC reporting.

Figure 22: Overview of research actions

6.5 Critique and contribution

Discussing the findings we also need to take into account possible deficits of this research. Firstly the respondents' expertise could only be assumed and it was not verified. The many answers showing a high percentage in the "neutral" column might originate in the generally tough tangibility of GRC; however it could also be attributed to respondents being unsure because the statements overstrained their knowledge. Secondly the survey remains at a high level at some points because due to the large size of the questionnaire we did not ask respondents to name the reasons that led to their choice of answers, for instance. More detailed analysis will have to be provided through carrying out the actions recommended above.

Chapter 6 contributes to information systems research. Following the information systems research framework (Hevner, March, Park, & Ram, 2004), the survey has provided new information about several aspects of the research environment: the integration of governance, risk and compliance in large enterprises. The key findings help understand businesses' perceptions of integrated GRC and GRC software. The findings and the recommended actions can be used to further examine the environment until a sufficient understanding is gained to build more concrete theories and artefacts for design science, such as scientific GRC reference models (in contrast to the existing industry reference models identified in the prior research section) or software components.

6.6 Conclusion

In this chapter findings concerning the perception and application of integrated GRC and GRC software in large enterprises were discovered by means of a survey. The study has shown that the integration of GRC and the application of GRC software are ongoing topics in business that require more research. Thus from the findings a set of actions was derived that can help research gain further insights on the status quo and potential of GRC integration in business practice.

In this research project we are going to follow up some of the recommended actions, especially action for KF1, and to some extent also actions for KF2, KF3 and KF4. Through an analysis of GRC in the IT organisations of selected large enterprises we are going to analyse the status quo of IT GRC processes in detail (chapter 7) and we will elaborate on potentials for integration. In the course of that study we will also build a process model for IT GRC management (chapter 9).

Chapter 7. Integration of IT GRC – status quo in business practice

After having explored GRC in general, it is now time to turn to GRC for information technology. This chapter covers most aspects of the frame of reference for research of integrated GRC focusing on IT operations that are managed and supported through GRC.

7.1 Turning to GRC for information technology

Over the last decade the pressure on information technology managers in enterprises has steadily increased. The auditing profession observes a trend away from the examination of outcomes towards assurance of the processes that produce these outcomes (PricewaterhouseCoopers, 2007). Hence the growing importance of IT in enabling business processes has shifted the focus of auditors towards information systems. At the same time high-impact regulations have created new requirements for governance, risk management, and compliance in information technology.

According to the information systems research framework (Hevner, March, Park, & Ram, 2004), the relevance of scientific information systems research for the targeted environment has to be ensured. The involvement of people, the use of technology, strategies, and processes in the environment have to be considered. So far we hardly know anything about efforts to integrate GRC in information technology departments. As research lags behind the industry, an analysis of IT GRC in business practice is a good starting point to catch up.

As noted in chapter 4, scientific research on integrate GRC approaches is scarce. The relation of integrated GRC and IT has been examined even less. The ACM Digital Library returns no relevant result that takes a comprehensive view of GRC when searched for GRC as an acronym or for “governance, risk, compliance”. Sometimes two of the three disciplines were studied. For instance the connection of governance and compliance in information technology has been described superficially in an editorial (Müller & Terzidis, 2008) and through an analysis of the use of the two terms in the internet (Teubner & Feller, 2008). Both sources ignore the relation to risk management and are thus incomplete from the viewpoint of GRC.

In order to further catch up with IT GRC developments in the industry, the analysis of IT GRC in business practice is a consequential next step. With the understanding of the status quo and GRC integration efforts gained in such an analysis, the relevance of further research for the environment can be assured. Therefore chapter 7 answers the research question: *What is the status quo of IT GRC and its integration in large enterprises?*

7.2 Research methodology

As answers to the research question were not available in literature, it was obvious that primary research was required. Chapter 7 was carried out in four stages as depicted in Figure 23.

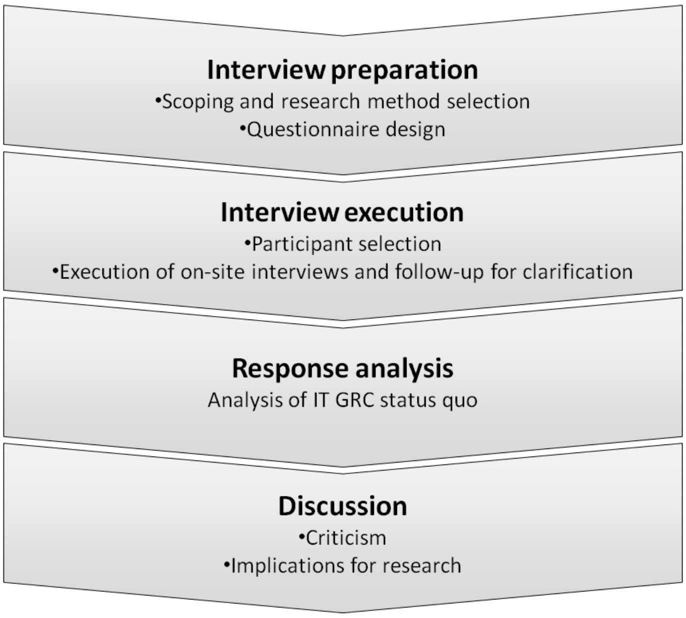

Interview preparation
•Scoping and research method selection
•Questionnaire design
Interview execution
•Participant selection
•Execution of on-site interviews and follow-up for clarification
Response analysis
Analysis of IT GRC status quo
Discussion
•Criticism
•Implications for research

Figure 23: Research methodology in chapter 7

In the preparation phase we first used the frame of reference for research of integrated GRC (see Figure 14) for scoping. The “operations managed and supported through GRC” in this case are operations of the IT departments. All other elements of the frame were considered in varying detail. We wanted inquire about all four components (strategy, processes, people and technology), across all three disciplines, and we looked if they were integrated and applied organisation-wide and holistically. GRC outcomes and the rules of GRC (internal policies, external regulations and the risk appetite) were only briefly addressed.

In selection of an appropriate research method qualitative methods were preferred (Myers, 2009) as the unsought topic of integrated GRC required direct interaction with respondents in order to explore interesting findings on the fly. Semi-structured interviews with open-ended answers should be carried out on-site among a small number of participating organisations. A pre-defined but flexible set of questions should guide through the interviews, allowing the interviewer to adapt questions to the situation, to change the question order and to ask new questions if beneficial to the procedure (Lindlof & Taylor, 2002). For comparability reasons the scope of potential participants was reduced to global IT departments based in German-speaking countries. The enterprises had to employ at least 10,000 people in a multinational organisational structure with subsidiaries in several countries. The complexity of large, globally active enterprises adds to the challenge of GRC integration, but potential synergies may be higher than in small companies.

The questionnaire design started with the decision for a basic structure of three sections: the first block treated ITG, ITRM, and ITC separately, gaining basic information such as definitions, standards followed, organisational entities involved or technology used for each of the three disciplines. The second block then asked questions about the integration of GRC. We focused on horizontal integration of the three disciplines with each other, not on vertical integration with business processes. These first two blocks were further subdivided into four question groups concerning strategy, processes, people and technology for GRC. The third block examined the relation of GRC on the corporate level and IT GRC. After the three researchers involved in chapter 7 had agreed on the questionnaire structure, potential questions were developed relying on the experience from previous chapters. The questions proposed were discussed and then admitted or rejected. The result of this process was a questionnaire (Appendix E – IT GRC integration study questionnaire) that led through the semi-structured interviews.

The interview execution phase started with the identification of relevant companies according to the scope outlined above. We were hoping for two to five participants, a small number that would nevertheless be sufficient because of the qualitative nature of the research. We approached a dozen companies from various industries that we had been in touch with through prior GRC research. The questionnaire was sent to IT managers or other personnel with the request to forward it to the people in charge of GRC activities within IT. Most companies declined the request because of confidentiality concerns, or because they did not feel mature in their IT GRC activities and probably did not want to make a bad impression, even though they knew that results would only be published after anonymisation. Finally three companies agreed to take part in the case studies:

i. TECHNOLOGY is a global provider of business software and consulting services. Its global IT department employs about 2,000 people, IT employees in business functions not included. For realisation of business processes the enterprise has mostly deployed SAP software.

ii. HEALTHCARE supplies healthcare products to clients around the world. Its large IT organisation provides the IT infrastructure and business support. SAP software is widely used by HEALTHCARE, but they also run business process solutions from several other vendors.

iii. ENERGY has most of its staff in Europe, but runs production and exploration activities in many other countries outside of Europe. Its IT department is an own legal entity fully owned by ENERGY's corporate organisation. It employs about 550 IT staff and 150 external contractors. IT personnel mainly work at two locations in Europe. Many administration tasks – about 30% of all processes supported through IT – are automated using SAP software. The SAP landscape alone has more than 7,000 users.

The interviews were all conducted by the same person in order to guarantee consistency. They were carried out in two-hour sessions within two months on the sites of participants. TECHNOLOGY and HEALTHCARE each had a single person respond to all questions, while ENERGY organised a meeting with four IT employees. Their roles are named in Table 8.

Table 8: Organisational role of interviewees in chapter 7

Participant	**Role of interviewees**
TECHNOLOGY	– Responsible person for IT Risk Management, Quality Management, IT Governance & Audit
HEALTHCARE	– Head of Global IT Compliance (also responsible for Risk Management & Audit)
ENERGY	– Head of Department: Mid- & Downstream Applications – Chief Information Security Officer (CISO) – Team Lead SAP Security; SAP CC / SAP Cross Functions – SAP Security team member

During and after the interview sessions the participants provided relevant documents, presentations and intranet contents that helped answer certain questions more precisely.

Finally (5) the answers were analysed, summed up and compared. The conclusions drawn are presented in the following section.

7.3 Results

Following the questionnaire structure, we will first present a description of the ITG, ITRM, and ITC processes in the enterprises before examining in how far they are integrated. Then we will elaborate on the companies' integration of IT GRC with GRC on the corporate level.

7.3.1 IT governance, IT risk management, and IT compliance

The analysis of the three companies' ITG showed interesting results, as described in the following.

IT governance

TECHNOLOGY has a strongly formalised, requirements-oriented understanding of IT governance. Its global IT governance framework collects requirements from national and international standards (such as the ISO/IEC standard for IT security management (ISO/IEC 27001:2005), BS 25999 for business continuity management (BSI, 2006; BSI, 2007) and ISO 9001 for quality management (ISO, 2008)), laws and regulations (e.g. SOx, insider & tax regulations, data protection laws), and supporting best practices (COBIT (IT Governance Institute, 2007), ITIL (OGC, 2007), and the project management guide PMBOK (Project Management Institute, 2008)). The framework "assures an effective business/IT interface and enables careful coordination of all IT activities to drive standardisation of IT processes and the IT technology landscape." A three-step ITG process was designed to keep the governance framework up-do-date (Figure 24).

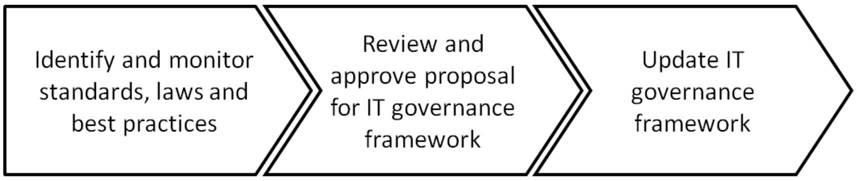

Identify and monitor standards, laws and best practices
Review and approve proposal for IT governance framework
Update IT governance framework

Figure 24: IT governance process of TECHNOLOGY

The process is triggered ad-hoc whenever changes in laws or standards or new risks emerge. Through the governance framework the whole IT organisation shares a common understanding of IT governance. ITG is further subdivided into IT security governance, governance of enterprise architecture and vendor management governance, all taken care of by different teams but aligned through the common framework.

HEALTHCARE defines "IT process governance" within IT service management (ITSM), established to "define and ensure process excellence in IT". Key objectives are the establishment of a harmonised IT service management framework, the implementation of service level agreement and best practices, the definition of key performance indicators and service level objectives, the fulfilment of regulatory requirements and increasing the efficiency of IT operations. A common understanding is shared by IT personnel through this definition as well as existing standard architectures and process definitions; the latter include COBIT and ITIL process that formalise many activities relevant for ITG, such as IT service management and auditing. An ITG function is defined on the group and divisional level. An ITG team takes care of incident management, change management and other ITG topics. HEALTHCARE currently discusses if the divisional and group-level functions should be merged.

ENERGY focuses on three deliverables for ITG: the maturity of services provided, business partner satisfaction, and project management effectiveness. The company uses governance to "address the right behaviour to achieve corporate goals". A triangle of the CIO representing the group's IT interests, the internal IT supplier of IT services and projects, and business operations defining the IT demand ensures alignment and the contribution to business value. The CIO is accountable for ITG, as he/she guides and governs IT activities and establishes processes, strategic principles and standards for IT projects, budgeting, operations and the IT architecture. The CIO also is responsible for IT sourcing, large strategic IT projects and IT trends monitoring and escalation. The ITG description further assigns accountability, responsibility and support tasks for project approvals, IT standards, audit guidelines, IT security, planning, budgeting and more to the CIO, the business unit IT leads and division IT leads. Lastly the involvement of various committees in IT is defined in the IT governance codex. Figure 25 highlights the building blocks of ENERGY's IT governance.

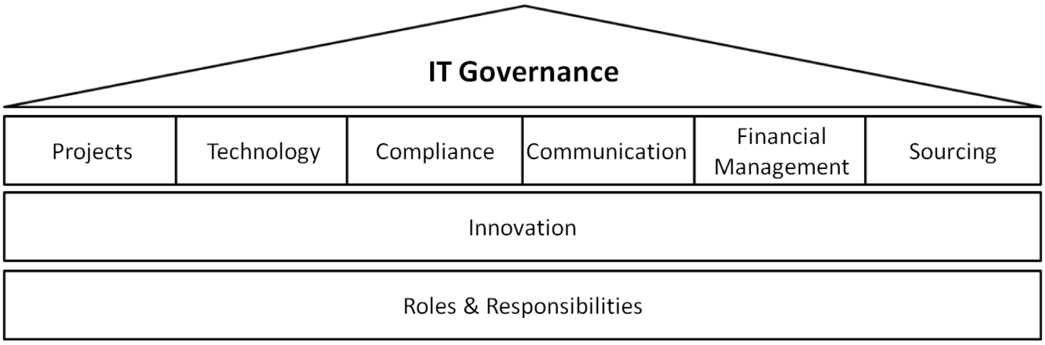


Figure 25: ENERGY's IT governance buildings blocks

In summary the three companies have different perspectives on IT governance: from a strongly formalised standards-oriented process view at TECHNOLOGY; over informal, implicit ITG embodied in the IT organisation's culture and processes; to a perspective where governance is clearly formalised, but focusing more on responsibilities and goals, centred on the CIO. None of the companies currently uses dedicated ITG software.

IT risk management

The presentation of the ITRM analysis is subdivided into the four levels of strategy, processes, people and technology.

IT risk management strategy

All three enterprises manifest the organisation-wide standardisation of ITRM in a central policy. At TECHNOLOGY and ENERGY, ITRM definitions follow the traditional view of risk as an event with negative impact; the modern perspective that includes upside risks, normally called opportunities (Moeller, 2007), is used by HEALTHCARE. The company sees the task of ITRM in the "establishment of a common view on and understanding of the risks and opportunities that HEALTHCARE IT faces [...]".

TECHNOLOGY uses the enterprise's general risk management definition also for IT: "Risk represents the danger posed by potential disruptions to TECHNOLOGY's ability to achieve its strategic, financial and operational objectives. […] Risk Management is the process by which TECHNOLOGY methodically addresses these risks."

ENERGY states: "The principal goal of ITRM is to protect the organisation and its ability to perform its mission. Therefore, the ITRM process will not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organisation." This means that ITRM is executed in cooperation with business lines (e.g. in order to calculate the business impact of risk events), and that the correct execution of ITRM is evaluated in audits.

IT risk management processes

According to their ITRM policies the companies' risk management processes are largely congruent, as Table 9 shows.

Table 9: High-level IT risk management processes of participants

TECHNOLOGY	HEALTHCARE	ENERGY
(Risk planning on corporate level)	Define risk objectives Risk information input	Establish context
Perform risk assessment	Risk identification	Risk identification
	Risk analysis	Risk estimation
	Risk evaluation	Risk evaluation
Perform risk assessment validation		
Perform risk response and monitoring	Risk treatment	Measure identification
		Measure planning
		Decision about risk treatment
		Approval by IS organisation
		Measure selection and implementation / risk acceptance
	Risk monitoring	
		Review
	Risk information and communication	

Minor differences are the validation steps that TECHNOLOGY implemented after risk assessment and that ENERGY runs for risk treatment. HEALTHCARE validates aggregated risks on the group level (the process list in Table 9 is used on the divisional level). ENERGY's review process highlights changes in the risk situation. HEALTHCARE's information and communication activities are also carried out by the other two companies, but they are not explicitly defined in their policies.

ENERGY describes three different process frameworks in its ITRM standard. At first it sets out a five-step process that includes two planning processes (setting a strategic target value for remaining risk, and developing strategies and policies to obtain the target), following the recommendation of ISO/IEC 27001 to design all information security management system processes as a Plan-Do-Check-Act cycle (Deming, 1982). However, this high-level description is not broken down into detail. Instead ENERGY outlines a super-ordinate ITRM process to enable continuous improvement. That process includes the definition of policies, business impact analysis, identification of IT assets and risk assessment, the identification of gaps between policy target values and actual values, and the checking and implementation of necessary measures. Lastly ENERGY describes a “key process” in detail that is aligned with the ISO/IEC 27005 standard for information security risk management. The steps of this process were included in Table 9, as they are the core of IT risk management within ENERGY.

HEALTHCARE uses three modified versions of the COSO Enterprise Risk Management cube (Figure 3) for its ITRM processes. The risk objectives dimension was replaced by risk areas (e.g. security, IT quality & compliance, operations). For the three different versions, the organizational hierarchy was in two cases substituted through IT systems and processes. Thus perspectives for systems, processes and legal entities are created.

