Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies

Abbas Shahim, Ronald Batenburg, Geert Vermunt

Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies

Abbas Shahim[1], Ronald Batenburg[2] and Geert Vermunt[3]

[1] VU University Amsterdam, Amsterdam, The Netherlands &
Atos Consulting, Utrecht, The Netherlands
abbas.shahim@atos.net
[2] Utrecht University, Utrecht, The Netherlands
r.s.batenburg@uu.nl
3 BWise, Rosmalen, The Netherlands
geert.vermunt@bwise.com

Abstract. Governance, Risk and Compliance (GRC) has become critical for organizations and so is the need to support this by ICT. This paper positions GRC into an integrated strategic perspective, providing guidelines to assess maturity and defining paths for achieving strategic alignment. The approach is applied to two case studies, clarifying the organizations' GRC maturity "as is" and "to be". These cases were studied in the utilities and financial sectors, both show that organizations can have similar GRC maturity levels but follow quite different paths to achieve alignment with regard to GRC. While the Dutch utility company stuck to a path where the organizational strategy with respect to GRC was taken as a starting point, the financial institution followed a path in which the IT solution strategy was leading. In interpreting this result, it appears that the existing IT assets are strongly impacting the selection of the alignment path. More case studies are advocated to further validate the approach and contribute to optimize the strategic and integrated perspective on GRC.

Keywords: compliance, governance, risk management, strategic alignment

1 Introduction

From the turn of the millennium, the trusted face of our global economy familiar to many of us has deeply and rapidly changed. Its irreversible shape represents a strong compliance driven approach to business governance that has dominated the agenda of the board ever since. This fundamental and quick transformation is the result of the most known accounting scandals that occurred shortly after the beginning of this century: the collapse of Enron and the fall of WorldCom. As a response to these corporate failures, the Sarbanes-Oxley Act, often abbreviated to SOX (see [16] for further information), was created and passed by the United States Congress in 2002 to stress the importance of business control and auditing so that the national confidence in the securities markets was restored again. Compliance with this enacted legislation is not only required of organizations that are publicly traded in the United States, but is also

xxxx, p. x, 2012.

mandatory for those outside of the Unites States under certain circumstances (e.g., foreign companies listed on the New York stock exchange). In consequence, organizations have placed a great emphasis on description, design and effectively operating controls with the purpose to adequately govern, mitigate risks and comply with SOX [19] – see also [18]. In general, it can be stated that the tightened regulatory compliance pressure put on organizations especially by SOX has in fact given a boost to the improvement of the existing GRC practices in the business and information technology (IT) sector [7]. Nowadays, organizations are confronted with broader GRC-associated matters that have established a new reality in which traditional strategies and assumptions seem to fail [6] – see also [20].

GRC is not new. Issues and challenges with respect to governance, risk management and compliance have always formed a substantial concern for a majority of organizations. Although the abbreviation of this concept indicates an interrelation between its components, the fact is that these functions are yet executed mostly in a fragmented fashion [15]. What is new about GRC is the awareness of organizations to take a united perspective to this concept for creating added-value and realizing competitive advantage. It is rightfully noted that the need for an integrated approach to this concept should at least be fulfilled by sophisticated risk management frameworks, improved compliance disciplines, revamped structures and modern technologies so that an advanced as well as a sound governance on a corporate level can be practiced more readily. GRC as a set of integrated concepts can thus be of significant value and make a contribution to outpace the competition when applied holistically within organizations [14]. Hence, due to this organizational impact, it is necessary to strategize the interrelated GRC perspective and to ascertain that it will be aligned properly with the business mission. In practice, however, we hardly encounter the full convergence of GRC disciplines in theoretical strategic models. GRC implementations are largely based on pragmatic compliance-related activities, and on reporting about these dominating actions despite the clear need to embrace an incorporated and strategic GRC view across business units, oversight functions and strategies. This is the main driver of the present paper that addresses the research question: *How can an integrated GRC approach be applied in organizations using a strategic alignment perspective?*

The paper is organized as follows. Next, we present a brief overview of definitions of integrated GRC. Thereafter we show how a strategic alignment perspective on GRC results in an approach used to assess the GRC maturity and alignment paths. In the empirical part of the paper, the approach is applied to two different case studies. The results of both case studies are presented, leading to a conclusion that will be discussed in the final part of this contribution.

