Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2010 Proceedings | Australasian (ACIS)

2010

Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from A Survey Among Large Enterprises

Nicolas Racz
Vienna University of Technology, racz@ifs.tuwien.ac.at

Johannes Panitz
Friedrich-Alexander University of Erlangen-Nuremberg, Johannes.Panitz@wiso.uni-erlangen.de

Michael Amberg
Friedrich-Alexander University of Erlangen-Nuremberg, amberg@wiso.uni-erlangen.de

Edgar Weippl
Vienna University of Technology, eweippl@ifs.tuwien.ac.at

Andreas Seufert
Steinbeis Hochschule Berlin, andreas.seufert@i-bi.de

Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises

Nicolas Racz[1], Johannes C. Panitz[2], Michael Amberg[2], Edgar Weippl[1], Andreas Seufert[3]

[1]Institute of Software Technology and Interactive Systems
Vienna University of Technology
Vienna, Austria
Email: racz@ifs.tuwien.ac.at, eweippl@ifs.tuwien.ac.at

[2]Chair of Information Systems III
Friedrich-Alexander University of Erlangen-Nuremberg
Nuremberg, Germany
Email: johannes.panitz@wiso.uni-erlangen.de, amberg@wiso.uni-erlangen.de

[2]Institute for Business Intelligence
Steinbeis Hochschule Berlin
Berlin, Germany
Email: andreas.seufert@i-bi.de

Abstract

The focus on governance, risk and compliance (GRC) is steadily increasing as companies are facing increased risk and a growing number of legal, regulatory and other compliance requirements. Enterprises start to emphasise the integration and automation of GRC activities in order to efficiently manage them. This research evaluates how integrated GRC and GRC software are perceived and applied in large enterprises. Through a survey among large enterprises several key findings are derived. Even though integrated GRC is deemed useful and integration efforts are ongoing, many companies are unsure about the importance of an integrated approach. Half of organisations have deployed integrated GRC software that helps leverage the benefits of GRC. Solutions developed in-house are more often used than standard solutions. Participants are unsatisfied with their current reporting solutions. The authors recommend actions for research to follow up on each of the findings.

Keywords

Governance, risk management, compliance, GRC, software

MOTIVATION

Corporate governance scandals, increased risk in the business environment and the introduction of countless new regulations have spurred an increased focus on companies‘ governance, risk and compliance (GRC) activities over the last decade (Frigo and Anderson 2009; Racz et al. 2010a). 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 et al. 2004) and lead to a duplication of efforts, redundant solutions, higher cost and increased risk. Most companies acknowledge that their GRC activities are not yet fully integrated (OCEG 2007).

Several experts argue that a holistic, integrated and strategic approach to GRC can add value and create competitive advantage (Chaterjee and 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). In this effort they often rely on software for governance, risk and compliance (Approva 2007). Specialised solutions can help achieve considerable improvements of GRC operations (Fisher 2007; Rasmussen 2007) through automation of management, work flow, documentation, testing and reporting of GRC activities. The importance of IT in supporting GRC processes is steadily increasing (Jackson 2007).

Despite the significance of GRC in business practice, scientific research on integrated GRC in general and on the use of GRC software in business in specific is scarce (Racz et al. 2010a). Having previously researched the GRC area from different perspectives based on publications and theory, the authors now wanted to gain an impression of GRC in business practice of large enterprises. They strived to identify the status quo of horizontal GRC

integration – the integration of the three disciplines with each other – and the role of software in enabling this integration in order to discover future research opportunities. The examination of related work in the subsequent section draws a picture of the current status of GRC research, and it points out hitherto insufficiently researched areas allowing for the derivation of this paper's research question.