A notable difference in the three companies’ ITRM is their risk assessment procedure. TECHNOLOGY only classifies risk using five rough ranges of financial impact and probability. HEALTHCARE calculates the impact of each risk more precisely, but also using ranges. ENERGY follows the methodology of a software product called “CRISAM” for implementation of ITRM; CRISAM does not use probabilities at all. Instead it relies on the comparison of actual impacts with target values.

IT risk management people

Various people are taking part in ITRM efforts in the companies examined. The setup is similar in all cases. At TECHNOLOGY our interviewee is responsible for the correct execution of ITRM activities. His boss is accountable. Risk owners lead the process execution for their respective risks. For HEALTHCARE the team of our interviewee manages IT risks; system owners carry out the risk assessments of their systems. At ENERGY, the CISO also leads ITRM. Risk owners, process owners and area managers support the business impact evaluation.

IT risk management technology

TECHNOLOGY uses a giant spreadsheet generated through a Microsoft Access database in which assets, control objectives, risks and controls are stored and tracked. HEALTHCARE also uses Access supported by a balanced scorecard showing existing and upcoming risks. The company plans to install a new ITRM solution soon. ENERGY has deployed the ITRM software “CRISAM”, which was attributed a large degree of completeness, reporting and compliance support by research (Zarakowitis, 2009).

IT compliance

TECHNOLOGY sees IT compliance as part of IT security. SOx compliance dominates, but other standards from the ITG framework are also certified against. The main compliance process for SOx consists of four phases: control documentation, control design assessment, control effectiveness testing, and corporate sign-off. SOx compliance is checked twice a year. ISO 9001, ISO/IEC 27000, and BS 25999 compliance are checked yearly. Audits are coordinated by means of an audit map. The main people involved in ITC are the IT security team of our interviewee and operational IT managers. Responsibility is in the hands of the interviewee, while his boss is held accountable. TECHNOLOGY has 90 automated IT controls in place that are managed through a deprecated version of a tool for automated IT controls. The giant spreadsheet based on the Access database that is used in ITRM is also used for ITC, as it holds mappings of risks to controls, regulations to controls and control status tracking.

The interviewee of HEALTHCARE is responsible and accountable for all ITC activities. For compliance assessments, IT topics (general topics, SAP, the non-SAP CRM system etc.) are subdivided into compliance topics (user equipment, education/training, IT security, change management, infrastructure, support…) and linked to “reasons” (e.g. external policies and laws) and controls. Once a year, an assessment sheet is sent to all sites, including target levels for control fulfilment, control weights, and an applicability column. If applicable, sites have to rate their maturity level (compliant, planned, in process or not compliant). The team of our interviewee then compares the sheet to the results of the last evaluation. The outcome and some other factors influence the decision if an audit is carried out. Audits are planned once a year; there are 14 audit types (e.g. site audit, ITG audit, IT service management audit) carried out at different intervals. An Access database saves all audit actions. Reminder functionality helps track and complete audit activities. The database and the spreadsheets sent to the sites are about to be superseded by a standard software audit tool allowing for direct data input. The tool supports audit planning and field work. It automates compliance tracking, and it will push information and action items to relevant users in the company’s portal.

ENERGY does not have a defined stand-alone ITC process, as ITC activities are integrated with ITRM (see below). These integrated activities evolve around the ISO/IEC 27000 row standards, recommendations of the Business Continuity Institute and the Statement on Auditing Standards 70 (AICPA, 1992). The CIO office constantly carries out IT audits. Software from Tripwire supports compliance management, while applications of several other vendors ensure prevention, monitoring and detection of compliance. SAP Access Control manages access and authorisation controls.

On top of the ITC activities already described, all companies have internal corporate audit teams that carry out additional audits independently, reporting directly to the board.

Summary

Aggregating the multi-faceted characteristics of the three IT GRC disciplines is difficult. We suggest a basic categorisation along two dimensions. Formalisation refers to the formal definition of strategies, processes and organisational roles. Process automation reaches from the mere existence of defined processes to support through appropriate software that automates processes as good as possible.

It is generally observable that process automation has only been leveraged strongly in risk management. ITC is highly formalised. Apart from the ITC integration with ITRM at ENERGY, ITRM and ITC are very similar in the companies reviewed. Only the ITG approaches differ strongly.

7.3.2 Integration of IT GRC

Now being aware of the participants' basic setup of the three IT GRC disciplines, we will describe their integration.

IT GRC strategy

First we inquired about the use of the acronym GRC. TECHNOLOGY has established the term to describe integrated activities on a corporate level. It is the only company that has established a corporate GRC function. Within IT, however, the acronym "SQRC" for "Security, Quality, Risk & Compliance" is more common. HEALTHCARE in accordance with its lack of a formally defined governance function talks of an "IRC" approach – "Integrated Risk & Compliance". In the long term an extension of integration activities including governance and thus installing "GRC" is planned. When ENERGY mentions GRC it does not refer to an integrated approach, but to GRC software, especially having in mind the GRC portfolio of software vendor SAP. In order to avoid confusion we will still use the term "GRC" for all companies in the meaning of our definition from chapter 4.

The concepts for IT GRC integration activities were all developed in-house. External frameworks for GRC or IT GRC were not used. IT GRC integration efforts were mainly pushed by the head of global IT risk management, compliance & audit of HEALTHCARE and the CISO of ENERGY, respectively, because they saw room for improvement in IT GRC activities. TECHNOLOGY's integration efforts were triggered by an external cause, as the challenge of complying with the Sarbanes-Oxley Act could be responded to more efficiently after a standardisation of IT processes. The strong interest in GRC integration that is observable in the three companies is reflected in their integration efforts described in the following.

IT GRC process integration

The relation between IT governance and the two other disciplines is two-fold (Racz, Weippl, & Seufert, 2010b). ITG governs ITRM and ITC while they in return support IT governance (e.g. through provision of risk data and through the assurance that governance policies are respected). The two-fold relation can be observed in the examined companies. On the process level participants integrate ITG, ITRM, and ITC in various ways.

Within TECHNOLOGY changes in the risk and compliance environment, such as the emergence of new material risks or new regulations, trigger an update of the ITG framework. The framework influences ITRM and ITC as it defines the standards that have to be adhered to. Risk and compliance further interact through the inclusion of the risk of non-compliance in ITRM. Moreover for certain system audits risk-based approaches relying on risk management data are used, helping to prioritise which systems and which applications within these systems should be the focus of auditors.

HEALTHCARE's integration activities mostly focus on risk and compliance. Only little informal integration of ITG with ITRM and ITC management is observable, as governance is acknowledged as the "top of the GRC pyramid". For example audits of IT security are basically governance audits, even though the word is not used. ITRM identifies compliance gaps that influence standards and processes that may be attributed to governance. However, ITG has yet to be formalised before integration possibilities can really be leveraged in a systematic manner at HEALTHCARE. The risk and compliance integration on the other hand is already advanced due to a first integration project that was ongoing at the time of the interview. In general HEALTHCARE sees risk management as the core activity of GRC. ITC processes are carried out in conformance with the leading ITRM process. Risk identification corresponds to non-compliance identification; risk analysis to non-compliance analysis and audits; evaluations of risks and non-compliance follow the same rules; and risk treatment and risk monitoring are applied to compliance issues as well. The integrated risk and compliance management is commonly (not separately for each purpose) supported through ticket systems, hotlines for whistle blowing, methods like impact analysis and fishbone diagrams, for instance. ITRM and ITC activities are further integrated through the frequent execution of risk-based audits and through the assessment of risks of non-compliance, as "IT quality and compliance" is one of the risk areas in the adapted COSO model of HEALTHCARE.

ENERGY also completely integrates ITC with ITRM and has done so since the first introduction of a dedicated ITRM process two years ago. A continuous improvement process is in place to enhance integration. ITC at ENERGY is not a separate process, but compliance issues are addressed through risk management. The priority of risks defines the priority of control measures within compliance. ENERGY does not include the risk of non-compliance as a risk category. Instead that risk is taken into account indirectly through lowered quality levels in the case of non-compliance, thus raising other risks. ITG at ENERGY enters the picture through audits that examine if the CISO fulfils his/her function. That way the governing function over ITRM and ITC, which belong to the CISO's responsibility area, is met to a certain extent. Compliance is one of the building blocks of ITG. Risk management data is used in governance decisions.

IT GRC people

Integration of IT GRC on the organisational level is far advanced in all three organisations. Responsibility for ITRM and ITC is already centralised in the hands of the interview partners. Their teams also support them in the global enforcement of IT GRC activities. System owners or site managers account at the same time for the execution of ITRM and ITC processes in their areas of responsibility. ITG is less tangible in the three companies. Eventually the CIO is always responsible for IT governance. However the actual execution of ITG processes is spread or not transparent; TECHNOLOGY has three ITG teams taking care of different governance facets (see above); HEALTHCARE has ITG functions on the group and divisional level; and ENERGY distributes ITG responsibilities within the CIO office. All three companies assure that (explicit or implicit) ITG requirements are met through the involvement of our interview partners in important projects that could affect ITG.

IT GRC technology

As explained in chapter 5, GRC technology can enable the integration of GRC data and of front-ends. It can also harmonise reporting through integrated GRC reports, and it can be integrated with enterprise resource planning software.

The current IT solution at TECHNOLOGY can be optimised. The giant Access database enables a holistic view on main IT GRC management. Consistency is ensured through a walkthrough with the different stakeholders and is maintained by the IT Risk Management team. However this manual process and the gathering of information via email are very tedious. Our interview partner would like to upgrade his software solution to the latest release of SAP GRC risk management. As of now, operational risk management software is used on the corporate level for strategic risks and to enter high-level IT risks, but that software is not used for all operational ITRM activities for several reasons; for instance, for specific ITRM data extra fields would be required to ensure correct status reporting about potential corrective and preventive actions. The software for internal controls has insufficient reporting capabilities. Moreover it cannot be integrated with the Access database; for example, automatic updates of the control status are not possible.

HEALTHCARE is in the process of replacing its current solution involving Microsoft Access, Excel and emails with an integrated IT risk and compliance solution. The results of risk and compliance assessments will be entered directly into the application by system owners, site managers and other relevant personnel. The mapping of risks to controls, regulations or assets as done today will still be enabled by the software. Reporting capabilities are integrated. An integrated multi-regulatory compliance framework will help reduce compliance complexity and it will prevent duplicate efforts.

As mentioned before ENERGY has deployed SAP-BO Access Control, but this is more of an operational tool and thus it is not in the scope of IT GRC management. The CRISAM software has helped standardise ITRM and it supports compliance checks, but the additional automated control and monitoring solutions are disconnected. In summary, only HEALTHCARE is soon going to have software in place that covers more than one discipline of IT GRC.

Integration benefits

TECHNOLOGY says that the integrated GRC approach brings about big advantages as it drives the global standardisation of processes using the pressure of regulations. Today maintenance efforts for GRC-related topics such as access management are by far lower than they used to be. The GR processes themselves are also more efficient than in the past. At HEALTHCARE audits can be targeted in a better way through the integration of ITRM with ITC. Results are better as more material risks can be identified. Increased transparency enables an improved selection of prevention efforts. IT processes are improved because inefficiencies can be recognised better through a comprehensive overview of all risks. Many policies were made redundant because through process adaptations they are now automatically respected. Management always receives a fact-based overview of which topics should be treated with priority. ENERGY states that the IT GRC integration helps prioritise actions concerning risks and controls. It increases transparency in processes and service and thus offers the possibility for improvements. IT GRC processes are now more effective and efficient than in the past. However, this is mainly because ITRM was established for the first time. A comparison with times where ITRM was executed separately is therefore not possible.

Summary

The integration on the strategic, process and organisational levels seems to be more advanced than on the technology level, as the overview in Table 10 shows.

Table 10: Comparison of IT GRC integration

	TECHNOLOGY	HEALTHCARE	ENERGY
Strategy			
GRC understanding	concept; corporate GRC but SQRC in IT	concept; IRC without governance	software; SAP GRC portfolio
Integration mainly promoted by	Sarbanes-Oxley Act	Head of global IT compliance	CISO
Process			
Risk of non-compliance used	yes	yes	indirectly considered
IT integrated with ITRM	yes, partially	yes	yes
ITG supported by ITRM & ITC	yes	hardly	yes
ITG oversees ITRM & ITC	yes	no	yes
Risk-based auditing used	little	heavily	intermediate
People			
Responsibility for ITRM & ITC	centralised	centralised	centralised
ITG responsibility	spread among ITG teams	separate on group and divisional level	centralised in CIO office
Technology			
ITG (not ITSM)	no dedicated application	no dedicated application	no dedicated application
IT risk and compliance management	Access database maps regulations, risks & controls	Access database, but integrated software is being implemented	controls mapped in CRISAM application
ITC data automatically updates ITRM	no	no	no
GRC repository for all GRC data	no	no	no

Judging the observed status quo along the formalisation and process automation dimensions, we can state that ENERGY and TECHNOLOGY could improve process automation through the use of integrated GRC software. TECHNOLOGY formalises the interaction of ITG, ITRM, and ITC most – at least in the restricted focus of its ITG framework. Process automation will be highest at HEALTHCARE one the ongoing integration project is finished.

7.3.3 IT GRC integration with corporate GRC

The concept of integrated GRC suggests the integration of all GRC activities of an organisation – not only those of the IT department. In how far is IT GRC integrated with corporate-level GRC? TECHNOLOGY sticks out at first sight from an organisational point of view as it is the only company that has established a corporate, global GRC function. That function aligns GRC activities enterprise-wide, leading and helping business lines and supporting functions such as IT adhere to GRC requirements.

Still, looking at the relation of corporate and IT the corporate governance codex of TECHNOLOGY was not used in the definition of the ITG framework. ITG at HEALTHCARE was developed in accordance with the corporate governance requirements, but does not refer to it in its key objectives. At ENERGY the ITG model was developed while the IT strategies of the different business units were merged and standardised. Corporate governance at ENERGY did influence this process, and the role of the CIO in corporate governance connects it with ITG.

The relation of corporate risk management to ITRM is similar for HEALTHCARE and TECHNOLOGY, but differs at ENERGY. All three use software applications for strategic risk management. A small number of aggregated risks from ITRM are entered into the corporate software. At ENERGY, for instance, these are risks with a material impact on earnings before interest and taxes (EBIT); facts and figures are translated into the ERM ontology to guarantee comparability with other ERM data. Personnel responsible for ERM rely on the data input from IT. The risk management process definitions in the companies differ. At ENERGY different processes (with similar activities) are used to carry out ITRM and ERM. TECHNOLOGY and HEALTHCARE, in contrast, use a single policy for all types of risk including IT risk. This is the approach suggested in chapter 8. HEALTHCARE has already harmonised corporate and ITRM processes, and now discusses if the execution of the risk management processes should also be synchronised. That way, group-level risks would be broken down to lower levels, and other risks on these lower levels would be identified in the same breath.

ITC is connected to corporate compliance in several ways. Only a part of the myriad of GRC requirements is directed towards IT operations. Thus processes have to be examined end-to-end. The SOx process at TECHNOLOGY, for example, is led by the corporate GRC function; the IT organisation is aligned with and engaged in the corporate SOx process. At HEALTHCARE, internal controls for financial reporting are audited by IT and by the finance department. Due to its role as an enabler of business, IT is often just one of several parties involved in a compliance procedure. Moreover companies have corporate internal audit teams that audit all parts of the enterprise, including IT. That way and through sign-offs across hierarchy levels organisational integration of compliance is established.

Lastly integration aspects exist on the technology level. Automated controls provided by IT not only monitor IT-specific processes, but also business operations supported by IT through the application of business rules. TECHNOLOGY’s automated control application is used in the SOx process, both by corporate GRC and by IT. But compliance technology integration at the three companies examined hardly surpasses IT controls. For example, TECHNOLOGY uses a central company-wide tool combining all strategic and operative risks throughout all business functions including the IT control side; but for the mapping of assets to risks and controls, however, it had to deploy a separate Access database. ENERGY and HEALTHCARE do not have a central tool in place that stores all compliance-relevant data (standards, audit results, logs, control information...). HEALTHCARE is currently pondering the introduction of such a tool.

Translating these results into the previously used dimensions of formalisation and process automation, all companies range on the low side of process automation (with a slight edge for TECHNOLOGY), as the use of common technologies is hardly leveraged. Formalisation is medium at ENERGY and HEALTHCARE and slightly lower at TECHNOLOGY due to its lack of an ITG and corporate governance connection.

7.3.4 Discussion

Chapter 7 contributes to information systems research in several ways. The status quo of IT GRC activities in three large enterprises is presented. Integration efforts concerning the three disciplines and integration of IT GRC with corporate-level GRC are identified. The result helps understand integration possibilities and different approaches to IT GRC and its three sub-disciplines. A largely undiscovered potential for further integration seems to lie in process automation through application of integrated software solutions. Formalisation is generally high but it varies, especially with respect to ITG. The exemplary IT GRC integration in business practice can later be compared to reference models from theory in order to identify applicability and shortcomings. New theory can build on the results to increase the likelihood of its relevance.

Naturally some points of critique can be directed to the methodology applied. Firstly, the examination of three companies is not representative. But at least it gives impressions of IT GRC in three different industries. Considering the variety found in the companies’ IT

GRC processes, the findings are a satisfying result for an explorative study. Secondly, it is hard to judge in how far the interviewees' answers actually reflect the reality in their companies. For instance, are policies really adhered to? Interviewee's might not exactly know the answer, or they might tend to draw a polished picture of their areas of responsibility. A deeper analysis through witnessing processes at execution or through interviews of more employees could have avoided this deficit. However, we assumed that participants would not agree to such a proceeding. Thirdly, in hindsight we would have liked to know more about the GRC technology used. Looking at spreadsheets such as the risk-controls mapping turned out to be very helpful in understanding the contents of certain processes. However, software applications are too complex to be quickly grasped, and in the interviews there was no time for demonstration. We thus had to rely on vendors' tool descriptions. A more detailed question catalogue about software functionality and its use could have helped gain more insights.