2 Integrated GRC

2.1 Definitions

Various definitions of GRC are provided in the literature (e.g., [21] – see also [3]). Using different point of views, the definitions mostly describe this concept in terms of

controlling and improving processes. A scientific GRC definition indicates the ethics in addition to other pertinent aspects such as risk appetite, internal policies and external regulations [14]. The definition presented by one of the Big Four accountancy firms describes that GRC is not a technology tool, but a model that leaders look at to drive maximum value out of the business model [6]. Throughout the rest of this paper, we refer to the GRC definition provided by the Open Compliance & Ethics Group (OCEG) for two main reasons. First, we notice that it is the one that is most referred to in the literature and in practice (e.g., [2], and [8] – see also [10] and [5]). Second, This global non-profit think tank expounds its view on an integrated approach to create a GRC system by means of four perspectives [33, 34]: 1) integration of GRC disciplines, 2) integration of GRC activities across risk categories and departments, 3) integration of GRC activities with business processes, and 4) integration to provide a single version of the truth. OCEG stresses the synergistic impact of an integrated approach to this concept and explains that it is more than solely the consolidation of three disciplines. It defines GRC as follows [9]: "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."

2.2 A Strategic Alignment Perspective

One of the key elements in the OCEG definition of GRC is the notion of alignment to achieve integration – of disciplines, activities and information. As a concept, alignment has a long history in both organization science and information systems research. Scholars in the 1990s already argued that companies fail to realize performance improvements due to the lack of alignment between the business and IT strategies [4]. Results of studies dedicated to measuring the effect of business-IT alignment on performance indicate that there is a positive correlation between business-IT alignment and organizational performance, in which top performers are those companies which effectively align their business with their IT strategies. This outcome comes to vitiate the claim that highly sophisticated IT can solely improve business performance, but what is of greater importance is the alignment between both IT and business strategies [17]. Following this line of argumentation, it can be expected that if an organization integrates GRC it will benefit more from IT if its applications are in conformance with the business processes present in the organization. In this context strategic or business-IT alignment implies the process of finding the right match and the alignment between a GRC solution and the organization. If this alignment perspective is applied to integrated GRC, a model can be defined as in figure 1. This model is based on the strategic alignment model of Henderson and Venkatraman [4] and positions an instance of the integrated GRC approach on both the business and on the IT dimension. The idea is that alignment can be realized by bringing the business

and IT strategy together, where strategy is involving formulation and implementation [4].