PRIOR RESEARCH

Even though the term "GRC" was first mentioned in 2004 (PricewaterhouseCoopers 2004), scientific research has only recently started to examine the integrated approach to governance, risk, and compliance. 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 and Rosemann (2005), for instance). This paper focuses on the horizontal integration; consequently "integration" in the following refers to horizontal integration. Existing publications about integrated GRC are mostly driven by software vendors, consulting and auditing companies, and market analysts (Racz et al. 2010a). Racz et al. (2010a) developed the so far sole scientifically derived and validated GRC definition: "*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.*" The same authors created an integrated process model for IT governance, risk, and compliance management (Racz et al. 2010b). In addition, Marekfia and Nissen (2009) suggest a conceptual reference framework for strategic GRC management. Both neither related their model to integrated GRC software, nor did they validate the concepts.

As far as research on integrated GRC software is concerned, Racz et al. (2010c) conducted a survey among vendors of GRC platforms. Among other points the research study highlighted that while vendors share a common understanding of GRC in general and while they agree on the benefits delivered by GRC, their perceptions of GRC functionality are diverse and their tools differ in the degree of integration. Vendors also have a more constricted view on the GRC domain than market research companies do. These companies provide studies and evaluations of GRC software. Gartner Research and Forrester Research publish yearly software rankings (Caldwell et al. 2009, McClean 2009) thus giving an overview of the GRC software market. Besides these software rankings the market research companies have developed various GRC frameworks and reference models. AMR Research published a GRC framework in 2008 (Hagerty et al. 2008), which it used to compose vendor-specific software analyses. The analysts also provide high-level research of GRC software portfolios in general (Caldwell 2008, Proctor et al. 2008, McClean et al. 2009). However all the market research publications are vendor centric. They do not provide insights on the actual use of integrated GRC in business practice.

Other GRC publications that are neither from scientific nor market research include the work of the Open Compliance and Ethics Group (OCEG) that provides reference models for GRC processes (OCEG 2009a) and software (OCEG 2009b). Further process models for GRC with little or no relation to software have been provided by Paulus (2009), Frigo and Anderson (2009), Tapscott (2006) and by OCEG chairman Mitchell (2007), who describes his idea of GRC as a means to achieve "principled performance" – i.e. attaining objectives while respecting mandatory and voluntary boundaries.

Evidently prior research has already suggested reference models for GRC processes and it has evaluated GRC software from a functional point of view. However the deployment and use of integrated GRC software have not been examined so far. Furthermore no empirically based insights into end-user requirements exist. The research at hand represents a first step towards closing this gap, answering the research question: *How are integrated GRC and GRC software perceived and applied in large enterprises?*

RESEARCH METHODOLOGY

The methodology applied in our research consists of three phases: survey design, survey execution, and survey analysis.

In the survey design phase we first agreed on a common understanding of GRC, relying on the definition cited above (Racz et al. 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.

As we had already gained attention through prior research activities in German-speaking countries, the survey was targeted towards professionals based in these 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 1.

Table 1: 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 et al. 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 (Schnell et al. 1999).

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 the authors generally focus on GRC in large enterprises in their research. A complete list of the statements and answers per Likert category in percent is attached below in appendix 1. The results were used to derive five key findings (KF). Each finding was based on a distinct set of answers (see Table 2). The key findings are described in the results section.

Table 2: 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

RESULTS

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 suggests examining GRC integration within and across four components: strategy, processes, people (the organisational structure) and technology (Racz et al. 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.

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 et al. 2010a) or stakeholder satisfaction and potential benefits (Marekfia and 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 and 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.

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 et al. 2010c). 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.

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.

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 organizations 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).

Summary

Figure 1 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.