7.3.5 Conclusion

Chapter 7 shows that IT GRC integration efforts have been undertaken in large enterprises in various ways. There is an agreement that synergies exist and that they need to be leveraged. Even though many commonalities can be observed there is no common approach to IT GRC integration. In chapter 8 we will take up the notion observed in two of the companies that did not use separate IT risk management frameworks. In chapter 9 we will then provide a common approach to IT GRC integration through suggestion of an integrated process model.

Chapter 8. Questioning the need for separate IT risk management frameworks

The alignment of IT with business objectives is an important part of contemporary IT management. Ever since the creation of the term “enterprise risk management” the search for integration possibilities within ERM has been ongoing. However as of today different frameworks are used for the management of business risks and IT risks. The emergence of horizontal integration (across disciplines and across departments) and vertical integration (across the organisational hierarchy and across process levels) has helped realise that formerly separate approaches are often redundant (Mitchell, 2007b), which provokes to establish the hypothesis that a separate management of IT risks might not be justified.

Reference models for IT GRC should enable integration of GRC on the enterprise level with IT GRC to ensure reciprocal support and alignment (Figure 15). The literature review in chapter 4 showed that enterprise risk management is a key methodology within GRC. Thus as a first preparation for creation of a process model for IT GRC, we want to find out if ERM processes could be used for IT risks as well, as this would facilitate the integration of IT GRC and overall GRC.

8.1 ERM and ITRM

A quick scan of the ACM, SpringerLink and EmeraldInsight databases shows that in research as of today enterprise risk management and IT risk management (ITRM) have hardly ever crossed paths. Only Foley uses ERM processes to manage security risks (Foley, 2009).

In practice enterprise risk management and IT risk management are also treated as separate topics. With ISO 31000:2009 (2009) (superseding AS/NZS 4360:2004 (2004)) and ISO/IEC 27005:2008 (2008) the International Organisation for Standardization treats ERM and information security risk management (including ITRM) in two distinct standards. ISO 31000 does not even reference ISO/IEC 27005. The alignment of IT with business in practice is mainly done through the IT governance and management frameworks COBIT (Control Objectives for Information and related Technology (IT Governance Institute, 2007)) and ITIL (IT Infrastructure Library (OGC, 2007)). These frameworks suggest enabling alignment through deriving IT goals from business goals.

We can conclude that while the connection of IT risks with business objectives is enforced at present, the merger of ITRM with ERM on a process level is hardly looked at. The frame of reference for research of integrated GRC presented in chapter 4 recommends identifying integration possibilities on the strategic, process, organisational and technology level. Strategically, through the alignment of IT goals with business goals, the integration is already ongoing. We suggest to take the next step and to review potential synergies of ERM and ITRM on the process level. That way we can decide later on in how far ERM should be respected or even included in a process model for IT GRC management. Following the claim of ERM to cover all risks of an enterprise, ITRM should either be completely covered by ERM and therefore be redundant; or it might enhance the broader ERM through detailed consideration of IT specifics in the risk management process.

8.2 Research methodology

In order to evaluate our hypothesis we decided to carry out an exemplary comparison of an ERM framework with an ITRM framework. Of course a comparison of two frameworks is not representative, but we selected widely-used frameworks (see below) that therefore suffice to provide an indication about the hypotheses' validity. The methodology applied consists of four steps (Figure 26). First, we selected a framework for ERM and one for ITRM. Second, the frameworks' commonalities were identified. Third, we analysed the references of the ERM framework to IT risk and vice versa. Finally we discussed and summed up the results.

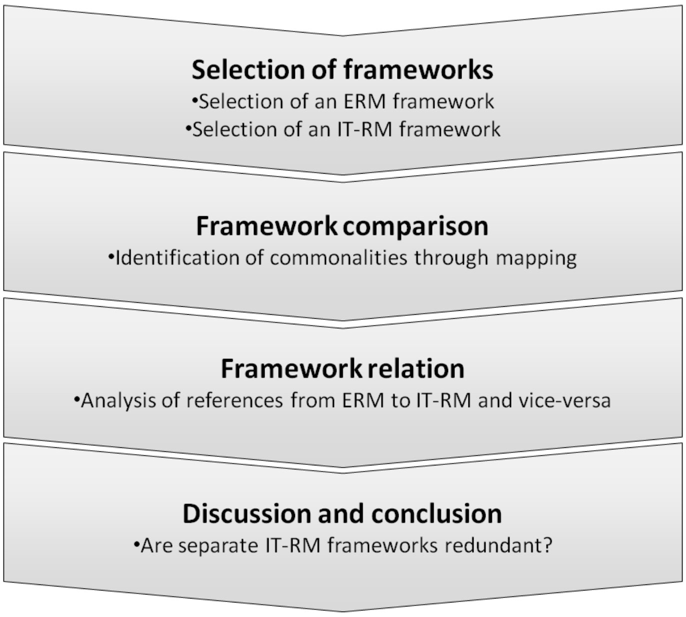

Selection of frameworks
•Selection of an ERM framework
•Selection of an IT-RM framework
Framework comparison
•Identification of commonalities through mapping
Framework relation
•Analysis of references from ERM to IT-RM and vice-versa
Discussion and conclusion
•Are separate IT-RM frameworks redundant?

Figure 26: Research methodology in chapter 8

In the selection process for an ERM framework we considered ISO 31000:2009 and COSO ERM, two well-known standards for ERM. Their process models are very similar. On a high level they only differ in their wording. “Establishing the context” in the ISO standard corresponds to the “internal environment” of COSO ERM, “risk evaluation” and “risk treatment” equal “risk response” and “control activities”, etc. Eventually we opted for COSO ERM, as it is the successor of the widely implemented COSO framework for internal control (COSO, 1992), a de-facto standard explicitly acknowledged in the US Public Company Accounting Oversight Board Auditing Standard No. 5 for financial reporting (Public Company Accounting Oversight Board, 2007). The standard is referenced in the Sarbanes Oxley Act of 2002, which of all regulations passed in the new millennium probably has the strongest impact on risk management and internal control systems.

For IT risk management we chose the ISACA Risk IT Framework because it complements COBIT, which is arguably the most appropriate control and governance framework used by many organisations world-wide to ensure alignment of IT and business goals (Ridley, Young, & Carroll, 2004). The framework’s importance is expected to grow since the new COBIT version 5, which is currently in development, plans to consolidate and integrate the Risk IT framework (ISACA, 2010). ISO/IEC 27005:2008 was also considered. As it includes all aspects of information security (including non-IT aspects), its scope surpasses the ISACA framework, which is limited to information technology. In our opinion Risk IT is more detailed, and it draws out the specifics of ITRM more clearly.

The identification of the frameworks’ commonalities in the second phase of our research was done through a mapping of the described processes of ISACA Risk IT to those of COSO ERM. The documentation of COSO ERM proved to be a hurdle. On the highest level the framework consists of seven processes and the “internal environment” component. Unfortunately the processes are not broken down. Instead COSO just names the basic sub-components, such as “risk tolerance” or “inherent and residual risk”. In order to map the processes of ISACA Risk IT, we had to go through the complete description of the COSO components to find if the same processes were included.

The qualitative analysis of references from ERM to ITRM and vice versa in the third research step was followed by a descriptive discussion and summary of the insights gained in the research process.

8.3 Results

The results of the framework comparison are described in the following.

8.3.1 Mapping of ISACA Risk IT to COSO ERM

This comparison of risk management frameworks is based on the assumption that "risk" in ERM has the same characteristics as "risk" in ITRM. In COSO ERM, risk is "the possibility that an event will occur and adversely affect the achievement of objectives; events with a potentially positive impact may offset negative impacts or they may represent opportunities" (COSO, 2004). Throughout the framework "risk" then also refers to upside risk (opportunities). According to ISACA Risk-IT, IT risk is "a component of the overall risk universe of the enterprise [...]. IT risk is business risk [...]. It consists of IT-related events and conditions that could potentially impact the business" (ISACA, 2009a). The two frameworks consequently share a common understanding of the term "risk".

ISACA Risk-IT consists of the three processes risk governance, risk evaluation, and risk response on level one, with three sub-processes each on level two. Level three comprises 43 processes. COSO ERM on the other hand describes 8 high level processes with 41 sub-components. While the ERM framework is more profound on the internal environment component and on risk aggregation, Risk IT is more specific when it comes to IT specific and communication processes. Still, all but seven of the ITRM processes can easily be mapped to COSO components (seeAppendix F – Mapping of ISACA Risk IT to COSO ERM).

Two of the exceptions deal with ERM integration: "RG2.2: Co-ordinate IT risk strategy and business risk strategy", and "RG2.3: Adapt IT risk practices to enterprise risk practices". They treat the alignment of IT and business risks on a strategic and on a process level; we will analyse them later on in the section about ERM references in the ITRM framework. Three other processes that could not be mapped belong to the process group "RG3: Make risk-aware business decisions": "RG3.1: Gain management buy-in for the IT risk analysis approach", "RG3.2: Approve IT risk analysis", and "RG3.5: Prioritise IT risk response activities". Management buy-in for risk analysis approaches and their approval is not explicitly mentioned in COSO ERM, but it could seamlessly be integrated with the "internal environment" component. Prioritisation of response activities is probably so self-evident that COSO ERM does not highlight it; in COSO the prioritisation could be part of risk response. Furthermore the processes "RE2.4: Perform a peer review of IT risk analysis" and "RE3.3: Understand IT capabilities" do not exist in COSO ERM. Peer reviews are a control mechanism that can be seamlessly included in the ERM process. Understanding IT capabilities is an extremely general "process" that is a prerequisite for any kind of IT activity, therefore suitable to be added to the "internal environment" component of COSO ERM.

As we can see, drawing from the standards IT risks may be treated like any other risk, as the ITRM framework is completely absorbed in COSO ERM, apart from the ERM integration specifics (RG2.2, RG2.3) analysed below. The ISACA framework does not explain why an IT-specific risk management framework in the hierarchical relationship to ERM would be necessary. It even disposes of the distinction by stating that “IT risk is business risk”, consisting of “IT-related events that could potentially impact the business” (ISACA, 2009a). Thus the need for separate IT risk frameworks is questionable. It seems to be owed more to the complexity of IT, to habits and to the separation of IT and business responsibilities in modern organisations than to a real business reason.

8.3.2 References of COSO ERM to ISACA Risk IT and vice versa

In fact the Risk IT Framework (RG1.1) recommends taking a top-down, end-to-end look at business services and processes and identifying the major points of IT support. However it does little to support this advice. The relation to ERM is explicitly treated in the framework. “Integrate with ERM” as a sub-process of “risk governance” states as goal to integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level. Five key activities shall help achieve this goal. Three of them are governance processes indispensable for any risk domain: establishing and maintaining accountability for ITRM (RG2.1), providing adequate resources for ITRM (RG2.4) and providing independent assurance over ITRM (RG2.5). RG2.1 involves business with IT risk through risk ownership and the ability to address IT risk issues. RG2.4 weighs investing resources for IT risks with investments in competing business risk issues, thus surpassing the IT risk domain and respecting all risk domains of ERM. RG2.5 actually is not ERM-specific at all.

Consequently we are left with the two other processes allegedly dealing with ERM integration that could not be mapped to COSO ERM before: “co-ordinate IT risk strategy and business risk strategy” (RG2.2) and “adapt IT risk practices to enterprise risk practices” (RG2.3). RG2.2 requires to “integrate any IT specifics into one enterprise approach” and to define the IT department’s role in operational risk management. Existing ERM principles and views of risk should be used wherever possible. How this integration works is not explained. RG2.3 demands that the business context for IT, and ERM expectations, activities and methods relevant to ITRM be understood. ITRM should be enhanced with useful ERM activities, ERM expectations should be met, and methods of other functions should be identified. The gaps between IT risk and ERM shall be closed – but the framework owes a clear explanation of how this could be done.

The COSO ERM framework on the other hand gives even less advice on ITRM. It is only high-level guidance as far as IT is concerned, but specifics of IT risk management may still be considered on lower process levels (Moeller, 2007). It mentions the importance of information systems controls due to the “widespread reliance on information systems” (COSO, 2004). General controls shall ensure the continued, proper operation of information systems, while application controls ensure completeness, accuracy and validity of information. General controls are further subdivided into controls for information technology management, information technology infrastructure, security management and software acquisition, development and maintenance. Apart from these control-related hints there is no detailed reference in COSO ERM to information technology. IT risks are not even mentioned. Thus the COSO ERM document remains on a very high level, not helping practitioners deal with IT risks in the ERM context.

8.4 Discussion

Drawing on the results we see the hypotheses that a separate framework for ITRM might not be necessary preliminarily affirmed. ISACA implies a hierarchical structure between ERM and ITRM, but our research rather suggests that the ITRM framework might inhibit the integration with ERM through introduction of a redundant framework into the process. Certainly the comparison of two frameworks is not sufficient to prove the hypothesis, but it is a hint that further efforts to confirm the assertion are worthwhile. Future research would have to provide real case study examples to prove the point.

In practice today ITRM is started within the IT organisation and it is aligned with business mainly through business objectives. ERM is a top-down approach, and ITRM is top-down within IT, but bottom-up on the enterprise level, as IT risks are analysed and subsequently linked to business objectives and quantifications from operational risk management. For example an IT risk manager might look at a database and identify the data therein, then find out which applications it is used in, next look at which business processes they support and, eventually, what the (financial) impact on these processes would be if the data lost its integrity, validity, privacy or availability (Rath & Sponholz, 2009). Historically the coexistence of ERM and ITRM can be explained because enterprise-wide approaches to risk have only emerged over the last decade (COSO ERM as the first ERM framework was only published in 2004). ITRM meanwhile has been around for much longer due to ever-present IT security and operational issues.

We argue that the more reasonable way to manage risks would be to follow a business process top-down to all its enabling resources, be they human or natural resources, technology or information. Starting at the process level, business would have to consult IT as part of the ERM exercise to deliver the IT resources linked to a specific process on the application, data and infrastructure level. Then the events and risks (e.g. data loss due to a virus) could be analysed hand-in-hand by business and IT. The main advantage of this end-to-end approach is that only relevant, value-creating business processes would be considered, and that they could be prioritised early-on.

8.5 Conclusion

The analysis of the COSO ERM and ISACA Risk IT frameworks has shown that the need for a separate ITRM framework indeed is questionable. The majority of ITRM processes match the ERM components; the few remaining processes can be integrated with ERM. Research should evaluate the possibility of creating an integrated approach to IT risks within enterprise risk management that makes the application of separate ITRM frameworks redundant. Such an approach could use ERM processes for ITRM. This finding will be taken into consideration in the following creation of a process model for IT GRC management (chapter 9).

Chapter 9. A process model for integrated IT GRC management

With the insights gained in the chapter 4 to 8 we are now ready to build a first process reference model for integrated IT GRC management. In chapter 4 we suggested a GRC definition and frame of reference that are applied. In chapter 5 we found out that in order to build software reference models, state-of-the-art GRC software should not be relied on. Instead, GRC processes have to be identified, as we will do now. Recommended action 1 in chapter 6 asked for identification of GRC potentials, which the model to be built is going to point out. Chapter 7 demonstrated different approaches to IT GRC processes as well as the lack of an integrated model. In chapter 8 we concluded that ERM processes should be used to carry out ITRM. Chapter 9 will incorporate these insights.

9.1 Existing GRC process models and frameworks

Even though they have been mentioned before, we will now look more closely at the existing five frameworks claiming to integrate governance, risk, and compliance, in order to highlight their shortcomings and the need for the integrated IT GRC management process model.

The Open Compliance and Ethics Group (OCEG) has developed the “GRC Capability Model”, an exhaustive model consisting of nine components (categories) and 29 sub-elements, for each of which core sub-practices are listed (OCEG, 2009). The OCEG model is certainly very useful for professionals who want to gain an understanding of all possible GRC activities. However it does not distinguish between operative and management processes. Furthermore, it does not explicitly point out where the integration of formerly distinct disciplines takes place. Sometimes the adopted integration can be guessed, but this is easy only in obvious cases, such as when compliance risks are mentioned in risk analysis. Moreover the model shows only few governance aspects in the GRC process. While the role of governance is explained in detail in the introductory sections, in the process model it only reappears in the sub-practice “analyse governance culture and management style.” The extent to which the model supports governance processes is not clarified. Lastly, due to its greenfield development approach the model does not explain how it relates to existing standards.

Mitchell, who was also engaged in the creation of the OCEG model, proposes a framework to drive “principled performance” (Mitchell, 2007b). According to this model, an enterprise tries to overcome obstacles and achieve its objectives while staying between mandated and voluntary boundaries. Mitchell lists ten areas that are part of GRC and that share a common meta-process: objective setting, boundary identification, risk assessment, proactive actions, detection and checking, response, evaluation, improvement, and communication. While delivering this notable insight, he does not go further and lay out in detail how these common processes could be shared across the ten areas to leverage synergies.

Sachar Paulus describes a “GRC reference architecture” (Paulus, 2009) consisting of four major phases: requirements modelling, status investigation, situation improvement, and crisis and incident management. While this model is concise and easy to understand, it contradicts the generally more common comprehensive understanding of GRC as it claims that certain processes, such as financial risk management, do not belong to GRC. Like the OCEG model, it does a poor job in drawing out where integration between the three disciplines is accomplished.

The framework provided by Frigo and Anderson (2009) lacks detail and arbitrarily mixes processes with organisational entities and objectives.

Tapscott (2006) describes an integrated approach to GRC based on four core values, but he does not translate this approach into a process model.

Finally, none of the five models elaborates explicitly on IT GRC. Their applicability to GRC for information technology can only be guessed. As the derivation of the models from existing standards, research, or best practices is also hardly visible, we conclude that a scientific process model for integrated IT GRC has yet to be created.

9.2 Research methodology

The methodology applied in this chapter consists of four stages.