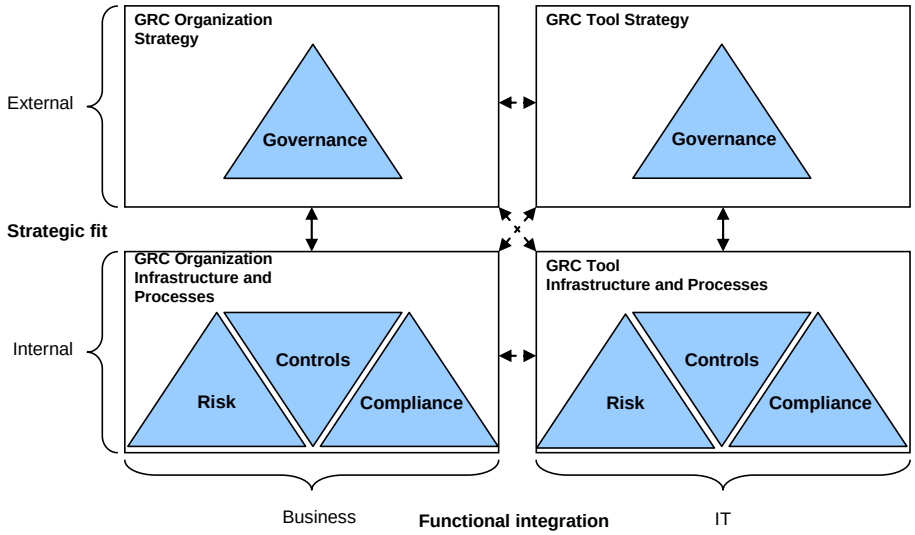

Fig. 1: GRC plotted in the strategic alignment model by [4]; the GRC strategic alignment model.

The vision of GRC from a strategic alignment perspective is plotted on the four domains from the strategic alignment model, based on the two building blocks defined by Henderson and Venkatraman: strategic fit and functional integration [4]. The strategic fit dimension represents the integration of the external and internal domain. The external domain, on a business level, addresses the arena in which corporate decisions are made concerning strategy and distinctive strategy attributes which distinguish the firm from competitors. The element 'Governance' is positioned in this domain because it is concerned with the GRC strategy in the organization. The internal domain, on a business level, pertains to the organizational structure and the critical business processes that are available in the organization. The elements of 'Risk', 'Control' and 'Compliance' are positioned in this domain because these elements relate to the structure of GRC and the processes involved with GRC, e.g. the risk-control structure in the organization. The fit between the external and internal domain in the business domain is argued to be critical when maximizing economic performance [1]. This relation can be reflected in the IT domain, resulting in a proposition that in the IT domain a similar separation between the external and internal domains can be made and that a fit between these domains is critical for IT in an organization [4]. Integrating the business and the IT domain is coined by Henderson and Venkatraman as functional integration. In the GRC perspective, the IT domain represents the GRC solution which forms a system of record for GRC in the organization. The strategic alignment model distinguishes two kinds of functional integration between the business and IT domain: strategic integration (i.e. attempts are made to align both

business and IT strategy) and integration of organization and processes (i.e. operational integration concerned with aligning infrastructure and processes on both business and IT level) [4]. Following the strategic alignment model of Henderson and Venkatraman, four alignment paths can be applied to the GRC domain illustrated in figure 2:

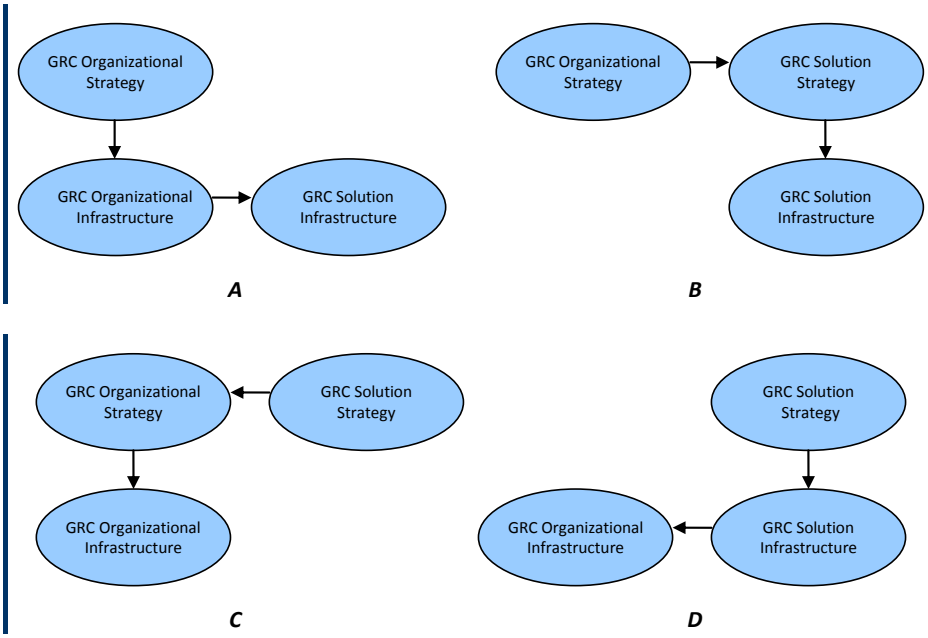

Fig. 2: Four paths to reach strategic alignment in GRC (A: Strategy execution, B: Technology transformation, C: Competitive potential, D: Service level).

1. The "strategy execution" path, translated to a GRC perspective, is displayed as "A". This path indicates that GRC strategy and GRC infrastructure are constructed in the business domain. A GRC solution is selected which could form a fit between the GRC infrastructure on both business and IT domain.
2. The "technology transformation" path for GRC is displayed as "B". In this perspective a GRC strategy is developed in a business domain and a GRC solution is selected which concurs with this strategy. The infrastructure from the GRC solution is embedded in the organization.
3. The "competitive potential" path, translated to a GRC perspective, is displayed as "C". In this path the strategy from the GRC solution is the driver. The GRC strategy and infrastructure in the business domain are geared towards the strategy which is adopted in the GRC solution.
4. The "service level" path for GRC is displayed as "D". In this case the vision of GRC adopted in the GRC solution is integrated in the GRC organizational infrastructure.

3 Methods and measurements

3.1 A GRC Framework

To operationalize and measure the GRC strategic alignment model as presented in figure 1, the next step needed is a specification of practices related to GRC and a maturity scale to measure these practices. For this aim, practices were distilled from the OCEG maturity models covering GRC. Governance includes 12 practices: code of conduct, strategy, organizational chart, accountabilities, meetings between accountable parties, process integration with business process, KPIs, reporting, budget, cost/benefit monitoring, transparency, and training. Risk holds 7 practices: risk assessment, risk overview, risk overview contains IT risks, risk review, incident reporting, emergency process for gaps and incidents, and root cause analysis for gap or incident. Compliance contains 4 practices: overview of regulatory boundaries, overview of internal and external rules and regulations, compliance review, and processes when confronted with non-compliance [36, 37, 38]. Table 1 provides our measurement framework and shows the proposed five-point scale for maturity levels to measure the three GRC domains.

Table 1: GRC domains and number of practices derived from OCEG [11], [12], [13].

Domain	**# Practices**	**Maturity levels**				
		1	2	3	4	5
Governance	12					
Risk	7					
Compliance	4					

The five-level GRC maturity scale is defined as follows:

1. The practice is not available in the organization.
2. The organization is developing the practice.
3. The practice is available in the organization, but fragmented or used inconsistently throughout the organization.
4. The practice is integrated, available in the organization, and used consistently.
5. The practice is consistently measured and undergoing improvements.

We base this scale on the Capability Maturity Model (CMM), which was originally developed by the Software Engineering Institute [22]. The CMM five-level model fits our aim to specifically assess how IT contributes to the maturity of GRC from an alignment perspective. We are aware that there is specific literature describing GRC maturity levels as well such as the model developed by KPMG [6].