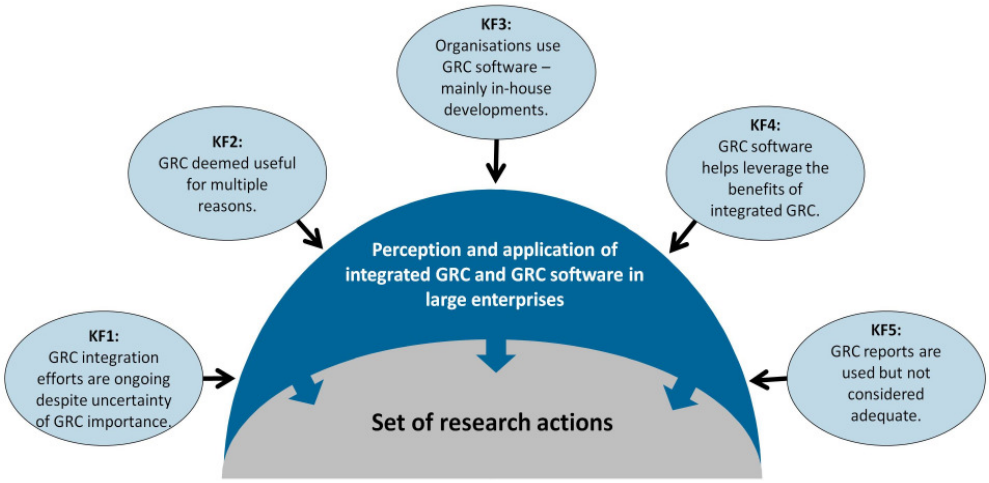

Figure 1: The five key findings of the study

DISCUSSION

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

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.

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?

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.

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.

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.

Figure 2 summarises the recommended actions for research.

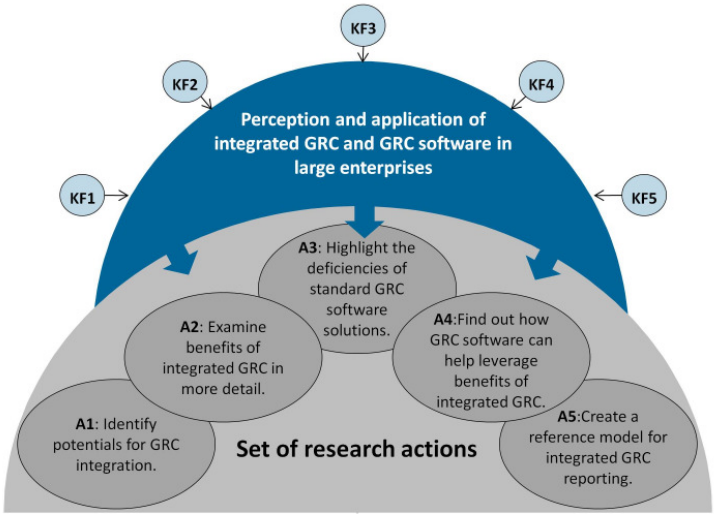

Figure 2: Overview of research actions

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.

The paper at hand contributes to information systems research. Following the information systems research framework (Hevner 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 represent a first step in understanding 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.

CONCLUSION AND FUTURE RESEARCH

Through a survey we discovered findings concerning the perception and application of integrated GRC and GRC software in large enterprises. 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 future research we are going to follow up some of the recommended actions. 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 and we will elaborate on potentials for integration. In the course of that study we will also validate a formerly created process model for IT GRC management; that model will then serve as a basis in the creation of a technology reference model for GRC software. Moreover we are going to deepen the research on GRC reporting in suggesting a reference structure and contents for integrated reports, and improvements that enable currently insufficient software solutions to deliver these reports.

REFERENCES

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

Approva 2007. "2007 Approva GRC Survey." Retrieved 10 December, 2009, from http://www.approva.com/survey

Caldwell, F. 2008, "The Enterprise Governance, Risk and Compliance Platform Defined." Retrieved 18 April, 2010, from http://www.gartner.com/DisplayDocument?doc_cd=155196

Caldwell, F., Eid, T., and Casper, C. 2009. "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms." Retrieved 18 April, 2010, from http://paisley.thomsonreuters.com/website/pcweb.nsf/pages/ARAE-6XANSY

Chaterjee, A. and Milam, D. 2008. "Gaining Competitive Advantage from Compliance and Risk Management." D. Pantaleo, and N. Pal (eds.), *From Strategy to Execution - Turning Accelerated Global Change into Opportunity*, Berlin: Springer.

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

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

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

Frigo, M.L., and Anderson, R.J. 2009. "A Strategic Framework for Governance, Risk, and Compliance," *Strategic Finance* (44:1), February, pp 20-61.