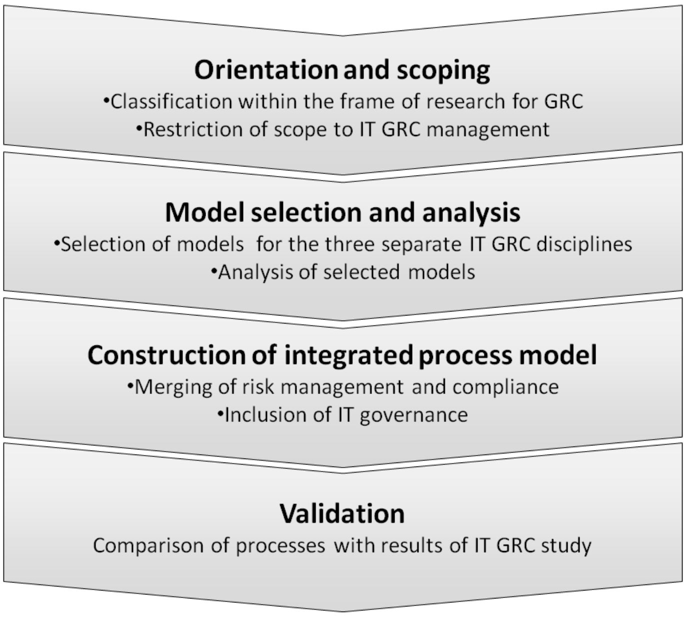

Orientation and scoping
•Classification within the frame of research for GRC
•Restriction of scope to IT GRC management
Model selection and analysis
•Selection of models for the three separate IT GRC disciplines
•Analysis of selected models
Construction of integrated process model
•Merging of risk management and compliance
•Inclusion of IT governance
Validation
Comparison of processes with results of IT GRC study

Figure 27: Research methodology in chapter 9

The complexity of the governance, risk and compliance domain mandated a clear classification of the elements of GRC to be considered in our research. Based on a previously developed GRC definition and frame of reference for GRC research, we restricted the scope to IT GRC management. Consequently we selected and analysed models for the three separate IT GRC disciplines – IT governance, IT risk management, and IT compliance. In the final stage of our research we merged the three selected high-level process frameworks into a single process model. First we explained how IT compliance can be integrated with risk management through consideration of the risk of non-compliance and the mapping of IT compliance processes to similar processes in risk management. Second we examined the relation of IT governance to IT risk management and IT compliance before merging the three disciplines in a single process model through identification of commonalities and mapping of overlapping or combinable processes. In the final stage of the research a rough validation was carried out through the comparison of the model with IT GRC processes in three multinational companies.

9.3 Towards a process model for integrated IT governance, risk and compliance management

In the following we describe the selected process models for IT governance, (IT) risk management, and IT compliance.

9.3.1 Orientation and scoping

For scoping and orientation within the GRC domain we built on the previously developed definition of GRC (chapter 4). We classified this research step within the frame of reference for research of integrated GRC. In this section we show possibilities for integrating the high-level processes of the three disciplines: IT governance, IT risk management, and IT compliance. The scope of operations managed and supported through GRC is therefore restricted to IT operations. The elements from the frame of reference's that are considered in this section are highlighted in grey.

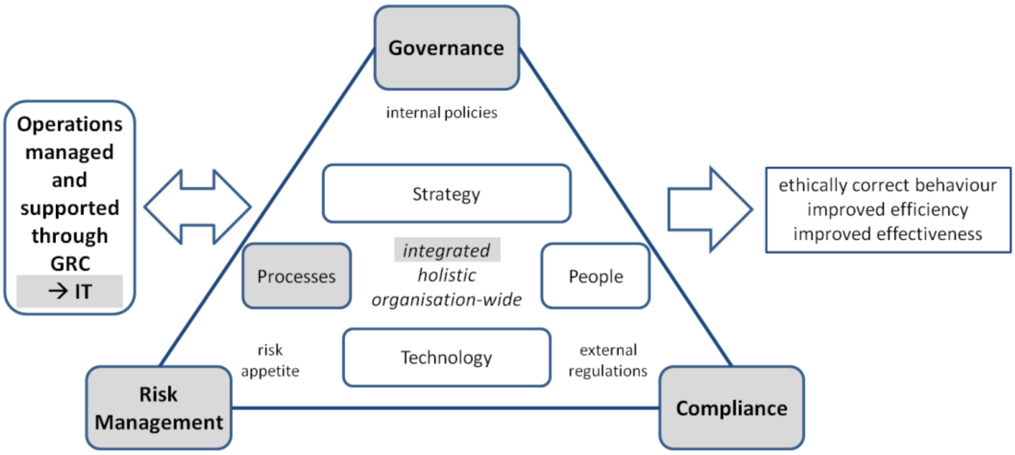


Figure 28: Elements in focus in the frame of reference for GRC research

As previously mentioned, IT GRC is seen as a subset of corporate GRC (Klotz & Dorn, 2008). The three IT GRC disciplines are subsets of their corporate counterparts as depicted in Figure 29.

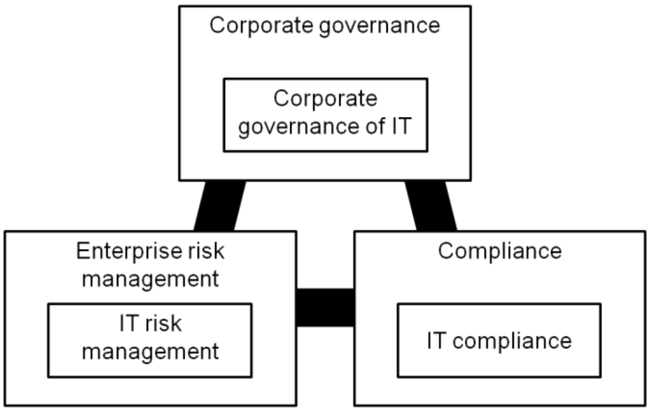


Figure 29: IT GRC as a subset of GRC

IT GRC processes were put into an enterprise process context following the new St. Gallen Management Model (Rüegg-Sturm, 2003) that distinguishes three process categories: management processes, business processes, and support processes. Risk management, information management, communication, and legal processes such as compliance management are classified as support processes. Governance processes, however, are considered management processes; since they govern the allocation of resources, they belong to the operative management process category of the St. Gallen model. Consequently an IT GRC process has to be able to

i. support management processes through the provision of information about IT risks and IT compliance aspects and through an IT governance framework that can be referred to when taking decisions; and
ii. help business processes and other support processes to be executed in an effective and efficient manner through consideration of IT risks, IT compliance aspects and through an IT governance framework.

To avoid getting lost in detail we further restricted the scope to the highest level of process descriptions provided in the frameworks we included. Such a management process may be executed on a regular or an ad-hoc basis. We do not want to focus on the operative details of IT GRC, such as how an incident is stored, but on the high-level processes that provide the support outlined above.

9.3.2 Model selection and analysis

After defining the scope we analysed a variety of standards and frameworks that describe the separate disciplines of IT governance, risk management, and compliance before selecting one for each discipline as a process foundation for our research.

IT governance

As pointed out in chapter 2, thus far no single theory adequately explains governance in full (McGinnis, Pumphrey, Trimmer, & Wiggins, 2004). Previous studies have focused primarily on structural mechanisms of IT governance while neglecting the process mechanisms (Ribbers, Peterson, & Parker, 2002). Lewis & Millar (2009) identified two schools of thought of IT governance – one focuses on decision making and accountability, while the other is primarily concerned with controls and risk management. Due to our focus on processes and the integration with risk management and compliance, we adopted the second perspective as used in the standard ISO/IEC 38500:2008 (2008) (for the definition see chapter 2).

We chose the process model of the ISO/IEC standard over the widely implemented frameworks COBIT (IT Governance Institute, 2007) and ITIL (OGC, 2007) because both of these frameworks go much further than governance through inclusion of specific practices and implementation advice for IT management, controls, and assurance. They include many aspects of risk management and compliance, which would make a clear analysis of GRC and its integration capabilities difficult. Therefore they are both more suitable for consideration at a later stage of GRC research when we are ready to examine the extent to which these models already include integrative aspects of the process model to be developed.

Governance is not a one-and-done process, but a system that comprises processes that may be executed whenever needed. The ISO/IEC standard recommends three process steps – evaluate, direct, and monitor – to be applied across six principles: responsibility, strategy, acquisition, performance, conformance, and human behaviour. The framework putting corporate governance in context with business processes is drawn out above in Figure 2. As mentioned there, Ohki et al. (2009) recommended adding "reporting to stakeholders" as a fourth process step, which we will now take into account.

IT risk management

Due to risk management's core function in GRC we assume that the selection of an enterprise risk management framework that does not focus on IT will facilitate integration with non-IT GRC in future research. Thus we decided to use the COSO ERM framework (COSO, 2004). This is the consequence of our finding in chapter 8 that separate ITRM frameworks might be redundant. ISO/IEC 27005:2008 (2008) was not adopted as it focuses on information security risk management. While ISO 31000:2009 (2009) (superseding AS/NZS 4360:2004 (2004)) for risk management uses different wording than COSO ERM for the main processes, it basically contains the same elements.

COSO ERM is high-level guidance as far as IT is concerned, but specifics of IT risk management may still be considered at lower process levels (Moeller, 2007). Another reason to build our research on COSO ERM is that it is an enhancement of the COSO framework for internal control (COSO, 1992). As mentioned above, this framework is a de-facto standard explicitly acknowledged by the US Public Company Accounting Oversight Board in its Auditing Standard No. 5 for financial reporting (Public Company Accounting Oversight Board, 2007), which is referenced in the Sarbanes Oxley Act of 2002. Therefore many companies are already using the predecessor framework of COSO ERM, also for internal controls over IT (Gupta, 2009).

The COSO cube in Figure 3 describes eight high-level processes (risk components) for risk management that are executed across the organisational hierarchy and that support the achievement of objectives in four categories. Just like governance, risk management processes are executed at varying frequencies. They might be carried out at fix time intervals, be event-driven (e.g. due to a new project or a major change in the organisation's environment) or even be perpetual through continuous monitoring and adaptation.

IT compliance

For IT compliance we selected the process model suggested by Rath and Sponholz (2009) because this generic model can also be applied to non-IT compliance. The model divides the general process of IT compliance into four sub-processes depicted in Figure 4: requirements analysis, deviation analysis, deficiency management, and reporting/documentation.

Requirements analysis comprises the identification of regulatory, legal, contractual, and other obligations that affect the organisation’s IT operations. Internal policies, such as best practices for software engineering or security guidelines, can also be included. Companies often build regulatory databases or use services such as the Unified Compliance Framework (UCF) to comprehensively collect their IT compliance requirements. The requirements build the foundation of a company’s internal control system as far as IT is concerned.

Once the requirements have been identified, adherence is examined for instance through internal and external audits, self assessments, and security checks. The frequency of these examinations depends on external requirements and on the impact of potential deviations. Whereas a yearly examination will be sufficient in many cases, continuous monitoring may be recommendable in other cases.

The results of the deviation analysis define the requirements for deficiency management. At this stage existing deficiencies are eliminated through improvement of existing controls, creation of new controls, or through a makeover of parts of the control system.

All actions taken in the first three stages are documented, and relevant information is reported to internal and external stakeholders. The information reported may include incidents, sign-off status, dashboards monitoring the status of compliance activities, or key risk indicators, for instance.

9.3.3 Construction of a process model for integrated IT GRC management

The main commonality of the process models for separate governance, risk management, and compliance management is that they all follow a scheme that is similar to methodologies such as the PDCA cycle (Deming, 1982) and Six Sigma (Tennant, 2001). After a phase of target setting and requirements analysis action plans are defined and executed. Meanwhile monitoring ensures the proper execution of these actions and reporting informs stakeholders about the performance of the process. Improvements are implemented gradually. Now the question is: how can these process steps be defined so that governance, risk management and compliance are included comprehensively?

The most obvious way is to start from the most detailed process model we reviewed – COSO ERM – and see if it could also include governance and compliance processes. Starting from risk management also makes sense because it enables applying a risk-based perspective to governance and compliance, allowing for a quantifiable frame for decisions. We will first merge compliance management with risk management before adding governance.

Merging risk and compliance management

The COSO framework states that "enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting, and compliance with laws and regulations" (COSO, 2004). Hence COSO ERM already considers compliance with external laws and regulations and integrates it with its objectives categories for compliance and reporting. Internal policies or contractual compliance obligations are mentioned only in the internal environment component, but can also be added to the compliance objectives if more formalisation is required. "Reporting objectives" also includes compliance reporting, and "information and communication" asks for transparent provision of compliance information to appropriate personnel. Furthermore, COSO ERM mentions the compliance responsibilities of directors, managers, risk and financial officers, internal auditors, as well as other personnel and external parties.

Unfortunately COSO ERM does not completely integrate compliance processes with risk management processes. For example the risk of non-compliance is not mentioned in the process descriptions of event identification, risk assessment, risk response, or in the control activities. However the common procedure to join risk management and compliance on a process level is to include compliance as "risk of non-compliance" in the risk management process. This enables a risk-based approach to compliance management – a quantitative analysis and prioritisation of actions depending on the probability and impact of a compliance violation. Merging IT compliance with COSO ERM is explained in Table 11:

Table 11: Integration of IT compliance with risk management

COSO ERM component	IT compliance component	IT compliance integration
Internal environment	Requirements analysis	Evaluation of the IT organisation's internal environment and its congruence with the company's overall internal environment
Objective setting	Requirements analysis	Derivation of IT compliance and IT compliance reporting objectives from business objectives
Event identification	Requirements analysis	Identification of events compromising IT compliance
Risk assessment	Deviation analysis	Assessment of the risk of non-compliance in the IT environment
Risk response	Deficiency management	Definition of how to deal with the risk of non-compliance in IT
Control activities	Deficiency management	Definition of policies and procedures to control the risk of non-compliance in IT
Information & communication	Reporting/ documentation	Definition and implementation of IT compliance reporting
Monitoring	Deviation analysis	Continuous monitoring and audits of IT compliance

IT compliance can thus be integrated and even consolidated with risk management. The degree of consolidation is defined by the joint process execution. Weak consolidation means that the risk management process is executed for the IT implementation of a certain business process, and then the whole process is repeated with regard to only IT compliance risks – often spurred by the separation of responsibilities in an organisation. Strong consolidation means that when the risk management process is executed all IT risks including the risk of non-compliance are immediately considered as well.

Adding IT governance

Governance in general and IT governance in the case of IT GRC represents a higher control level than risk management and compliance processes if the organisation is regarded as a cybernetic system (Lewis & Millar, 2009). The relationship of IT governance and IT risk management / IT compliance is twofold.

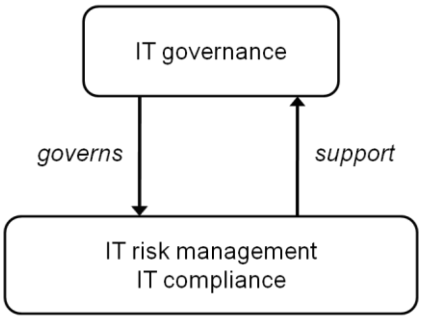


Figure 30: The relationship of IT governance to IT risk management and IT compliance

As Figure 30 shows, on the one hand risk management and compliance activities support the assertion of governance. Compliance management leads to conformance obligations (regulatory, legislation, common law, and contractual) concerning the acceptable use of IT (ISO/IEC 38500:2008, 2008). The IT governance principle of conformance deals with evaluating, directing and monitoring compliance. ISO/IEC38500:2800 requires that risk management be applied to processes to enable conformance, and that it is applied to IT use in general and in IT acquisitions; it requires evaluating risks to continued operation, integrity of information and protection of IT assets, and it demands that risks may be reported by anyone at anytime.

On the other hand, IT governance governs IT risk management and IT compliance activities, i.e. it ensures that they are carried out correctly and in accordance with the ideas provided through the organisation's overall governance and IT governance. The ISO/IEC standard requires that "directors should ensure that IT used are subject to appropriate risk assessment and evaluation, as described in relevant international and national standards" (ISO/IEC 38500:2008, 2008).

IT governance provides the frame for IT risk management and IT compliance decisions. IT risk management and IT compliance management are means to help governance permeate IT operations. Respecting these relations and mapping the IT governance processes (extended with reporting) to the risk management processes with integrated compliance processes as described above, we can derive a process model for integrated IT GRC management (Figure 31).

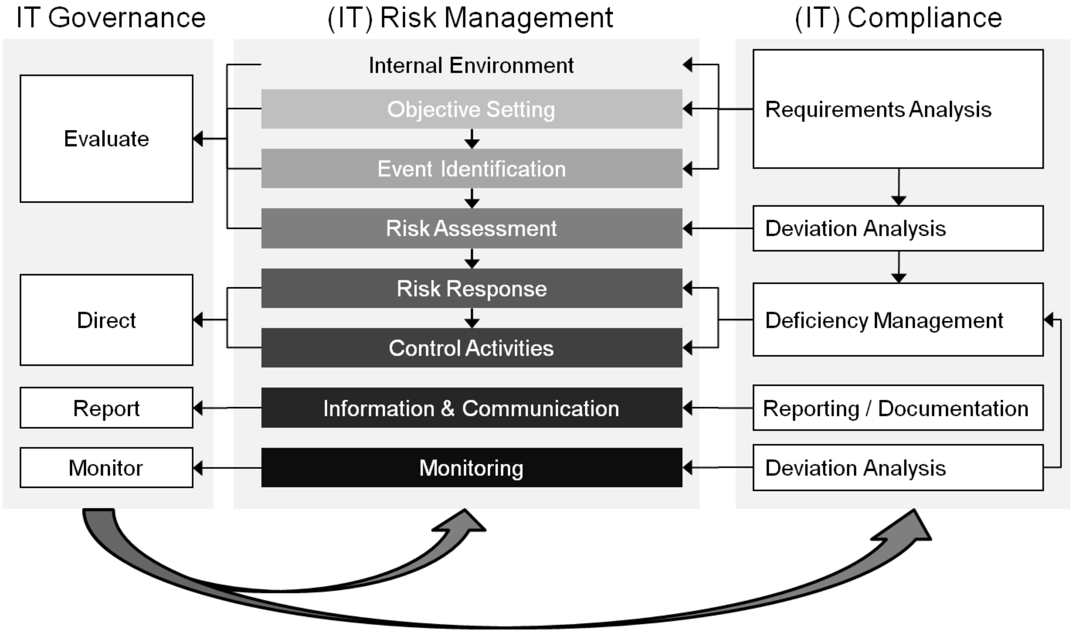


Figure 31: Process model for integrated IT GRC management

The process model has the characteristics of operative management and support processes as stated in the new St. Gallen Management model. Firstly, management and business and support processes within and outside of IT operations can leverage the output of IT risk management and compliance processes. Secondly, IT governance acts as a frame of reference for IT operations, including IT risk management and IT compliance.