4 Analysis of Two Case Studies

In 2008, two case studies of Dutch companies were performed on the role that IT fulfilled in supporting the GRC processes in the organization. The two main goals were (1) to investigate how the organization achieved strategic alignment of IT with the business (applying the four alignment parts as presented in figure 2), and (2) to assess the organization on its GRC maturity (applying the maturity model as presented by Table 1). The approach followed during the two case studies can be described as follows. Firstly, a site visit was planned that included semi-structured interviews with GRC managers. The GRC managers that were invited to the interviews had an in-depth knowledge of the organizations' GRC maturity and deployment of a GRC solution in the organization. The interviews were used to assess the GRC maturity of the organization, by means of a questionnaire based on the measurement framework and practices. This questionnaire covers all three domains, the organization's GRC practices and the accompanying five-point maturity scale. The interview partners were asked to score, for each GRC practice, the "as is" maturity and how the alignment with IT helped to reach a certain "to be" maturity. For each of the three domains (Governance, Risk and Compliance) the scores on the practices were averaged. This processing of the answers resulted in a visualization of the GRC maturity status of the organization, describing the "as is" and "to be" maturity. This visualization was subsequently validated during a site visit. Secondly, the GRC-managers of the organizations were interviewed on the deployment process of IT in their organization, and to document their experiences in aligning IT with the business processes. Based on this interview, the type of alignment path followed by the organization (as defined in figure 2) was reconstructed and likewise validated.

4.1 Case 1: Dutch Utilities Company

Setting & GRC maturity. This company is a large energy producer and supplier with its customer base located in the Netherlands and Belgium. The company houses approximately 5,500 employees and has a turnover of approximately 9 billion euro. The organization was one of the first companies in the utilities sector to begin with separate compliance activities and integrating these activities with governance and risk management. The GRC maturity questionnaire that was completed by the respondents resulted into the figure 3, indicating the present state of GRC maturity and the maturity level the organization is aiming for within 2-3 years. The company proved to be performing at a maturity level of 3+ for many GRC areas, especially risk management. The lower maturity in the Governance domain can be explained because of the fact that the GRC organization is not yet modelled. The company's ambition is to charter the entire GRC organization with the use of IT and to raise maturity. Also the Compliance domain is lagging behind with respect to Risk management. This can be explained by compliance processes that are not performed as integrated throughout the organization and the use of other, siloed, "home-made", software. Evaluations on

the way the software in the company is used should guide the compliance processes to a higher level.

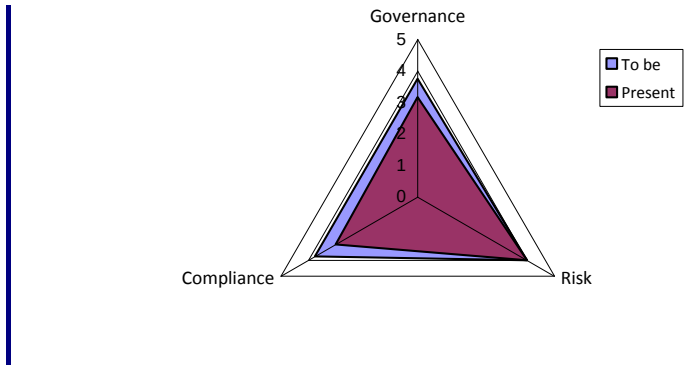

Fig. 3: The present and to be GRC maturity of the Dutch utilities company that was assessed.

Strategic alignment. Following our conceptual model as presented in figure 2, the deployment of the GRC IT solution in this case study can be classified as the "Technology transformation" path illustrated in figure 4. The company sensed the need for a specialized solution to support GRC and defined high-level business requirements that should be matched by the GRC solution strategy. The implementation of the GRC solution infrastructure was then done simultaneously and according to the specifications of the GRC solution strategy.

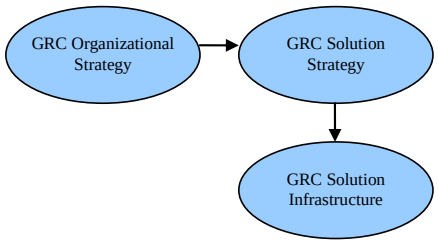

Fig. 4: Strategic alignment by the Dutch utility company through the "technology transformation" path.

The utility company used IT to manage the controls throughout the organization. Future plans consisted of the ambition to evaluate how an improved connection with other IT solutions available in the company (e.g. process modelling software) could be reached, or whether an entirely different solution should be deployed to replace several different solutions. This could bring the alignment between IT and business and the maturity of the GRC processes to yet a higher level.