Hagerty, J., Verma, K., and Gaughan, D. 2008. "The Governance, Risk Management, and Compliance (GRC) Landscape, Part 2: Software's Integral Role in GRC Automation." Retrieved 21 April, 2010, from http://www.acl.com/pdfs/AMR_Research__Governance_Risk_Management_2.pdf

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

Jackson, R. 2007, "The future is now, Cutting Edge Technology for GRC" *Inside Counsel*, (17:1), June. Retrieved 21 April 2010 from http://www.oceg.org/view/18808

Marekfia, W., and Nissen, V. 2009. "Strategisches GRC-Management – Grundzüge eines konzeptionellen Bezugsrahmens." *Forschungsberichte zur Unternehmensberatung* (2009:2), November. Retrieved 7 May, 2010, from http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-18253/FUB-2009-01.pdf

McClean, C. 2009. "The Forrester Wave: Enterprise Governance, Risk, And Compliance Platforms, Q3 2009." Retrieved 21 April, 2010, from http://www.openpages.com/Information-Center-Registration/Campaign_36.asp

McClean, C., McNabb, K., and Dill, A. 2009. "The GRC Technology Puzzle: Getting all the Pieces to Fit." Retrieved 21 April, 2010, from http://www.forrester.com/rb/Research/grc_technology_puzzle_getting_all_pieces_to/q/id/45772/t/2

Menzies, C. 2006. *Sarbanes-Oxley und Corporate Compliance - Nachhaltigkeit, Optimierung, Integration.* Stuttgart: Schäffer-Poeschel.

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

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

OCEG 2007. "Key findings report The 2007 GRC Strategy Study" Retrieved 14 April, 2010, from http://www.oceg.org

OCEG 2009a. "GRC Capability Model. Red Book 2.0." Retrieved 14 April, 2010, from http://www.oceg.org

OCEG 2009b. "GRC-IT Blueprint. Version 1.0." Retrieved 14 April, 2010, from http://www.oceg.org

Panitz, J.C., Wiener, M. and Amberg, M. 2010. „A Balanced Scorecard for Compliance – requirements of a comprehensive compliance reporting." Accepted at the 16th Americas Conference on Information Systems 2010.

Paulus, S. 2009. "A GRC reference architecture. Overview report." Retrieved 21 April, 2010, from http://www.kuppingercole.com/report/sp_overview_repo_grc_arch_051009

PricewaterhouseCoopers 2004. "Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management." Retrieved 7 May, 2010, from http://www.globalcompliance.com/pdf/PwCIntegrityDrivenPerformance.pdf

Proctor, P.E., Caldwell, F., and Eid, T. 2008. "A Comparison Model for the GRC Marketplace, 2008 to 2010." Retrieved 18 April, 2010, from http://www.gartner.com/DisplayDocument?id=712207

Racz, N., Weippl, E., and Seufert, A. 2010a. "A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)," *Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings.* Berlin: Springer, pp 107-116.

Racz, N., Weippl, E., and Seufert, A. 2010b. "A Process Model for Integrated IT Governance, Risk & Compliance Management," *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., and Seufert, A. 2011. "GRC software as seen by software vendors and market research," *Accepted at the 44th Hawaiian International Conference on System Sciences, 2011.*

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

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

Tapscott, D. 2006. "Trust and Competitive Advantage: An Integrated Approach to Governance, Risk & Compliance." Retrieved 18 April, 2010, from http://www.findwhitepapers.com/whitepaper1714/

Volonino, L., Gessner, G. H. and Kermis, G. F. 2004. "Holistic Compliance with Sarbanes Oxley," *Communications of the Association for Information Systems* (14:1), pp 219-233.

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

ACKNOWLEDGEMENTS

We thank Ülkühan Kapar for her support in conducting the survey. We also thank all survey participants.

APPENDIX 1

Table 2. Survey statements and results (48 large enterprises; results 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,	17%	31%	25%	25%	2%

	risk, and compliance.					
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 would make risk management more difficult.	13%	58%	15%	6%	8%
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%

COPYRIGHT