A concrete example helps understand the interaction of the disciplines in the integrated model. During a periodic risk management exercise that includes IT compliance requirements analysis an IT manager finds that in one of the company's smaller markets a new national standard for data security has been introduced that surpasses the requirements of the existing standard. The manager needs to ponder investing resources to adhere to the new standard; the acquisition of costly hardware and the introduction of tedious security processes would be required. However the manager might also opt to keep the status quo, as the measures required in the new standard might increase data security only marginally compared to the investment needed to comply with the standard. The deviation analysis as part of the risk assessment process identifies several gaps; therefore the probability of non-compliance is high. In contrast the risk of a data leak is low, as existing security measures have already proven to be effective. The potential financial impact is calculated through quantitative risk assessment methods considering the loss of revenue as a consequence of reputational risk, and the ad-hoc setup of a compliance project under time pressure. From a financial point of view adherence to the standard does not seem to pay off. However the organisation's IT governance codex highlights the organisation's role as a leader in data security practices, which has been considered in the setting of compliance objectives. In order to solve the contradiction, the manager informs his boss, the company's chief information officer, of the situation, delivering the financial analysis as well as the soft facts surrounding the issue. After sitting together with managers from business, the CIO directs that the IT governance codex be revised to find out if a stronger emphasis on financial considerations in compliance decisions is needed, and that the new data security standard shall be ignored for the time being. Thus risk acceptance is chosen as risk response. The only control / deficiency management activity introduced is the monitoring of the standard's acceptance in the industry. If competitors gained an advantage through complying with the standard, the company's decision might have to be reconsidered as the financial risk might prove to be higher than originally reckoned. Finally, the whole decision process and its results are documented and reported to the stakeholders that are concerned of governance, risk, and compliance.

9.3.4 Model validation

The information gathered in Chapter 7 can be used to validate the process model. The IT GRC management processes of three multinational companies were analysed with a focus on integration aspects. The companies came from three different industries: software, healthcare and energy.

For validation purposes we first checked in how far the separate processes of IT governance, IT risk management and IT compliance proposed in the model coincide with the processes observed in the companies. The IT risk management process is strongly formalised in all three enterprises; on a high level the process steps match those of our process model. The IT compliance processes also look like the four steps in our model, even though IT compliance is rather described from a requirements perspective than from a process perspective. IT governance processes, however, differ in the three companies, and none of the companies considered ISO/IEC 38500:2008 when building their own frameworks. The healthcare company does not formally define IT governance at all. The software company has deployed a three-step process of identifying requirements, reviewing and approving of the proposal for the IT governance framework, and updating the framework. This requirements-oriented view of IT governance leaves out many of the ISO/IEC contents. The enterprise from the energy sector, in contrast, describes all IT governance processes used in our model, even though the wording is different and its view of IT governance surpasses the scope of our model, also including some management aspects. The ISO/IEC standard used in our model does not contradict reality in the companies; it covers most of the IT governance in the energy company, it could establish formalisation of IT governance in the healthcare company, and it suggests a wider scope of

IT governance for the software enterprise. Thus as used in our model each of the three disciplines on its own as used should be applicable.

Integration aspects of IT compliance with IT risk management could be observed as described in this document. The energy company carries out all IT compliance processes embedded into IT risk management. The other two companies also integrate the two activities to a certain extent through the risk of non-compliance and through risk-based audits, among other things. The integration with IT governance, in contrast, is hardly ever formalised. New material risks, changes in existing risks, and new compliance requirements trigger updates of the software company's IT governance framework. The energy company mainly links IT governance with the other functions through organisational means by centralising responsibilities for IT risk management and IT compliance within the CIO office. Even though more formalised integration could not be observed, the general setting in the companies would enable it. The claim of the process model's relevance in practice and of its validity can be sustained.

9.4 Discussion

On a high level the integration of IT governance as described in ISO 38500:2008 extended with reporting, of COSO ERM and of IT compliance is feasible. It is necessary to mention several points of critique that can be directed at our research methodology. Firstly, the selection of ISO/IEC 38500:2008, COSO ERM and the IT compliance process model might seem arbitrary to a certain extent. However all three are valid models applied in and derived from best practices in governance, risk management and compliance. Secondly, through adopting a process perspective we have disregarded structural elements of GRC and especially of IT governance. They are not indispensable in creating a process model, but they will have to be examined at another point in time to complete the governance picture. Thirdly, the applicability of the theoretic model has not yet been proven in practice. This will be done at a later stage of research once the model has been broken down to lower process levels and amended with the strategy, organisation and technology aspects of IT GRC.

The model proposed in chapter 9 exceeds the existing GRC models presented above in various ways, thereby extending the knowledge base of information systems research (Hevner, March, Park, & Ram, 2004). Firstly integrated GRC models have thus far been set up without showing the path from separate disciplines to an integrated approach. This is a gap from both research and professional perspectives. For research the logical deduction from the existing knowledge base is missing. For professionals it complicates change management. This gap should be filled through the approach applied in the construction of our model. Secondly our model was explicitly developed for IT GRC, whereas the applicability of existing models to the information technology domain is not evident. At the same time we did not disregard the relation of IT GRC and overall GRC. We tried to facilitate the convergence of GRC with IT GRC through selection of COSO ERM and a generic IT compliance model. Thirdly the role of governance in existing models was rather vague, whereas our model points out the two-fold relation of governance to the two other components and shows how they integrate. Finally our model is based on existing standards and best practices, and the research methodology builds on a scientifically developed GRC definition and a frame of reference for research, whereas existing models were either created in greenfield approaches or there is no explanation as to how they were derived.

9.5 Conclusion

Chapter 9 presented a high-level process model for integrated IT GRC management, thus providing an artefact for the information systems research knowledge base. As a side effect the frame of reference for GRC research was also used; its application successfully helped set and visualise the scope of the research project. It was exemplarily explained how the processes of the separate disciplines of IT governance, IT risk management, and IT compliance relate and how they can be integrated. The model’s validity seems to be given; of course a full proof would only be enabled by the implementation of the model in a real-world scenario.

Chapter 10. Summary and future research

For information systems research, GRC is relevant from the two perspectives of “GRC for IT” (IT GRC) and “IT for GRC” (GRC software). This research project for the first time thoroughly examined both perspectives in a scientific manner. At the beginning, a literature review gave an overview of state-of-the-art GRC research (or the lack thereof) and of driving forces and topics within GRC. From existing definitions and surveys a scientific short-definition was derived and validated in a survey among GRC professionals. Based on the definition a frame of reference for research of GRC was constructed. In order to get an idea of state-of-the-art GRC software, software vendor and market research perspectives were analysed by means of an exploratory survey. The status quo of GRC and GRC software use in large enterprises was examined through a detailed quantitative survey. To complete the picture and to turn towards IT GRC, the status quo of IT GRC management in three large enterprises was investigated. We compared ERM and ITRM frameworks. Lastly, a high-level process model for integrated IT GRC management was developed.

Naturally only a small set of GRC aspects could be highlighted in the research at hand. The many findings and implications for research mentioned provide lots of opportunities for future research within GRC. Some of them were highlighted in Chapter 6, but in this summary we want to provide a broader overview, as the opportunities can be found in all parts of the frame of reference for GRC research.

Future research should examine both horizontal integration (between the three disciplines of GRC) and vertical integration (GRC integration with business processes). This dissertation focused on the former, because it is a prerequisite for studies of the latter. Turning to vertical integration before the nature of horizontal integration is understood and defined would mean taking the traditional, out-dated silo approach to governance, risk management and compliance. Thus we recommend that researchers always start with horizontal integration – if not to provide new insights, so at least to understand the status quo and to apply it in their studies.

We want to suggest three broad research questions as a stimulus for fellow researchers.

i. For horizontal integration future research should break down the IT GRC process model provided in this dissertation to lower levels. On one occasion that has already been done: Vicente & da Silva (2011) merged their conceptual model for GRC with our process model to create a business architecture for integrated GRC.

Researchers following the same path will gain an in-depth understanding of horizontal integration on the process level. This will will enable them to derive requirements for integrated GRC software, as the low-level processes reveal data objects that can be translated into data models, while the processes themselves can form an IT process architecture. That way the pitfall described in Chapter 5 – basing research on inappropriate existing software solutions – is avoided. In terms of a broad research question the recommended analysis of horizontal integration can be phrased in the following way, respecting the four main components of GRC from the frame of reference for GRC research:

How can governance, risk and compliance be integrated with each other in detail on the strategic, process, people and technology levels?

ii. Vertical integration requires not only granular detail of GRC processes, but also in-depth analysis of the respective business processes that are subject of GRC integration. Large ERP software vendors have taken steps into this direction, mainly focusing on automated process controls. The possibilities in this area are vast, as processes and GRC requirements vary depending on the industry, location and legal form of a company. Instead of getting lost in detail, though, research should focus on concepts for process integration identification and on general integration possibilities provided by software technology. The resulting concepts and tools should be universally applicable while only the underlying contents change. Research on vertical integration should thus answer the question: *How can GRC be integrated with business processes on the strategic, process, people and technology levels?*

iii. Integration models as resulting from the first two research questions require validation in real business scenarios in order to prove their relevance. The fact that more and more companies are now adopting integrated GRC approaches offers the opportunity for model validation. Moreover it allows research to carry out ex-ante and ex-post analysis in order to find out in how far the objectives of GRC – increased efficiency, increased effectiveness and ethically correct behaviour – are furthered by such initiatives. The analysis of benefits was also recommended in Chapter 6, as the perceived benefits are somewhat accepted in practice but have not been proven by research to date. Studying the benefits of GRC should be done pursuing the research question:

In how far does integrated GRC improve efficiency and effectiveness of the concerned processes, and does it advocate ethically correct behaviour?

For our part we support any kind of GRC research not only through our publications, but also by means of our website grc-resource.com that provides basic information on

GRC. We encourage other researchers to ask for advice when structuring their studies or to send their papers to us if they want to gather feedback.

The interesting topic of GRC should be picked up by more researchers. It seems that in the research community GRC has witnessed increased attention while this project was carried out. Two conferences (Informatik 2010 and the Australasian Conference on Information Systems, ACIS 2010) featured tracks focusing on GRC, explicitly mentioning integration aspects. Thus we expect GRC not only to grow in business, but also to take a more prominent role in information systems research. We are glad to contribute to this development with the research presented in this dissertation.

Bibliography (cited references)

Ahlemann, F., & Gastl, H. (2007). Process Model for an Empirically Grounded Reference Model Construction. In P. Fettke, & P. Loos (Eds.), *Reference Modelling for Business Systems Analysis* (pp. 77-97). Hershey: Idea Group.

AICPA. (1992). 70 Statement on Auditing Standards: Reports on the Processing of Transactions by Service Organizations.

Albrecht, P. (1998). Auf dem Weg zu einem holistischen Risikomanagement. Mannheimer Manuskripte zur Risikotheorie, Porftolio Management und Versicherungswirtschaft .

Amberg, M., & Mossanen, K. (2008, January). Ergebnisse aus Wissenschaft und Forschung: Ignorieren von gesellschaftlicher Verantwortung zahlt sich nicht aus. *HR § Compliance , 3* (1), pp. 12-13.

Applegate, L. (1999, March). Rigor and Relevance in IS Research - Introduction. *MIS Quarterly , 23* (1), pp. 1-2.

Approva. (2007). *2007 Approva GRC survey*. Retrieved April 22, 2009

AS/NZS 4360:2004. (2004). Risk management. AS/NZS.

Balzi, B., Deckstein, D., & Schmitt, J. (2006). *Siemens Forced to Battle Internal Corruption*. Retrieved September 07, 2008, from http://www.spiegel.de/international/spiegel/0,1518,451105,00.html

Banham, R. (2007). Is ERM GRC? Or vice versa? *Treasury & Risk , 2* (6), pp. 48-50.

Basel Committee on Banking Supervision. (2004). *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework* . Retrieved July 23, 2009, from http://www.bis.org/publ/bcbs107.pdf

Benston, G., & Hartgraves, A. (2002). Enron, what happened and what we can learn from it. *Journal of Accounting and Public Policy , 21* (2), pp. 105-127.

Bernstein, P. (1996). *Against the Gods: The Remarkable Story of Risk.* New York: John Wiley and Sons.

Böhm, M. (2008). IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. *HMD - Praxis der Wirtschaftsinformatik* (263), pp. 15-29.

Böhm, M., Goeken, M., & Johannsen, W. (2009). Compliance und Alignment: Vorgabenkonformität und Strategieabglich als Erfolgsfaktoren für eine wettbewerbsfähige IT. *HMD - Praxis der Wirtschaftsinformatik* (269), pp. 7-17.

Broady, D., & Roland, H. (2008). *SAP GRC for Dummies.* Indianapolis: Wiley.

Brown, A., & Grant, G. (2005). Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systems, 15*, pp. 696-712.

BSI. (2006). BS 25999-1 Business Continuity Management. Code of Practice.

BSI. (2007). BS 25999-2 Specification for Business Continuity Management.

Burnaby, P., & Hass, S. (2009). Ten steps to enterprise-wide risk management. *Corporate Governance , 9* (5), pp. 539-550.

Caldwell, F. (2008). *The Enterprise Governance, Risk and Compliance Platform Defined*. Retrieved July 8, 2009, from http://www.gartner.com/DisplayDocument?doc_cd=155196

Caldwell, F., & Eid, T. (2008). *Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, 2008*. Retrieved July 11, 2009, from http://www.metricstream.com/regForms/gartner_mq_reg.htm

Caldwell, F., Eid, T., & Casper, C. (2009). *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, 2009*. Retrieved January 5, 2009, from http://paisley.thomsonreuters.com/website/pcweb.nsf/pages/ARAE-6XANSY

Caldwell, F., Proctor, P., & Nicolett, M. (2010). *EMC buys Archer for enhanced IT GRC capabilities*. Retrieved May 23, 2010, from http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1275214

Chatterjee, A., & Milam, D. (2008). Gaining Competitive Advantage from Compliance and Risk Management. In D. Pantaleo, & N. Pal (Eds.), *From Strategy to Execution - Turning Accelerated Global Change into Opportunity* (pp. 167-183). Berlin: Springer.

Coderre, D. (2005). Global Technology Audit Guide. Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. Retrieved January 7, 2010, from http://www.theiia.org/download.cfm?file=19897

Corporate Integrity, LLC. (2007). *What is GRC?* Retrieved April 14, 2009, from http://www.corp-integrity.com/about/grc.html

COSO. (2004). *Enterprise risk management framework*. Retrieved February 12, 2010, from http://www.coso.org

COSO. (1992). *Internal control - integrated framework*. Retrieved February 12, 2010, from http://www.coso.org

Curran, B. (2007). Defragmenting GRC. *Pharmaceutical Technology , 4* (16), pp. 20-23.

Dameri, R. (2009, February). Improving the Benefits of IT Compliance Using Enterprise Management Information Systems. *Electronic Journal of Information Systems Evaluation , 12* (1), pp. 27-38.

Dawson, M. (2008, August). Integrating Compliance Risk Management into Enterprise Risk Management. *Bank Accounting and Finance , 21* (5), pp. 30-33.

DeLoach, J. (2000). Enterprise-Wide Risk Management: Strategies for Linking Risk & Opportunity. Chicago: Financial Times / Prentice Hall.

Deming, W. (1982). *Out of the Crisis.* Cambridge (MA): MIT.

Denk, R., & Exner-Merkelt, K. (2005). Corporate Risk Management. Unternehmensweites Risikomanagement als Führungsaufgabe. Wien: Linde.

Detecon. (2010). IKS - Interne Kontrollsysteme nach der 8. EU-Richtlinie. Zürich: Detecon.

Deutscher Bundestag. (1998). Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). Berlin: Deutscher Bundestag.

Dittmar, L. (2007). Demystifying GRC. *Business Trends Quarterly , 2* (4), pp. 16-18.

Economist Intelligence Unit. (2008). *Managing risk through financial processes. Embedding governance, risk and compliance*. Retrieved April 21, 2009, from http://graphics.eiu.com/marketing/pdf/SAP%20GRC.pdf

Fettke, P. (2006). State-of-the-Art des State-of-the-Art. Eine Untersuchung der Forschungsmethode „Review" innerhalb der Wirtschaftsinformatik. *Wirtschaftsinformatik , 48* (4), pp. 257-266.

Financial Times Deutschland. (2009, April 14). *Lehman Brothers und die Autobombe*. Retrieved November 6, 2010, from http://www.ftd.de/unternehmen/finanzdienstleister/:gewaltiger-uranvorrat-lehman-brothers-und-die-atombombe/499823.html

Fisher, J. (2007, January). Compliance in the Performance Management Context. What technologies could simplify compliance and automate information gathering. *Bank Accounting and Finance , 5* (1), pp. 41-44.

Foley, S. (2009). Security Risk Management using Internal Controls. *Proceedings of the first ACM workshop on Information security governance* (pp. 59-64). New York: ACM.

Francis, S., & Richards, T. (2007, October). Why ERM matters... and how to accelerate progress. *Risk Management , 15*, pp. 28-31.

Frigo, S., & Anderson, R. (2009). A Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance , 44* (1), pp. 20-61.

Gupta, P. (2009). Internal Control. COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices. Retrieved January 2010, 2010, from http://ssrn.com/abstract=1417604

Hagerty, J., Verma, K., & Gaughan, D. (2008). *The Governance, Risk Management, and Compliance (GRC) Landscape, Part 2: Software's Integral Role in GRC Automation*. Retrieved January 10, 2010, from http://www.metricstream.com/regForms/amr_grc_reg.htm

Harper, D. (2010). *Online Etymology Dictionary*. Retrieved November 01, 2010, from http://www.etymonline.com

Hauschka, C. (Ed.). (2007). Corporate Compliance - Handbuch der Haftungsvermeidung im Unternehmen. München: Beck.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly , 28* (1), pp. 75-105.

Hilb, M. (2009). *Integrierte Corporate Governance.* Berlin: Springer.