4.2 Case 2: Dutch Financial Institution

Setting & GRC maturity. This company is a worldwide financial institution that delivers services in the area of banking, investments, life assurances and pensions. The roots of the institution are present in the Netherlands. The company houses approximately 107,000 employees and has a turnover of approximately 47 billion euro. Besides laws like SOX, the institution has to comply with the Basel II framework (see www.bis.org/publ/bcbsca.htm for further information). This set of international standards and best practices has led to a specific arrangement of the organization into four departments operating as silos. The maturity questionnaire as completed by the respondents results in figure 5. It shows the present state of GRC maturity and the maturity the organization is aiming for within 2-3 years. The institution proves to be at a 3+ maturity for all three areas. The ambition is still to keep on improving the maturity of the GRC practices in their organization, supported by a GRC solution. The institution is quite ambitious in its approach towards GRC. This is, among others, represented by the fact that a chief risk officer is represented on the board. The organization recognizes that a higher maturity concerning GRC can only be obtained by enhancements in the integration between the four departments and to start performing GRC as one integrated activity across the institution. IT needs to play a critical part in this process of integration, but can only be effectively used when it is aligned with the GRC business processes across the organization.

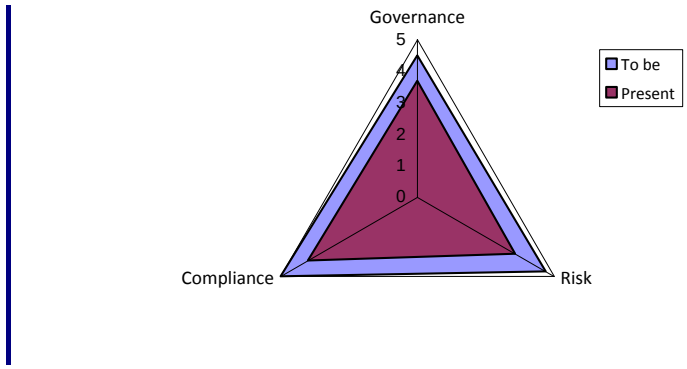

Fig. 5: The present and to be GRC maturity level of the Dutch financial institution that was assessed.

Strategic alignment. As shown in figure 6, the deployment of the IT solution can be characterized by the "service level" perspective, following our conceptual model in figure 2. When aligning IT with the business, the GRC solution strategy of the financial institution was the main driver because the actual GRC solution infrastructure would act as an addition to already available software. Then, the GRC IT solution was adapted the business processes, based on the processes incorporated in the software.

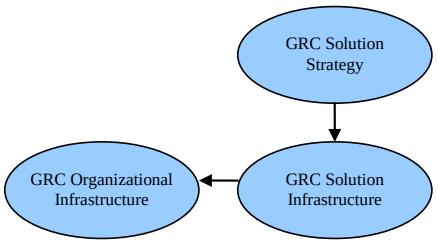

Fig. 6: Strategic alignment of the Dutch financial institution through the "service level" path.

Currently the solution is fully operational within the Operations & IT department, and several other departments have followed this implementation. The institution has the ambition to further deploy the solution throughout the organization, creating one integrated way of handling GRC.

5 Conclusions

This paper was triggered by a need to answer the research question: How can an integrated GRC approach be applied in organizations using a strategic alignment perspective? To achieve an answer to this question, several theoretical definitions of integrated GRC were reviewed, and a strategic alignment perspective was developed for the GRC domain which resulted in an approach to assess the GRC maturity and alignment paths for organizations. The empirical part of the paper then showed how the strategic perspective on GRC and its corresponding assessment framework were applied to two case studies. A large Dutch utility company and a financial institution were studied through a limited number of interviews with responsible managers who also provided feedback on the GRC assessment. Comparing the results of the two case studies showed that organizations have attained similar GRC maturity levels, while they have followed quite different paths to align IT to the business domain. Where the organizational strategy with regard to GRC led at the Dutch utility company, the financial institution selected a path in which the IT solution strategy was taken as starting point. In interpreting this result, it appears that the existing IT assets impact strongly on the selection of the alignment path.

