A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)

Nicolas Racz[1], Edgar Weippl[1], and Andreas Seufert[2]

[1] TU Vienna, Institute for Software Technology and Interactive Systems, Favoritenstr. 9-11, 1040 Vienna, Austria
{racz,eweippl}@ifs.tuwien.ac.at
[2] Steinbeis Hochschule Berlin, Institut für Business Intelligence, Gürtelstr. 29A/30, 10247 Berlin, Germany
Andreas.Seufert@i-bi.de

Abstract. Governance, Risk and Compliance (GRC) is an emerging topic in the business and information technology world. However to this day the concept behind the acronym has neither been adequately researched, nor is there a common understanding among professionals. The research at hand provides a frame of reference for research of integrated GRC that was derived from the first scientifically grounded definition of the term. By means of a literature review the authors merge observations, an analysis of existing definitions and results from prior surveys in the derivation of a single-phrase definition. The definition is evaluated and improved through a survey among GRC professionals. Finally a frame of reference for GRC research is constructed.

Keywords: governance, risk, compliance, GRC, integrated, definition.

1 Introduction and Motivation

The acronym "GRC" (governance, risk and compliance) has rapidly penetrated the business community over the last years. It has made its way into software labels, marketing slides and department names in global enterprises. In the early days of GRC, PricewaterhouseCoopers [1] 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." In the authors' opinion 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" [2] to a degree that it was even recommended to avoid definitional debates [3]. This is partly owed to the lack of a scientifically grounded definition; instead software vendors and consultants publish definitions 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 [4] – and an already strong impact today. In 2008 about 40 billion

B. De Decker and I. Schaumüller-Bichl (Eds.): CMS 2010, LNCS 6109, pp. 106–117, 2010.

US-dollars were spent on services, technology and content related to GRC [5]. The business network LinkedIn lists close to 4,000 GRC professionals. Do they really work in a blurred, intangible domain? Researchers and professionals in IS security view GRC as a means to draw the attention of management to information security and to make its benefits understandable and tangible for business people.

This research was carried out in order to develop a frame of reference that supports GRC research in general and the creation of reference models for integrated GRC according to the process model for an empirically grounded reference model construction [6] in specific. 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. Our paper 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" [7].

2 Research Methodology

The methodology applied to carry out this research consists of four stages.

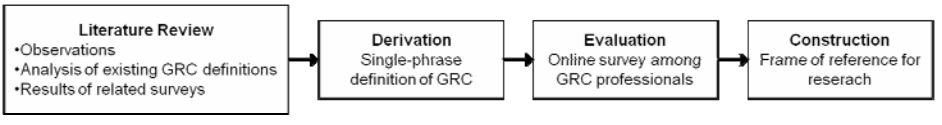

Fig. 1. Research methodology

The first stage is a review of GRC publications following the classifications of Fettke [8] 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	see "motivation" section
	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 "future research" section

Fig. 2. Publication review properties (based on 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 wanted to identify the meaning of GRC as a whole and not that of its fragments alone, we restricted 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. From the findings only those results were chosen that fulfilled 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. 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 were used in the derivation of a single-phrase working definition of integrated GRC.

In a third stage an anonymous online survey was 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. 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. 4% work for other types of organisations. 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 [6], the frame is a condensed high-level abstraction of a future reference model, created to support navigation within the problem domain of GRC. As proposed by Schlagheck [9] the frame of reference is developed early in parallel with the problem definition helping to scope GRC modelling and other research projects, to identify single model elements and to guarantee completeness.

3 Literature Review Results

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

3.1 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" [10, 11]. Both publications only provide short definitions of governance, risk management and compliance separately. O1 demonstrates the lack of research participation in GRC.

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.

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 organizations face" [12]. 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%.

O5: ERM is an important methodology within GRC. Inspired by the article "Is ERM GRC? Or Vice Versa?" [13] 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.

3.2 Literature Review – GRC Definitions

One in three of the analysed publications offers 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.

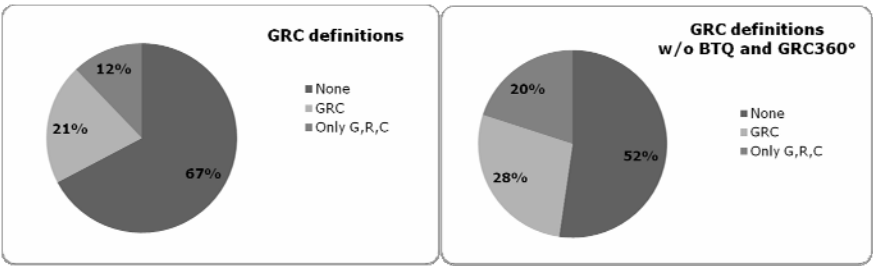

Fig. 3. GRC definitions in publications

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 [14] 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 [15, 16, 17]. 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 [13] 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 [18] 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 organization 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 [1, 19, 20]. Corporate Integrity

[21] goes as far as calling GRC a "philosophy of business" that "permeates the organization: its oversight, its processes, its culture." Mitchell [10] speaks of "principled performance", which is picked up by Hovis [22]: "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 [23] 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 organization 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 [16] 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 [24] and [25], 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) that technology is a key – but GRC is more than just technology, and (iii) that integrated GRC is supposed to improve the performance of processes.