Hoffmann, M. (2007). Governance, Risk und Compliance (GRC) - ein integrierter Ansatz. *IM - Information Management & Consulting , 24* (1), pp. 74-81.

Hovis, J. (2007). *CIO at the center*. Retrieved April 23, 2009, from http://www.oracle.com/dm/08q3field/ogec_wp_cio.pdf

ISACA. (2010). *COBIT 5 Design Paper Exposure Draft*. Retrieved May 20, 2010, from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT5_Design_Exposure_18Mar2010.pdf

ISACA. (2009b). Implementing and Continually Improving IT Governance. Rolling Meadows: ISACA.

ISACA. (2009a). *The Risk IT Framework.* Rolling Meadows: ISACA.

ISO 31000:2009. (2009). Risk management – Principles and guidelines. ISO.

ISO. (2008). ISO 9001:2008; Quality management systems - Requirements. ISO.

ISO/IEC 27001:2005. (2005). Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC.

ISO/IEC 27005:2008. (2008). Information security risk management. ISO/IEC.

ISO/IEC 38500:2008. (2008). Corporate governance of information technology. ISO/IEC.

IT Governance Institute. (2007). *COBIT 4.1.* Rolling Meadows: ISACA.

IT Policy Compliance Group. (2008). *2008 Annual Report. IT Governance, Risk, and Compliance*. Retrieved April 21, 2009, from http://www.itpolicycompliance.com/pdfs/ITPCGAnnualReport2008.pdf

Jackson, R. (2007, June). The future is now, Cutting Edge Technology for GRC. *Inside Counsel , 17* (1).

Kahn Consulting. (2008). *GRC, E-Discovery, and RIM: state of the industry*. Retrieved January 28, 2009, from http://www.kahnconsultinginc.com/library/KCI-GRC-RIM-EDD-survey.pdf

Kelly, J. (2008). *Risk management surpasses compliance as top GRC priority*. Retrieved January 11, 2009, from http://go.techtarget.com/r/3484977/6129174

Kersten, H., & Klett, G. (2008). *Der IT Security Manager.* Wiesbaden: Vieweg & Teubner.

Klotz, M., & Dorn, D.-W. (2008). IT Compliance - Begriff, Umfang und relevante Regelwerke. *HMD - Praxis der Wirtschaftsinformatik* (263), pp. 5-14.

KPMG. (2008). *Governance, risk, and compliance. Driving value through controls monitoring*. Retrieved April 17, 2009, from http://www.kpmg.ca/en/services/advisory/documents/GovernanceRiskCompliance.pdf

Lattemann, C. (2010). Corporate Governance im globalisierten Informationszeitalter. München: Oldenbourg.

Leibs, S. (2007). *One for three*. Retrieved June 27, 2009, from CFO Magazine 2007/9: http://www.cfo.com/article.cfm/9689509

Lewis, E., & Millar, G. (2009). The viable governance model – a theoretical model for the governance of IT. *Proceedings of the 42nd Hawaii International Conference on System Sciences.*

Liegl, P. (2009). Die Anforderungen von EUROSOX an IT-Prozesse (Master Thesis). Vienna: TU Vienna.

Lindlof, T., & Taylor, B. (2002). *Qualitative Communication Research Methods.* Thousand Oaks, CA: Sage.

Lo, A. (2009). Regulatory reform in the wake of the financial crisis of 2007-2008. *Journal of Financial Economic Policy , 1* (1), pp. 4-43.

Ludewig, J., & Lichter, H. (2006). *Software Engineering.* Heidelberg: Dpunkt.

Madhani, P. (2009, June). Bankruptcy of Lehman Brothers. A Pointer of Subprime Crisis. *The Accounting World , 1* (6), pp. 33-39.

Mallin, C. (2007). *Corporate Governance.* Oxford: Oxford University Press.

Mardjono, A. (2005). A tale of corporate governance: lessons why firms fail. *Managerial Auditing Journal , 20* (3), pp. 272-283.

Mardjono, A. (2005). A tale of corporate governance: lessons why firms fail. *Managerial Auditing Journal , 20* (3), pp. 272-283.

Marekfia, W., & Nissen, V. (2009). *Strategisches GRC-Management - Grundzüge eines konzeptionellen Bezugrahmens.* Retrieved May 7, 2010, from Forschungsberichte zur Unternehmensberatung: http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18253/FUB-2009-01.pdf

Martin, W., & Nussdorfer, R. (2005). White Paper 'Pulse Check': Operational, Tactical and Strategic CPM. Part 1: Vendor Independent White Paper and Reference Architecture. Retrieved July 3, 2008, from http://www.qis.dk/WP_Uafh/CPM%20-%20Corporate%20Performance%20Management%20WhitePaper.pdf

McClean, C. (2009). *The Forrester Wave: Enterprise Governance, Risk, and Compliance Platforms, Q3 2009*. Retrieved July 7, 2009, from http://img.en25.com/Web/OpenPages/Forrester_wave_ent_gov_risk_compl.pdf

McClean, C., McNabb, K., & Dill, A. (2009). *The GRC Technology Puzzle: Getting all the Pieces to Fit*. Retrieved January 10, 2010, from http://www.forrester.com/Research/Document/Excerpt/0,7211,45772,00.html

McGinnis, S., Pumphrey, K., Trimmer, K., & Wiggins, C. (2004). Sustaining and extending organization strategy via information technology governance. *Proceedings of the 37th Hawaii International Conference on System Sciences.*

Melis, A. (2004). *Corporate Governance Failures. To What Extent is Parmalat a Particularly Italian Case?* Retrieved November 06, 2010, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=563223

Menzies, C. (Ed.). (2004). Sarbanes-Oxley Act. Professionelles Management interner Kontrollen. Stuttgart: Schäffer-Poeschel.

Menzies, C. (Ed.). (2006). *Sarbanes-Oxley und Corporate Compliance.* Stuttgart: Schäffer-Poeschel.

Merriam-Webster. (2010). *Merriam-Webster Dictionary*. Retrieved November 01, 2010, from http://www.merriam-webster.com

Mitchell, S. (2007a). *GRC – more than three letters*. Retrieved September 12, 2008, from http://grc360.blog.oceg.org/2007/08/grc-more-than-three-letters.html

Mitchell, S. (2007b). GRC360: A framework to help organisations drive principled performance. *International Journal of Disclosure and Governance , 4* (4), pp. 279-296.

Moeller, R. (2007). *COSO Enterprise Risk Management.* New Jersey: Wiley.

Mossanen, K. (2010). *Compliance im IT-Outsourcing.* Hamburg: Dr. Kovac.

Müller, G., & Terzidis, O. (2008, October). IT-Compliance und IT-Governance. *Wirtschaftsinformatik , 50* (5), pp. 341-343.

Musura, J. (2010). *Credit Default Swaps and Financial Market Stability. Diploma Thesis.* Vienna: Vienna University of Economics and Business.

Myers, M. (2009). Qualitative Research in Business & Management. London: Sage.

Nadhirah, A., & Khairuddin, H. (2008). Enterprise level IT risk management. *Proceedings of the 9th Conference on Applied Computer Science* (pp. 401-404). Venice: WSEAS.

OCEG. (2009). *GRC Capability Model. "Red Book" 2.0.* Retrieved November 11, 2009, from http://www.oceg.org

OCEG. (2009). *GRC-IT Blueprint. Version 1.0*. Retrieved November 12, 2009, from http://www.oceg.org

OGC. (2007). *ITIL v3*. Retrieved February 12, 2010, from http://www.itil-officialsite.com

Ohki, E., Harada, Y., Kawachugi, S., Shiozaki, T., & Kagaua, T. (2009). Information Security Governance Framework. *Proceedings of the first ACM workshop on Information security governance.*

Organisation for Economic Co-Operation and Development. (2004). *OECD Principles of Corporate Governance.* Paris: OECD.

Othersen, M., & McClean, C. (2009). *Consolidation Looms for the IT GRC Market*. Retrieved May 23, 2010, from http://www.forrester.com/rb/Research/consolidation_looms_for_it_grc_market/q/id/47027/t/2

Panitz, J., Wiener, M., & Amberg, M. (2010). A Balanced Scorecard for Compliance – requirements of a comprehensive compliance reporting. *Proceedings of the 16th Americas Conference on Information Systems.*

Paulus, S. (2009). *A GRC reference architecture. Overview report.* Retrieved November 18, 2009, from http://www.kuppingercole.com/report/sp_overview_repo_grc_arch_051009

PricewaterhouseCoopers. (2005). *8th Annual Global CEO Survey. Bold Ambitions, Careful Choices*. Retrieved June 28, 2010, from http://www.grc-resource.com/resources/pwc_8th_ceo_survey.pdf

PricewaterhouseCoopers. (2004). *Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management.* Retrieved January 01, 2010, from http://www.globalcompliance.com/pdf/PwCIntegrityDrivenPerformance.pdf

PricewaterhouseCoopers. (2007). *Internal Audit 2012. A study examining the future of internal auditing and the potential decline of a controls-centric approach*. Retrieved January 5, 2010, from http://www.pwchk.com/home/webmedia/633305443662968204/ia2012_nov2007.pdf

Proctor, P., Caldwell, F., & Eid, T. (2008). *A Comparison Model for the GRC Marketplace, 2008 to 2010*. Retrieved June 30, 2008, from http://www.gartner.com/DisplayDocument?id=712207

Project Management Institute. (2008). A Guide to the Project Management Body of Knowledge (PMBOK Guide). Fourth Edition. Newtown Square: PMI.

Prokein, O. (2008). IT-Risikomanagement. Identifikation, Quantizifierung und wirtschaftliche Steuerung. Wiesbaden: Gabler.

Public Company Accounting Oversight Board. (2007). Auditing Standard No. 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. Retrieved January 21, 2010, from http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises. *Proceedings of the 21st Australasian Conference on Information Systems, ACIS 2011.*

Racz, N., Weippl, E., & Bonazzi, R. (2011). IT Governance, Risk & Compliance (GRC) Integration and Status Quo. An Explorative Industry Case Study. *Proceedings of the 1st International Workshop on IT GRC, IT GRC 2011.*

Racz, N., Weippl, E., & Seufert, A. (2010a). A frame of reference for research of integrated Governance, Risk & Compliance (GRC). In B. De Decker, & I. Schaumüller-Bichl (Ed.), *Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings* (pp. 106-117). Berlin: Springer.

Racz, N., Weippl, E., & Seufert, A. (2010b). A process model for integrated IT governance, risk, and compliance management. In J. Bardzins, & M. Kirikova (Ed.), *Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010* (pp. 155-170). Riga: Riga University Press.

Racz, N., Weippl, E., & Seufert, A. (2010c). Questioning the need for separate IT risk management frameworks. In K.-P. Fähnrich, & B. Franczyk (Ed.), *Lecture Notes in Informatics (LNI) P-176 Proceedings, Informatik 2010. 2,* pp. 245-252. Bonn: Gesellschaft für Informatik.

Racz, N., Weippl, E., & Seufert, A. (2011). Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives. *Proceedings of the 44th Hawaii International Conference on System Sciences, HICSS 2011.*

Rasmussen, M. (2008). *2008 GRC drivers, trends & market directions*. Retrieved July 10, 2009, from http://www12.sap.com/community/showdetail.epx?ItemID=11997

Rasmussen, M. (2007, May). Hand in Hand. *Business Trends Quarterly , 2* (2), pp. 44-46.

Rath, M., & Sponholz, R. (2009). IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Berlin: Schmidt.

Regierungskommission DCGK. (2010). *Deutscher Corporate Governance Kodex.* Berlin: Bundesministerium für Justiz.

Riaz, S. (2009). The global financial crisis: an institutional theory analysis. *Critical Perspectives on International Business , 5* (1/2), pp. 26-35.

Ribbers, P., Peterson, R., & Parker, M. (2002). Designing information technology governance processes: diagnosing contemporary practices and competing theories. *Proceedings of the 35th Hawaii International Conference on System Sciences.*

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *Proceedings of the 37th Hawaii International Conference on System Sciences.* Hawaii: IEEE.

Roman, G. (1984). A Taxonomy of Current Issues in Requirements Engineering. *IEEE Computer , 18* (4), pp. 14-23.

Rüegg-Sturm, J. (2003). Das neue St. Galler Management-Modell. Bern: Haupt.

Sackmann, S. (2008). Automatisierung von Compliance. *HMD - Praxis der Wirtschaftsinformatik* (263), pp. 39-46.

Schlagheck, B. (2000). Object-oriented reference models for process and project controlling. Foundation-construction-fields of application. Wiesbaden: Deutscher Univ.-Verlag.

Schnell, R., Hill, P., & Esser, E. (1999). *Methoden der empirischen Sozialforschung.* Munich: Oldenburg.

Special Investigative Committee of the Board of Directors of WorldCom, Inc. (2003). *Report of Investigation*. Retrieved October 30, 2010, from http://www.sec.gov/Archives/edgar/data/723527/000093176303001862/dex991.htm

Switzer, C. (2007). Integration innovation. *Business Trends Quarterly , 2* (4), pp. 26-32.

Tapscott, D. (2006). *Trust and Competitive Advantage: An Integrated Approach to Governance, Risk & Compliance*. Retrieved January 23, 2010, from http://www.findwhitepapers.com/whitepaper1714/

Tennant, G. (2001). Six Sigma: SPC and TQM in Manufacturing and Services. Aldershot: Gower.

Teubner, A., & Feller, T. (2008). Informationstechnologie, Governance und Compliance. *Wirtschaftsinformatik , 50* (5), pp. 400-407.

Teuteberg, F. (2010). IT-Risikomanagement - Eine Studie zum Status quo in deutschen Unternehmen. In F. Keuper, & F. Neumann (Eds.), *Governance, Risk Management und Compliance: Innovative Konzepte und Strategien* (pp. 69-89). Wiesbaden: Gabler.

The Committee on the Financial Aspects of Corporate Governance. (1992). *The Financial Aspects of Corporate Governance.* London: Gee.

U.S. Congress. (2002). *The Sarbanes-Oxley Act of 2002.* Washington D.C.: U.S. Congress.

United States Securities and Exchange Commission. (2009). *Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements*. Retrieved November 08, 2010, from http://www.sec.gov/news/studies/2009/sox-404_study.pdf

Vemuri, A. (2008). Strategic themes in risk and compliance. *FINsights* (2), pp. 2-5.

(2008). Compliance in der Unternehmerpraxis. In E. Vetter, G. Wecker, & H. van Laak (Eds.), *Compliance in der Unternehmerpraxis* (pp. 33-47). Wiesbaden: Gabler.

Vicente, P., & da Silva, M. (2011). A Business Architecture for integrated IT Governance, Risk and Compliance. *1st International Workshop on IT GRC, ITGRC 2011.* Washington, D.C.

Vinten, G. (2002). The corporate governance lessons of Enron. *Corporate Governance , 2* (4), pp. 4-9.

Volonino, L., Gessner, G., & Kermis, G. (2004). Holistic Compliane with Sarbanes Oxley. *Communications of the Association for Information Systems , 14* (1), pp. 219-233.

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, *8*.

Wechsler, P. (2008). The GRC harmony. *Treasury & Risk , 2* (6), p. 13.

Weill, P., & Ross, J. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Boston: Harvard Business Press.

World Economic Forum. (2010). *Global Risks 2010.* Geneva: World Economic Forum.

Zarakowitis, H. (2009). Evaluation of IT Risk Management Tools (Diploma Thesis). Vienna: TU Vienna.

Zur Muehlen, M., & Rosemann, M. (2005). *Integrating Risks in Business Process Models.* Retrieved May 20, 2010, from Proceedings of the 16th Australasian Conference on Information Systems: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.9487&rep=rep1&type=pdf

Acknowledgements

I want to thank Prof. Dr. Andreas Seufert (Steinbeis Hochschule Berlin), PD Dr. Edgar Weippl and O.Univ.Prof. Dipl.-Ing. Dr.techn. A Min Tjoa (both TU Vienna) for their personal, professional and administrative support throughout the research project. Thanks to the whole Institute of Business Intelligence (IBI), the Institute of Software Technology and Interactive Systems (ISIS) and Secure Business Austria (SBA) for the services provided in the course of my research.

Thank you to Sebastian Eickhoff for designing the GRC Resource logo and grc-resource.com website.

Further I would like to thank all experts and organisations that took part in our surveys and case studies. Without their contribution the composition of the research at hand would not have been possible.

Many thanks especially to Matthias Gleis of SAP and Patric Burkhart of BASF for giving me the chance to gain professional experience in addition to my scientific work.

Lastly I want to thank fellow researchers Johannes Christian Panitz and Ülkühan Kapar for the joint research about the GRC and GRC software status quo in organisations, and Riccardo Bonazzi for the cooperation concerning the case studies of the IT GRC management status quo.