This paper provides new insights but also invites an initiation of new directions for further research. One such direction is to practically support organizations that experience Governance, Risk and Compliance as separate and siloed concepts, and want to develop a holistic and united perspective to these concepts. Obviously, another direction for further research is to further validate and enrich our GRC maturity and alignment approach.

References

1. Chandler, A. D.: Strategy and Structure: Chapters in the history of American Enterprise. The MIT Press, Cambridge, Mass. (1962)
2. Dupuis, M., Endicott-Popovsky, B., Wang, H., Subramaniam, I., Du, Y.: Top-down mandates and the need for organizational governance, risk management, and compliance in China: A discussion, Asia-Pacific Economic Association (APEA), Sixth Annual Conference, Hong Kong, July 2010 (2010)
3. Frigo, M.L., Anderson, R.J.: A strategic framework for governance, risk and compliance, Strategic Finance, 90(8), 20-61 (2009)
4. Henderson, J. C., Venkatraman, N.: Strategic alignment: Leveraging Information Technology for transforming organizations. IBM Systems journal, 32(1), 472-484 (1999)
5. Koenig, D.R.: Enterprise risk management: A 360 degree review, Ductilibility, LLC, September 11 (2008)
6. KPMG: Survival of the most informed: GRC comes of age – How to envision, strategize, and lead to achieve enterprise resilience. KPMG International Cooperative (2010)
7. Madlener, J.J.: The implications of integrating governance, risk and compliance in business intelligence systems on corporate performance management. Erasmus University Rotterdam (2008)
8. Marks, N.: What is GRC and why does it matter? SAP, London (2010)
9. Mitchell, S.L., Stern Switzer, C.: GRC capability model Red Book 2.0, Open Compliance & Ethics Group (OCEG), April (2009)
10. MHI: Collaborative accountability in governance, risk, & compliance: Creating harmony across business roles, White Paper, MHI (2010)
11. OCEG: OCEG Corporate Compliance and Ethics Maturity Model™. from http://www.oceg.org/Download/OCCEMM (2007a)
12. OCEG: OCEG Corporate Governance Maturity Model™. from http://www.oceg.org/Download/CGMM (2007b)
13. OCEG: OCEG Matrix Adapted from RIMS ERM Risk maturity Model. from http://www.oceg.org/Download/RIMSERMM (2007c)
14. Racz, S., Weippl, E., Seufert, A.: A frame of reference for research of integrated governance, risk and compliance (GRC), International Federation for Information Processing (IFIP) (2010)
15. Robb, D.: IT-business alignment takes a step forward with GRC, CIO Update, March 9 (2010)
16. Sarbanes, P., Oxley, M.: Text of the Sarbanes Oxley Act., Washington: US Congress (2002)
17. Scheper, W.: Business IT Alignment: oplossing voor de productiviteitsparadox. Information Science. Utrecht University, Utrecht (2002)
18. Streng, R.J.: Corporate governance, internal control and risk management: The key role of information systems. Bertius Publishers, Moordrecht, The Netherlands (2010)
19. Tarantino, A.: Governance, risk and compliance handbook: Technology, finance, environmental, and international guidance and best practices. John Wiley & Sons, Inc., Hoboken, New Jersey (2008)
20. Tiazkun, S., Borovick, L.: Governance, risk and compliance, White Paper, IDC (2007)
21. Vemuri, A.: Strategic themes in risk and compliance, FINSights2, 2-5 (2008)
22. Venkatraman, N., Henderson, J. C., Oldach, S.: Continuous Strategic Alignment: Exploiting Information Technology Capabilities for Competitive Success. European Management Journal, 11(2), 139-149 (1993)