3.3 Literature Review – Previous Surveys of 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%) [...]." [4]. This shows a more deliberate idea of GRC than the results gathered by Approva [26] 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 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.

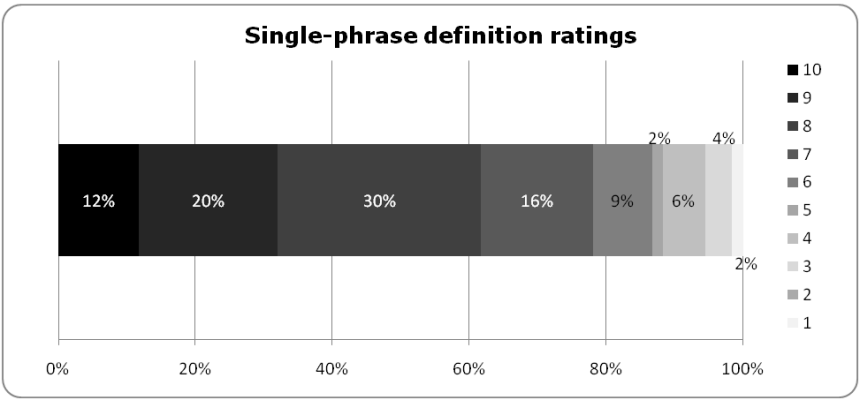

Fig. 4. Distribution of ratings of the single-phrase GRC definition

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.'

5 Construction of a Frame of Reference for 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.

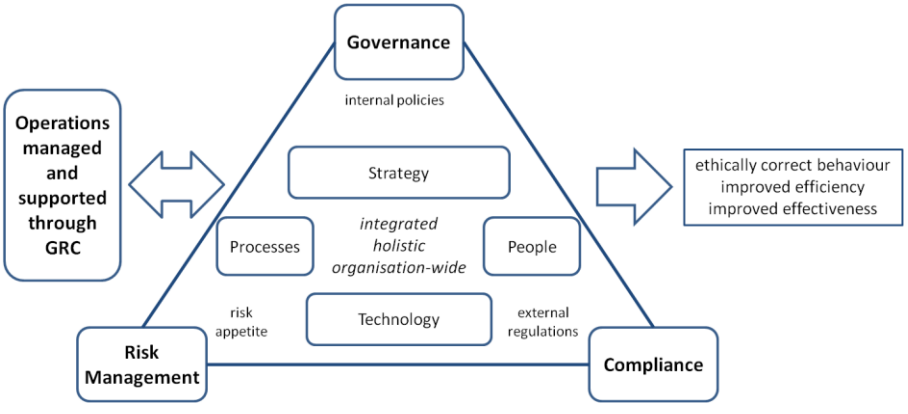

Fig. 5. Frame of reference for integrated GRC

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.

For information systems research another sub-category of GRC is of special interest: GRC processes that support the information technology operations of an organisation [27]. These GRC processes are commonly referred to as "IT GRC" [28].

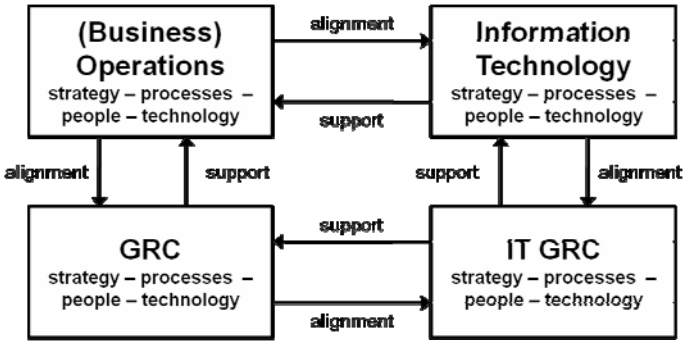

Fig. 6. GRC and IT GRC in the business and IT context

IT GRC deals primarily with issues of information security, IT compliance, IT and data governance, IT risk management and IT revision [29]. 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 above figure. 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; 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, 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.

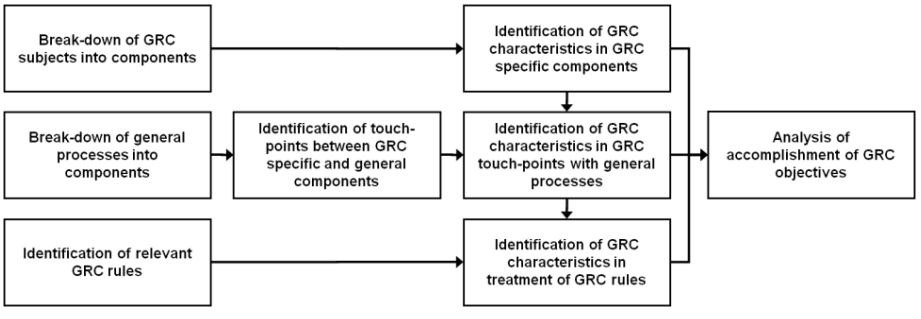

Fig. 7. Exemplary process model for integrated GRC research

6 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 fulfills its purpose.