Appendix A – List of manually processed websites

www.aberdeen.com
www.btquarterly.com
www.businessfinancemag.com
www.cfo.com
www.corp-integrity.com
www.deloitte.com
www.findwhitepapers.com
www.forrester.com
www.gartner.com
www.infosys.com
www.metricstream.com
www.oceg.org
www.oracle.com
www.paisley.com
www.pwc.com
www.sap.com

Appendix B – List of 107 publications from literature review

1. Approva Corporation (2007): 2007 Approva GRC Survey. Available from: http://www.approva.net/survey [Accessed 22 Apr 2009].
2. Asprion, P. & Knolmayer, G.F. (2008): Compliance-Software: Einsatzmöglichkeiten und Auswirkungen auf die Wirtschaftsprüfung. ERP Management, 2008/2, pp.28-31.
3. Banham, R. (2007): Is ERM GRC? Or Vice Versa? Treasury & Risk, Jun2007, pp.48-50.
4. Broady, D.V. & Roland, H.A. (2008): SAP GRC for Dummies. Indianapolis: Wiley.
5. Caldwell, F. (2007): GRC – Get It Right! Business Trends Quarterly, 2007/1, pp.58-60.
6. Caldwell, F. & Eid, T. (2008): Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. Available from: http://www.metricstream.com/regForms/gartner_mq_reg.htm [Accessed 11 Oct 2008].
7. Cangemi, M.P. (2008): The Controls Challenge. Bank Accounting & Finance, 2008/4, pp.43-52.
8. Childers, D. (2007): Getting a Clear View. Optimizing Issue Management. GRC360°, pp.10-12.
9. Corporate Integrity, LLC (2007): What is GRC? Available from: http://www.corp-integrity.com/about/grc.html [Accessed 14 Apr 2009].
10. Curran, B. (2007): Defragmenting GRC. Pharmaceutical Technology, 31 (2007/11), pp. 20-23.
11. Dickhart, G. (2008): Risk: Key to Governance. Internal Auditor, 65/6, pp.27-30.
12. Dittmar, L. (2006a): Enabler of GRC: What does utopia look like? Business Trends Quarterly, 2006/4, pp.20-22.
13. Dittmar, L. (2006b): Deloitte Panel Discussion. Business Trends Quarterly, 2006/3, pp.27-33.
14. Dittmar, L. (2006c): The Complete Package. Business Trends Quarterly, 2006/3, pp.42-44.
15. Dittmar, L. (2006d): Aligning IT Assets with Governance, Risk, and Compliance Needs: “What’s so different today?” Business Trends Quarterly, 2006/4, pp.34-42.
16. Dittmar, L. (2006e): Making the Connection. Information Governance is the Link to Enterprise Performance. GRC360°, 2006/2, pp.8-9.
17. Dittmar, L. (2006f): The Alignment Challenge. Defining and Meeting GRC Technology Needs. GRC360°, pp.10-25.
18. Dittmar, L. (2007a): Demystifying GRC. Business Trends Quarterly, 2007/4, pp.16-18. Available from: http://www.deloitte.com/dtt/cda/doc/content/us_grc_Demystifying%20GRC_Lee%20Dittmar.pdf [Accessed 14 Apr 2009].
19. Dittmar, L. (2007b): Tackling the Information Challenge. Now is the Time for Enterprise Information Governance. Business Trends Quarterly, 2007/2, pp.24-31. Available from: http://www.deloitte.com/dtt/cda/doc/content/us_grc_BTQ%20Effective%20Information%20Governance%20A%20Key%20Component%20to%20Improving%20Information%20Quality(2).pdf [Accessed 21 Apr 2009].
20. Dittmar, L. (2007c): First Steps on a Long Journey. Toward an Architected GRC System. GRC360°, 2007/2, p.1.
21. Dittmar, L. (2007d): The Key to Global Success. Unlocking the GRC Challenges. GRC360°, 2007/1, pp.4-7.
22. Dittmar, L. (2008): IT for GRC: Improving Information Quality. GRC360°, 2008/2, pp.4-7.
23. Dittmar, L. & Bishop, T. (2008): Focus on Financial Statement Fraud. GRC360°, 2008/1, pp.4-7.
24. Dittmar, L. & Porrello, K. (2007): Bringing Information Technology to the Front Burner – Why it Matters, How to Make it Happen. Business Trends Quarterly, 2007/3, pp.18-20.
25. Duckers, K. (2008): Strategic GRC Yields Clear Payback. Bank Technology News, 21/10, p.40.
26. Duffy, M.J. (2006): Measure Twice: Cut Once. Risk-Based Governance Pays Off. GRC360°, 2006/2, p.7.
27. Economist Intelligence Unit (2007): Fortifying the enterprise: Governance, risk and compliance strategies. Available from: http://www.oracle.com/go/?&Src=5634321&Act=80&pcode=NA05070152C39 [Accessed 23 Apr 2009].

28. Economist Intelligence Unit (2008): Managing risk through financial processes. Embedding governance, risk and compliance. Available from: http://www.cfo.com/whitepapers/index..cfm/register?action=whitepaperreg&whitepaper_id=13280389 [Accessed 21 Apr 2009].
29. Edwards, J. (2009): A Defining Moment. CFO Magazine, 2009/1. Available from: http://www.cfo.com/article.cfm/12835338?f=search [Accessed 22 Apr 2009].
30. Eid, T. & Caldwell, F. (2006): Finance and Audit GRC Software Market is Expanding. Available from: http://www.gartner.com/it/content/498300/498334/risk_research.pdf [Accessed 16 Apr 2009].
31. Epicor Software Corporation (2008): Achieving Efficient Governance, Risk and Compliance (GRC) Through Process and Automation. Available from: http://www.findwhitepapers.com/whitepaper4101/ [Accessed 24 Apr 2009].
32. Feldman, M. (2007): Avoiding GRC Landmines. Technologies for Navigating the Minefield. GRC360°, 2007/1, pp.19-21.
33. Frank, T. (2006): Drawing a Technology Roadmap. Survey Findings on Use of GRC Technologies. GRC360°, 2006/2, pp.17-19.
34. Frigo, M.L. & Anderson, R.J. (2009): A Strategic Framework for Governance, Risk, and Compliance. Strategic Finance, 44/1, pp.20-61.
35. Gill, S. & Leech, T. (2008): Conversations with Tim Leech – Perspectives from an industry expert. FINsights, 2, pp.62-64. Available from: http://www.infosys.com/FINsights/Finsights-financial-risk-with-Governance.pdf [Accessed 17 Apr 2009].
36. Gill, S. & Purushottam, U. (2008): Integrated GRC – Is Your Organisation Ready to Move? SETLabs Briefings, 6/3, pp.37-46.
37. Goff, J. (2008): The Emergence of Convergence. CFO Magazine, 2008/1. Available from: http://www.cfo.com/article.cfm/10345544?f=search [Accessed 22 Apr 2009].
38. Götz, B., Köhntopp, F., Mayer, B. & Wagner, G. (2008): Einsatz einer ganzheitlichen GRC-Softwarelösung. HMD – Praxis der Wirtschaftsinformatik, 2008/263, pp.89-98.
39. Herrod, C. & Anand, S. (2008): GRC Industry Survey 2008: A Benchmark For Compliance and Spending. Available from: http://www.grcg.com/storage/downloads/GRC-Industry-Survey.pdf [Accessed 23 Apr 2009].
40. Hoffmann, M. (2009): Governance, Risk und Compliance (GRC) – ein integrierter Ansatz. Information Management and Consulting, 24/1, pp.74-81.
41. Hovis, J.J. (2007): CIO at the Center. Available from: http://www.oracle.com/dm/08q3field/ogec_wp_cio.pdf [Accessed 23 Apr 2009].
42. IDS Scheer AG (2008): Governance, Risk & Compliance Management mit ARIS. Available from: http://www.ids-scheer.de/set/6473/Governance_Risk_%26_Compliance_WP_de_2008-06.pdf [Accessed 16 Apr 2009].
43. Irion, R. & Kugel, T. (2007): Besseres Risikomanagement. Geldinstitute, 2007/5, pp.14-15.
44. Jackson, R. (2007): The Future is Now. Cutting Edge Technology for GRC. GRC360°, 2007/2, pp.19-26.
45. Jutras, C. (2008): Are CFOs Ready For Unified GRC Solutions? Available from: http://download.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/brochures/download.epd?context=A9CEC035F7328E3FF5B86C8341B196B249F253FEDF521F7923B9F34FEBCA4A368DEE93BEF89ABDAF6E527E276DCDA4FBD6DB5D68DF813C99 [Accessed 23 Apr 2009].
46. Kahn Consulting, Inc. (2008): GRC, E-Discovery, and RIM: State of the Industry. Available from: http://www.kahnconsultinginc.com/library/KCI-GRC-RIM-EDD-survey.pdf [Accessed 21 Apr 2009].
47. Kampffmeyer, U. (2007): GRC. Governance, Risk Management und Compliance. Available from: http://www.competence-site.de/governance-risk-compliance.nsf/BE9935DC3A78A9BFC12575060044DFD0/$File/governance_risk_management%20compliance_project_consult_080820.pdf [Accessed 24 Apr 2009].
48. Kark, K. (2008): The Role Of Technology In Establishing A GRC Program. Business Trends Quarterly, 2008/2, p.105.
49. Kling, M. (2008): Effiziente Unterstützung interner Kontrollsysteme mit einer GRC Software Plattform. Available from: http://www.ids-scheer.de/set/6473/ARIS_Expert_Paper-GRC-Interne_Kontrollsysteme_Kling_-_2008-01_de.pdf [Accessed 23 Apr 2009].

50. KPMG (2008): Governance, Risk, and Compliance. Driving Value through Controls Monitoring. Available from: http://www.kpmg.ca/en/services/advisory/documents/GovernanceRiskCompliance.pdf [Accessed 17 Apr 2009].
51. Krell, E. (2009): GRC comes of Age. Available from: http://businessfinancemag.com/article/grc-goes-deep-0330 [Accessed 23 Apr 2009].
52. Lam, J. (2007): Operational Risk Management – Beyond Compliance to Value Creation. Available from: http://www.openpages.com [Accessed 22 Apr 2009].
53. Lattner, D. (2006): The Power of Positive Technology. Better Information Produces Better Results. GRC360°, 2006/2, pp.4-5.
54. Laurent, W. (2009): More than Risk? DM Review, 19/1, pp.41-44.
55. Leibs, S. (2007): One for Three. CFO Magazine, 2007/9. Available from: http://www.cfo.com/article.cfm/9689509?f=search [22 Apr 2009].
56. McClean, C. & Rasmussen, M. (2007): The Forrester Wave: Enterprise Governance, Risk, And Compliance Platforms, Q4 2007. Available from: http://www.metricstream.com/regForms/forrester_reg.htm [Accessed 11 Oct 2008].
57. McCuaig, B. (2008): Is Risk Management Failing? GRC360°, 2008/2, pp.8-9.
58. McHale, T. (2008): A Unified Approach To GRC. GRC360°, 2008/2, pp.16-17.
59. Menzies, C., Martin, A., Koch, M., Trebuth, C., Esche, S., Heinze, T., Roth, C., Schellhas, C., Stähle, P. (2007): Governance, Risk Management and Compliance: Sustainability and Integration supported by Technology. Available from: http://www.pwc.com/Extweb/onlineforms.nsf/docid/B169B64B3AF67550CA25756F00151FEB/$file/Governance_Mar09.pdf [Accessed 23 Apr 2009].
60. Mitchell, S.L. & Holst, S. (2006): Building a Bridge to Support Business Objectives. Business Trends Quarterly, 2006/3, pp.22-24.
61. Mitchell, S.L. (2007a): GRC – More than three letters. Available from: http://grc360.blog.oceg.org/2007/08/grc-more-than-three-letters.html [Accessed 14 Apr 2009].
62. Mitchell, S.L. (2007b): IT and GRC: A Crucial Partnership. In: GRC 360°, 2007/2, pp.13-16.
63. Mitchell, S.L. (2007c): GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance, 4/4, pp.279-296.
64. Moscaritolo, A. (2009): Governance, risk management and compliance: Putting it together. SC Magazine, 2007/3. Available from: http://www.scmagazineus.com/Governance-risk-management-and-compliance-Putting-it-together/article/128314/ [Accessed 24 Apr 2009].
65. Musthaler, L. & Musthaler, B. (2007): Governance, risk management and compliance and what it means to you. Available from: http://www.networkworld.com/newsletters/techexec/2007/0507techexec1.html [Accessed 24 Apr 2009].
66. OCEG (2007): Findings from the OCEG GRC Strategy Study: How we develop, manage and evaluate GRC efforts. GRC360°, 2007/3, pp.9-16.
67. OpenPages (2007): General Compliance Management: Reducing the Cost and Complexity of Complying with Multiple Regulations. Available from: http://www.openpages.com [Accessed 23 Apr 2009].
68. Pohlman, M.B. (22007): Oracle Identity Management: Governance, Risk and Compliance, 2nd Edition. Implementing Multinational Regulatory Compliance. Lincoln: iUniverse.
69. PricewaterhouseCoopers (2004): Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. Available from: http://www.globalcompliance.com/pdf/PwCIntegrityDrivenPerformance.pdf [Accessed 17 Apr 2009].
70. PricewaterhouseCoopers (2005): 8th Annual Global CEO Survey. Bold Ambitions, Careful Choices. Available from: http://www.pwc.ch/user_content/editor/files/publ_corp/pwc_8th_annual_global_ceo_survey_e.pdf [Accessed 14 Apr 2009] .
71. Purushottam, U., Gill, S., & Roongta, A. (2008): Integrated Controls Management – a cost effective approach to implementing GRC. FINsight, 2, pp. 55-60. Available from: http://www.infosys.com/FINsights/Finsights-financial-risk-with-Governance.pdf [Accessed 17 Apr 2009].
72. Rasmussen, M. (2006a): Enterprise Risk and Compliance Trends. Business Trends Quarterly, 2006/3, pp.36-38.

73. Rasmussen, M. (2006b): Overcoming Risk and Compliance Myopia. GRC Software Platform Market Landscape. Available from: http://logic.stanford.edu/POEM/externalpapers/grcdoc.pdf [Accessed 22 Apr 2009].
74. Rasmussen, M. (2006c): What’s My Line? Will the Real GRC Vendor Please Step Forward? GRC360°, 2006/2, pp.14-16.
75. Rasmussen, M. (2007): Hand in Hand. Business Trends Quarterly, 2007/2, pp.44-46.
76. Rasmussen, M. (2008): 2008 GRC Drivers, Trends, & Market Directions. Available from: https://www.distantmeasures.com/app/user/19/GRC.Perspectives%20-%20GRC%20Trends%202008.pdf [Accessed 23 Apr 2009].
77. Roland, H. (2007a): Using automated controls to ensure better, faster, cheaper audits. Financial Executive, 2007/11, pp.50-53.
78. Roland, H. (2007b): Balancing More than Just Books: Transforming the Role of a CFO. Business Trends Quarterly, 2007/4, pp.34-40.
79. Roland, H. (2007c): Finding the Right Controls for Success. Business Trends Quarterly, 2007/2, pp.36-42.
80. SAP AG (2006): An Integrated Approach to Managing Governance, Risk, And Compliance. Available from: http://www.zdnet.de/an_integrated_approach_to_managing_governance__risk__and_compliance_download-39002355-88007359-1.htm [Accessed 24 Apr 2009].
81. SAP AG (2007): Governance, Risk, and Compliance Management: Realizing the Value of Cross-Enterprise Solutions. Available from: http://www.findwhitepapers.com/whitepaper3679/ [Accessed 24 Apr 2009].
82. Schneider, G. (2008): Teil 2: SAP und der Themenkomplex GRC. IT-Sicherheit, 2008/5, pp.56-57.
83. Schöler, S. & Zink, O. (2008): Governance, Risk und Compliance mit SAP. Bonn: Galileo Press.
84. Sippy, N. (2007): Moving from reactive to strategic risk management. Business Trends Quarterly, 2007/3, pp.34-39.
85. Strong, T. & Javadizadeh, S. (2008): Issue and Incident Investigation. GRC360°, 2008/2, pp.18-19.
86. Switzer, C.S. (2007a): Ask the analysts: Where are we going with technology for GRC? GRC 360, 2007/1, pp.5-17.
87. Switzer, C.S. (2007b): Integration Innovation. Business Trends Quarterly, 2007/4, pp.26-32.
88. Switzer, C.S. (2007c): Fragmented GRC is Risky Business. Business Trends Quarterly, 2007/3, pp.40-42.
89. Switzer, C.S. (2008): Ask the Analysts: Chris McClean, John Haggerty and Michael Rasmussen. GRC360°, 2008/2, pp.24-26.
90. Switzer, C.S. & Hovis, J.J. (2008): CFO at the center. Available from: http://www.oracle.com/solutions/corporate_governance/oceg-critical-conversations-cfo-at-the-center-white-paper.pdf [Accessed 22 Apr 2009].
91. Tapscott, D. (2006): Trust and Competitive Advantage: An Integrated Approach to Governance, Risk & Compliance. Available from: http://www.findwhitepapers.com/whitepaper1714/ [Accessed 24 Apr 2009].
92. Tarantino, A. (2008): The Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices. Indianapolis: Wiley.
93. Taylor, S. (2007a): Resolving GRC Challenges with Resolver. Business Trends Quarterly, 2007/4, pp.42-43.
94. Taylor, S. (2007b): Whatever You Do, Don’t Work On Compliance. Business Trends Quarterly, 2007/2, pp.32-33.
95. Taylor, S. (2008): Service, please! Business Trends Quarterly, 2008/3, pp.74-76.
96. Teach, E. (2009): What We Talk about When We Talk about GRC. CFO Magazine, 2009/1, p.77.
97. Uppaladinni, R. & Chhawchharia, V. (2008a): Leveraging SaaS to manage GRC. FINsights, 2, pp.66-70. Available from: http://www.infosys.com/FINsights/Finsights-financial-risk-with-Governance.pdf [Accessed 17 Apr 2009].
98. Uppaladinni, R. & Chhawchharia, V. (2008b): Towards Assuring Enterprise-wide Compliance. SETLabs Briefings, 6/3, pp. 47-52.
99. Vemuri, A. (2008): Strategic themes in Risk and Compliance. FINsights, 2, pp.2-5. Available from: http://www.infosys.com/FINsights/Finsights-financial-risk-with-Governance.pdf [Accessed 17 Apr 2009].
100. Walker, S. & Rodriguez, R. (2008): GRC Strategic Agenda: The Value Proposition of Governance, Risk and Compliance. Available from: http://www.aberdeen.com/summary/report/benchmark/4519-RA-governance-risk-compliance.asp [Accessed 23 Apr 2009].
101. Wechsler, P. (2007): The GRC Harmony. Treasury & Risk, 2007/6, p.13.
102. Welu, T. (2007): The Ins & Outs Of GRC. Business Trends Quarterly, 2007/2, pp.20-23.

103. Wilhide, K. (2007): Oracle and SAP: Parallel Paths to GRC Supremacy. Available from: http://www.oracle.com/corporate/analyst/reports/ent_apps/erp/oracle-and-sap-parallel-paths-to-grc-supremacy.pdf [Accessed 08 Jul 2008].

104. Wilhide, K. & Hurwitz, D. (2008): How to stop worrying & embrace compliance. Business Trends Quarterly, 2008/2, pp.94-98.

105. Williams, P. (2007): The case for converging governance, risk and compliance. Available from: http://www.s12498.gridserver.com/news/The%20case%20for%20converging%20GRC.pdf [Accessed 24 Apr 2009].