The contribution of this research paper 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 modeling or other research of integrated GRC. The knowledge base of the information systems research framework [30] 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.

7 Conclusion and Future Research

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. In the near future we will try to enlarge the basis for GRC research by breaking down and describing the frame's components in order to create a research framework and reference model for integrated GRC in information systems management. 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.

References

1. PricewaterhouseCoopers: 8th annual global CEO survey, http://www.globes.co.il/Serve/Researches/documents/8thAnnualGlobalCEOSurvey.pdf
2. Leibs, S.: One for three. CFO Magazine (September 2007), http://www.cfo.com/article.cfm/9689509
3. Dittmar, L.: Demystifying GRC. Business Trends Quarterly 2(4), 16–18 (2007)
4. Kahn Consulting: GRC, E-Discovery, and RIM: state of the industry, http://www.kahnconsultinginc.com/library/KCI-GRC-RIM-EDD- survey.pdf
5. Rasmussen, M.: 2008 GRC drivers, trends & market directions, http://www12.sap.com/community/showdetail.epx?ItemID=11997

6. Ahlemann, F., Gastl, H.: Process Model for an Empirically Grounded Reference Model Construction. In: Fettke, P., Loos, P. (eds.) Reference Modelling for Business Systems Analysis, pp. 77–97. Idea Group, Hershey (2007)
7. Broady, D.V., Roland, H.A.: SAP GRC for dummies. Wiley, Indianapolis (2008)
8. Fettke, P.: State-of-the-Art des State-of-the-Art. Eine Untersuchung der Forschungsmethode 'Review' innerhalb der Wirtschaftsinformatik. Wirtschaftsinformatik 48/4, 257–266 (2006)
9. Schlagheck, B.: Object-oriented reference models for process and project controlling. In: Foundation-construction-fields of application. Deutscher Univ.-Verlag, Wiesbaden (2000)
10. Mitchell, S.L.: GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance 4(4), 279–296 (2007)
11. Tapscott, D.: Trust and competitive advantage: an integrated approach to governance, risk & compliance (2006), http://www.findwhitepapers.com/whitepaper1714/
12. Kelly, J.: Risk management surpasses compliance as top GRC priority, http://go.techtarget.com/r/3484977/6129174
13. Banham, R.: Is ERM GRC? Or vice versa? Treasury & Risk 2(6), 48–50 (2007)
14. Mitchell, S.L.: GRC – more than three letters, http://grc360.blog.oceg.org/2007/08/grc-more-than-three-letters.html
15. Hoffmann, M.: Governance, Risk und Compliance (GRC) – ein integrierter Ansatz. IM 24(1), 74–81 (2007)
16. Switzer, C.S.: Integration innovation. Business Trends Quarterly 2(4), 26–32 (2007)
17. Curran, B.: Defragmenting GRC. Pharmaceutical Technology 4(16), 20–23 (2007)
18. KPMG: Governance, risk, and compliance. Driving value through controls monitoring, http://www.kpmg.ca/en/services/advisory/documents/GovernanceRiskCompliance.pdf
19. Economist Intelligence Unit: Managing risk through financial processes. Embedding governance, risk and compliance, http://graphics.eiu.com/marketing/pdf/SAP%20GRC.pdf
20. Wechsler, P.: The GRC harmony. Treasury & Risk 2(6), 13 (2008)
21. Corporate Integrity: What is GRC?, http://www.corp-integrity.com/about/grc.html
22. Hovis, J.J.: CIO at the center, http://www.oracle.com/dm/08q3field/ogec_wp_cio.pdf
23. OCEG: GRC capability model. Red Book 2.0 (2009), http://www.oceg.com
24. Vemuri, A.: Strategic themes in risk and compliance. FINsights 2, 2–5 (2008)
25. Frigo, M.L., Anderson, R.J.: A strategic framework for governance, risk, and compliance. Strategic Finance 90(8), 20–61 (2009)
26. Approva Corporation: 2007 Approva GRC survey (2007), http://www.approva.net/survey
27. Teubner, A., Feller, T.: Informationstechnologie, Governance und Compliance. Wirtschaftsinformatik 50(5), 400–407 (2008)
28. IT Policy Compliance Group: 2008 Annual Report. IT Governance, Risk, and Compliance (2008), http://www.itpolicycompliance.com/pdfs/ITPCGAnnualReport2008.pdf
29. Rath, M., Sponholz, R.: IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Schmidt, Berlin (2009)
30. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Quarterly 28(1), 75–105 (2004)