106. Wilson, R. (2007): The 2006 GRC Index. Business Trends Quarterly, 2007/1, pp.52-54.

107. Wyszkowski, A. (2008): Managing Compliance Requirements. GRC360°, 2008/2, pp.20-21.

Appendix C – GRC vendor survey questionnaire

ANONYMISED MINI-SURVEY: GRC SOFTWARE ARCHITECTURES TODAY AND TOMORROW

Launched in 2008, ANONYMISED helps educate companies and the academic world about the integrated approach to Governance, Risk & Compliance. The mini-survey „GRC software architectures today and tomorrow" is conducted in order to offer GRC software vendors and industry experts a platform to promote their understanding of GRC – what GRC is today, and where it is heading in the future. The answers are going to be published on ANONYMISED. Similarities and differences are going to be outlined in research based on the answers. The survey consists of only 10 open-ended questions that enable you to elaborate on your point of view. Feel free to attach figures and documents. Please understand if you should receive follow-up questions on details of interest. The survey is conducted by ANONYMISED, who you can feel free to contact at ANONYMISED in case you have questions.

Survey Questions

1. How does your company define the term “GRC”?
2. How do you see the relation between Enterprise Risk Management (ERM) and GRC?
   Are they synonyms?
3. Please describe the software architecture of your company’s GRC portfolio.
   What are the components? How do they interact? How closely are they integrated? Same data model? Same interface? Single application? ...
4. Are you trying to deliver a complete GRC solution covering all aspects of GRC, or are you focusing on certain aspects only? Which GRC capabilities are you delivering?
   e.g. audit management, risk assessment, risk reporting, access control...
5. What is your GRC software’s unique selling point compared to competitor products?
   Please explain why only your software can deliver this advantage.
6. What are the top five benefits your customers gain when employing your GRC solution?
7. As a rule of thumb, which GRC applications and technologies would you centralise?
   Where would you apply single, company-wide solutions?
8. Which areas of your GRC portfolio are you especially trying to improve / further develop in the near future?
9. What is your company’s vision of an ideal GRC process / technology setup in the future?
   How does your vision differ from GRC process and technology landscapes in organisations today?
10. What do you consider to be the key technologies employed in GRC in the future?

Finally, please let us know in how far you agree with the publication of your answers:

a. Complete publication on grc-resource.com and in related research publications.
b. Anonymous inclusion on grc-resource.com and in research publications, anonymised quotes allowed.
c. Anonymous inclusion on grc-resource.com and in research publications without direct quotes.

Please send your answers in the format of your choice to info@grc-resource.com.

Appendix D – Results from survey among large organisations

Results from survey of 48 large enterprises; might not add up to 100% due to rounding.

#	Statement	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
S1	My organisation has a central GRC department or team.	27%	17%	31%	15%	10%
S2	My organisation takes a siloed approach to governance, risk, and compliance.	17%	31%	25%	25%	2%
S3	My organisation attaches importance to an integrated GRC approach.	6%	31%	42%	13%	8%
S4	In my organisation GRC is reported to executives in an integrated manner.	13%	27%	21%	31%	8%
S5	We use results from GRC monitoring for planning.	15%	44%	35%	6%	0%
S6	My organisation implements GRC activities on a uniform IT platform.	8%	21%	23%	33%	15%
S7	My organisation uses a separate compliance software solution.	38%	35%	19%	2%	6%
S8	My organisation uses a separate risk management software solution.	31%	33%	27%	8%	0%
S9	My organisation uses a standard software solution for GRC.	8%	6%	33%	23%	29%
S10	My organisation uses a GRC software solution.	13%	33%	27%	25%	2%
S11	My organisation uses an in-house developed software solution for GRC.	13%	27%	44%	10%	6%
S12	My organisation does not attribute importance to GRC software solutions, as they are a pure cost factor.	0%	4%	19%	29%	48%
S13	An integrated approach to GRC has more disadvantages than advantages.	2%	2%	23%	58%	15%
S14	GRC links daily operations to strategic objectives.	17%	44%	38%	2%	0%
S15	GRC helps analyse risks and thus creates competitive advantage.	19%	54%	21%	6%	0%
S16	Integrated GRC management gives an overview of all risks an organisation faces.	23%	58%	19%	0%	0%
S17	GRC does not improve risk prevention.	2%	4%	19%	50%	25%
S18	GRC software solutions enable an organisation-wide view of GRC processes.	8%	44%	35%	10%	2%
S19	GRC software solutions help recognise dependencies of different risks.	8%	46%	29%	15%	2%
S20	GRC software solutions do not help recognise dependencies between risks and regulations.	0%	8%	46%	40%	6%
S21	Investments in GRC software are higher than the resulting benefits.	0%	6%	52%	33%	8%
S22	Deploying a GRC software solution is of no benefit to the organisation.	0%	0%	42%	44%	15%
S23	The lack of an integrated GRC software platform	13%	58%	15%	6%	8%

	would make risk management more difficult.					
S24	Standard reports from GRC software solutions are insufficient.	19%	38%	33%	10%	0%
S25	Without an integrated GRC software platform we could not manage compliance as effectively.	13%	50%	25%	10%	2%
S26	GRC software solutions help automate documentation and reporting.	8%	50%	27%	10%	4%

Appendix E – IT GRC integration study questionnaire

1. **The three disciplines IT governance, IT risk management, and IT compliance**
   For each of the three disciplines...
   1.1. Strategy
   - Does your organization promote a common understanding of the term through a documented definition? If so, what is the definition?
   - Do you follow external standards?
   - Do you follow internal policies and / or procedures? Are they related to externals standards?

   1.2. Process
   - Do you have a formalised process in place? Please describe it.
   - If the process is informal, which activities would you count towards it?
   - What frequency are the processes carried out at?

   1.3. People
   - Which organisational entities are involved?
   - Which organisational roles have been defined?

   1.4. Technology
   - Have you deployed software to support the respective discipline? If so...
     - What is the name of the software?
     - What applications does it consist of?
     - Which processes does it support?
     - Who uses it?
     - What data is used and where is it stored?

2. **Integration of governance, risk, and compliance**
   2.1. Strategy
   - Is the acronym “GRC” used in your organisation?
     - If so, what does it refer to (software, department name, strategy...) and how is it defined?
   - Has your organisation deliberately addressed the integration of IT governance, IT risk management and IT compliance?

- Is there a strong interest in leveraging IT GRC synergies in your organisation? If so, why?
- Does your organisation follow a standard for IT GRC?

2.2. Process

- If there is a formalised IT governance process, in how far does it interact with IT risk management processes (e.g. use results from risk assessments, influence the internal environment for risk management...)?
- If there is a formalised IT governance process, in how far does it interact with IT compliance processes?
- Are IT risk management and IT compliance processes integrated?
    - Is the risk of non-compliance considered in IT risk management?
    - Do you use risk-based approaches to compliance (e.g. in audits)? Do they draw on results from risk management?
- If in place, which benefits to the integrated processes deliver?

2.3. People

- Are the topics of IT governance, IT risk management, and IT compliance managed by a central body within your organisation?
- Are there employees that are involved in both IT governance and IT risk management? What are their roles?
- Are there employees involved in both IT governance and IT compliance? What are their roles?
- Are there employees involved in both IT risk management and IT compliance? What are their roles?

2.4. Technology

- Have you deployed “integrated GRC” software to help manage your IT processes? If so...
    - What is the name of the software?
    - What applications does it consist of?
    - Which processes does it support?
    - Who uses it?
    - Which benefits has the deployment delivered?

3. **Relation of GRC and IT GRC**

   On each of the levels of strategy, processes, people and technology...

   - Is there a link between corporate governance and IT governance in your organisation?
   - Is IT risk management performed as a part of enterprise risk management?
   - Are non-IT Compliance initiatives linked to IT compliance?
   - In case your organisation promotes integrated GRC, how is IT GRC aligned with it?

Appendix F – Mapping of ISACA Risk IT to COSO ERM

Mapping of ISACA Risk IT processes to COSO ERM components. “Risk communication” and “Risk culture” in the RITF are not part of the process model, but they are separately described in the framework document and have therefore been added. The wording of two mapped components might be very different, especially since the COSO components have very general names and sometimes include a variety of processes in their description. Each of the three researchers involved first did the mapping on his own using the COSO ERM and ISACA Risk-IT process descriptions. Results were then merged and discrepancies were discussed until a joint decision could be taken.

COSO ERM Framework	ISACA Risk IT Framework
01 Internal environment	
01.01 Risk management philosophy	
01.02 Risk appetite	
01.03 Risk culture	RG1.5 Promote IT risk-aware culture
	Risk Culture
01.04 Board of directors	
01.05 Integrity and ethical values	
01.06 Commitment to competence	
01.07 Management philosophy and operating style	
01.08 Organisational structure	
01.09 Assignment of authority and responsibility	RG2.1 Establish and maintain accountability for IT risk management
	RG2.4 Provide adequate resources for IT risk management
01.10 Human resource policies and practices	
01.11 Differences in environment	
02 Objective setting	RE2.1 Define IT risk analysis scope
02.01 Strategic objectives	
02.02 Related objectives	RG2.4 Provide adequate resources for IT risk management
02.03 Selected objectives	
02.04 Risk appetite	RG3.3 Embed IT risk considerations in strategic business decision making
02.05 Risk tolerance	RG1.2 Propose IT risk tolerance thresholds
	RG1.3 Approve IT risk tolerance
03 Event identification	
03.01 Events	RE3.4 Update IT risk scenario components
03.02 Factors influencing strategy and	RE3.5 Maintain the IT risk register and IT risk

objectives	map
03.03 Methodology and techniques	RE3.6 Develop IT risk indicators
03.04 Event interdependencies	RE1.3 Collect data on risk events
03.05 Event categories	RE1.4 Identify risk factors
03.06 Risks and opportunities	RR1.4 Identify IT-related opportunities
04 Risk assessment	RG1.1 Perform enterprise IT risk assessment
04.01 Inherent and residual risk	RG3.4 Accept IT risk (= accept residual risk)
04.02 Likelihood and impact	RE2.2 Estimate IT risk
	RE3.1 Map IT resources to business processes
	RE3.2 Determine business criticality of IT resources
04.03 Qualitative and quantitative methodologies and techniques	RE1.1 Establish and maintain a model for data collection
	RE1.2 Collect data on the operating environment
04.04 Correlation	
05 Risk response	
05.01 Identify risk responses	RE2.3 Identify risk response options
05.02 Evaluate possible risk responses	RR1.3 Interpret independent IT assessment findings
05.03 Select response	RR3.1 Maintain incident response plans
	RR3.3 Initiate incident response
05.04 Portfolio view	
06 Control activities	
06.01 Integration with risk response	RR2.1 Inventory controls
06.02 Types of control activities	RR2.3 Respond to discovered risk exposure and opportunity
06.03 General controls	RR2.4 Implement controls
06.04 Application controls	
06.05 Entity-specific	
	RR3.2 Monitor IT risk
	RR2.2 Monitor operational alignment with risk tolerance thresholds
08 Monitoring	
08.01 Ongoing	
08.02 Separate evaluations	RG2.5 Provide independent assurance over IT risk management
08.03 Reporting deficiencies	
07 Information and communication	
07.01 Information	
07.02 Strategic and integrated systems	
07.03 Communication	RR2.5 Report IT risk action plan progress
	RR3.4 Communicate lessons learned from risk events
	RR1.1 Communicate IT risk analysis results
	RR1.2 Report IT risk management activities and state of compliance
	RG1.6 Encourage effective communication of IT risk
	RG1.4 Align IT risk policy
	Risk Communication

Appendix G – Publications of the author

The most important publications are marked in bold.

Racz, N., Weippl, E. & Seufert, A. (2010): A frame of reference for research of integrated Governance, Risk & Compliance (GRC). In: Bart De Decker, Ingrid Schaumüller-Bichl (Eds.), *Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings*. Berlin: Springer, pp. 106-117.

Racz, N., Weippl, E. & Seufert, A. (2010): A process model for integrated IT governance, risk, and compliance management. In: J. Barzdins & M. Kirikova (eds.), Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010. Riga: University of Latvia Press, pp. 155-170.

Racz, N., Weippl, E. & Seufert, A. (2010): Questioning the need for seperate IT risk management frameworks. In: K.-P. Fähnrich, B. Franczyk (eds.), Lecture Notes in Informatics (LNI) P-176, Informatik 2010 Proceedings, Band 2. Bonn: Gesellschaft für Informatik, pp. 245-252.

Racz, N., Panitz, J.C., Amberg, M., Weippl, E. & Seufert, A. (2010): Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a survey among large enterprises. In: ACIS 2010 Proceedings, Paper 21. Retrieved 13 December 2010 from: http://aisel.aisnet.org/acis2010/21

Racz, N., Weippl, E. & Seufert, A. (2011): 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, HICSS 2011. IEEE.

Racz, N., Weippl, E. & Seufert, A. (2011): Integrating IT Governance, Risk, and Compliance Management Processes. In: J. Barzdins & M. Kirikova (eds.), Databases and Information Systems VI. Selected Papers from the Ninth International Baltic Conference, DB&IS 2010. Amsterdam: IOS Press, pp. 325-338.

Racz, N., Weippl, E. & Bonazzi, R. (2011): IT Governance, Risk & Compliance (GRC) Status Quo and Integration. An Explorative Industry Case Study. In: Proceedings of the 1st International Workshop on IT Governance, Risk and Compliance, ITGRC 2011. IEEE.

Curriculum Vitae

Personal Data:

Name:	Nicolas Racz
Email:	nracz@grc-resource.com
Born:	25 July 1983 in Kelheim, Germany
Nationality:	German

Education:

10/2007 – 03/2011: Doctorate, Vienna University of Technology
Topic: Integrated Governance, Risk & Compliance (GRC)
www.grc-resource.com

10/2003 – 07/2007: Information Systems Studies, Stuttgart Media University, Stuttgart

1993 – 2002: Von-Müller-Gymnasium, Regensburg

Exchange semesters:

09/2006 – 01/2007: University of Bath / School of Management, United Kingdom
Studies: Business Administration

03/2006 – 06/2006: Haute Ecole d'Ingénierie et de Gestion, Lausanne, Switzerland
Studies: Gestion des technologies de l'information (IT Management)

Work experience:

03/2011 – present: Business Analyst: Arthur D. Little Austria GmbH

07/2010 – 09/2010 & Consultant: SAP Deutschland AG & Co. KG
04/2009 – 12/2009: Consulting Financials I, Walldorf

- Development tasks in an SAP BI project at European Central Bank in Frankfurt
- Analysis of SAP's order-to-cash cycle; key performance indicator definition and data preparation
- Evaluation of internal perspectives for GRC and consulting opportunities
- Acquisition of basic knowledge of SAP-BO Business Planning & Consolidation

07/2007 – 02/2008: Consultant: BASF AG, Global IT Governance
Integrated Global Reporting, Ludwigshafen

- Development of a global corporate performance management strategy for the BASF group
- Conception and management of a proof of concept using scenarios of global controlling
- Definition of the technical corporate performance management framework using SAP BI
- Overview of BI solutions of seven software vendors as part of the evaluation

03/2007 – 06/2007: Diploma thesis: „Microsoft and SAP BI Solutions in Business Intelligence Scenarios within Roche Diagnostics“, Basel

09/2005 – 02/2006 & Internships: Hoffmann-LaRoche Ltd., Diagnostics Division
08/2006 – 09/2006: Global SAP Program Management, Basel

- Third level support of the global SAP Business Information Warehouse
- SAP training: BW305 – Reporting & Analysis

08/2004 – 12/2004: Student worker: Informationsmanagement GmbH, Stuttgart

- Implementation of two pilot web-projects for T-Systems

06/2003 – 07/2003: Shift work: OSRAM Opto Semiconductors, Regensburg

07/2002 – 03/2003: Military service: Communications soldier, Cham and Regensburg

04/2000 – 07/2001: Internet guide / basketball expert: Clickfish.com GmbH

Own Projects:

05/2010 – present: Development of the prediction game tennis-prophet.com

- conceptual design; implementation instructing an Argentine web development company (Go-Live 05/2011)

04/2000 – present: Founder and manager of the fan community Sportforen.de

- Administration of the community holding over 13,000 registered members

10/1998 – present: Founder and manager of Crossover-Online.de, Germany's largest basketball website

- Team lead for about 25 editors, programmers and designers
- Accounting, sales, public relations and management of partners

02/2010 – 07/2010: Publisher of the basketball print magazine "Crossover"

- Project lead publishing the German 80-page magazine (print run 5,000)

01/2001 – 12/2004: Online shop: import and sale of basketball trading cards

Publications:

- A frame of reference for research of integrated Governance, Risk & Compliance (GRC).
  In: 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings. Springer.
- Integrating IT Governance, Risk, and Compliance Management Processes.
  In: Databases and Information Systems VI, DB&IS 2010 selected papers. IOS Press.
- Questioning the need for separate IT risk management frameworks.
  In: Proceedings of the Informatik 2010 Conference. Gesellschaft für Informatik.
- 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. AIS.
- GRC Software – An Exploratory Study of Software Vendor and Market Research Perspectives.
  In: Proceedings of the 44th Hawaii International Conference on System Sciences, HICSS 2011. IEEE.
- IT GRC Integration and Status Quo – An Exploratorive Industry Case Study.
  In: Proceedings of the 1st International Workshop on IT GRC, ITGRC 2011. IEEE.

Languages:

- German: native speaker
- English: business fluent
- French: very good knowledge; semester abroad in Lausanne
- Spanish: very good knowledge; two stays abroad in South America

Scholarships:

- Baden-Württemberg Scholarship, Erasmus, Free-Mover Scholarship, Stipendiary of e-fellows.net and students4excellence.at, TU Vienna PhD and merit grants

Hobbies and Interests:

Latin America:

- Language and cultural stays in Medellín, Colombia (02-03/2009) and Buenos Aires, Argentina (01-03/2010)
- Fund-raising drive for a Favela day-care centre in Brazil (2007)

Sports:

- Basketball in various clubs and on university teams
- In early life competitive Judoka, football player, table tennis player
- Passionate fan of basketball and football

Others:

- Literature, philosophy, politics