Journal of Service Science and Management, 2014, 7, 63-76
Published Online April 2014 in SciRes. http://www.scirp.org/journal/jssm
http://dx.doi.org/10.4236/jssm.2014.72007

Scientific Research

The Development of a Data-Centred Conceptual Reference Model for Strategic GRC-Management

Volker Nissen, Wolfgang Marekfia

Business Information Systems Engineering in Services, University of Technology Ilmenau, Ilmenau, Germany
Email: volker.nissen@tu-ilmenau.de

Received 30 January 2014; revised 28 February 2014; accepted 24 March 2014

Abstract

Until now there are only few ideas for an integrated governance, risk and compliance (GRC) management available with these referring to the management process of GRC only. In literature, mainly specific questions at a detailed level, like the automation of different controls, are discussed in the GRC context. To be in the position to entirely realise benefit potentials (e.g. improvement of processes), it is necessary to have an integrated GRC-Management focusing on the strategic business objectives. Starting from the requirements, this article deals with general guidelines for strategic GRC-Management showing which aspects have to be considered in terms of an integral approach. On this basis, a data-centred reference model explicates the structural connections of GRC-related data, and lays the basis for the implementation in practice.

Keywords

Governance, Risk, Compliance, Strategic Management, Information Objects, Reference Model

1. Introduction

Due to their diverse overlappings and dependences, governance, risk and compliance management [1] [2] are more and more seen as a connected topic under the acronym GRC. A study being recently carried out by the Open Compliance & Ethics Group [3] shows that the integration of GRC in practice proceeds and those companies see a possibility to improve their performance in it. Although first integrated approaches are available, [4]-[6] the borders of the topic areas remain altogether rather vague. On one hand there is a multitude of literature available concerning different sub-areas of GRC and dealing mainly with specific questions. On the other

How to cite this paper: Nissen, V. and Marekfia, W. (2014) The Development of a Data-Centred Conceptual Reference Model for Strategic GRC-Management. *Journal of Service Science and Management*, **7**, 63-76.
http://dx.doi.org/10.4236/jssm.2014.72007

hand there are already a few contributions available trying to structure and terminologically define GRC as an integrated approach [6] [7]. In practice, methodical weaknesses can be seen in approaches that realise individual regulatory requirements adequately, but are incapable of delivering a total overview concerning the status of GRC or the risk situation of a company. This may lead to gaps during the implementation process as well as to unnecessary double works. Moreover, governance can only then fulfill its task to support strategic decisions when adequate information is available from risk management and compliance management.

In its entirety GRC-Management cannot be limited to the aspect of integration only, but has to fulfil various requirements. The research project presented here in extracts takes—in addition to the integration of the three GRC sub-areas—the idea of a proactive and strategically adjusted GRC-Management as a basis, being referred to as "strategic GRC-Management". Here the focus is not on operational compliance and risk control but on the extensive planning and control of the GRC status, on the integration of different GRC-aspects as well as on strategic orientation and continuous improvement.

Racz *et al*. [6] as well as the "GRC Capability Model" of Mitchell and Switzer [5] put the process of GRC-Management into the centre of their observations. The "GRC Capability Model" shows possible GRC activities, but unfortunately the model it is not differentiated in management tasks and operative activities and the integration of GRC in the individual activities is not explicitly pointed out. In addition, it remains unclear, how the approach could be integrated into existing frameworks. Finally, governance aspects are only included to a limited extent. Racz *et al*. [6] develop a process model for "IT GRC". Here, it becomes clear that in the individual GRC disciplines a similar methodical procedure can be used, but concrete overlapping and interdependences are only dealt with marginally.

To develop a GRC-Management approach an analysis of the structural connections of the GRC-relevant information objects is necessary. The objective of this article, therefore, is the development of a data-centred conceptual reference model for strategic GRC-Management. Herewith especially two research questions are to be answered: 1) Which are the constituting information objects of strategic GRC-Management? 2) Which relations do these information objects have? The model aims to be a basis for the management of information being relevant for strategic GRC-Management. As a conclusion it can be useful as a basis for the development of GRC information systems as well as with view to the design of the GRC organisation. Furthermore, it can serve as a frame for the development of company specific models.

The article is structured as follows. In Section 2, our research method is described and linked to the field of reference modelling. In Section 3, requirements of strategic GRC-Management are outlined as they lay the foundation for our reference model. Then the model is developed, presented and evaluated. The article closes with a conclusion and some avenues for further research.

2. Foundations and Research Method

Reference models are universally applicable recommendations that can be used in a concrete modelling situation [8]. In comparison to ontologies, which as well are able to explicate the semantics of concepts and, therefore, the structure of GRC [9], reference models have the characteristic to function as a recommendation (to differentiate the terms see [10]). There are different method systems available dealing with reference modelling.

The architecture of integrated information systems (ARIS) [11] as a modelling concept differentiates between the views of organisation, of functions, of data, of results and of control/processes. Each view is looked at on the levels business concept, IT concept and implementation. In ARIS, modelling techniques are assigned to every view-level-combination. For the purpose of designing an application system the control/process view and the data view are particularly important.

We think that a reference model for GRC-Management can only be constructed on the understanding of the structure in terms of constituting GRC information objects and relations. Therefore, we focus the view of informations objects and their relation in our conceptual model. The Unified Modelling Language (UML) [12] contains different object-oriented kinds of graphs showing the structure, the behavior as well as the interaction. Classification graphs are core structures of UML with the structure being focused and a specific conceptual data modelling being supported.

This contribution uses a design science research approach. Design science research aims at creating innovative and useful IT artefacts [13] [14]. These artefacts are to be evaluated w.r.t. the utility provided in solving the

addressed problem. Peffers *et al*. [1] propose a process model for the conduct of design science research that has been the basis for our own investigation. More specifically, Peffers *et al*., integrating the views of different other researchers, propose six activities in their research methodology: identify problems and motivate, define objectives of a solution, design and develop artefact, demonstrate the use of the artefact, evaluate the results, communicate to the relevant audience.

The problem we focus on is the idea of a proactive and strategically adjusted GRC-Management. This is a relevant issue, as the approach promises benefits that are beyond operational compliance and risk control and can only be realised when one takes an integrated and strategic perspective on GRC with the aim to proactively plan and control the GRC status of the organisation as a whole. Our main objective here is the creation of a data-centred reference model [8] [15] that explicates the structural connections between the major information objects in strategic GRC-Management.

We derive the model content from the strategic GRC requirements and guidelines that were elaborated and presented in [16] and from the analysis of other models in the literature. A reference model is an example of an artefact in the sense of Hevner [13] [14]. Such a model is useful, because it lays the basis for the implementation of a corresponding strategic GRC-Management system in practice. The adequacy of the model elements and their relations is verified through an analysis of practical case studies in GRC. Finally, this paper is our attempt to communicate the findings to the relevant audience.

When it comes to modelling, the choice of the modelling technique should contain especially two aspects, being called "way of modeling" and "way of working" [17]. The first one concerns the choice of the modelling language. Here, UML classification graphs are used, as these support a specific conceptual modelling of the data and are mainly used in the models found in GRC literature. A modelling in entity relationship models [18] would be suitable, too. The "way of working" refers to the procedure of how the model is structured. Generally inductive and deductive approaches are possible for the construction of reference models.

Concerning the inductive way of working, it has to be said that reference models should be universally applicable in that sense that they should be valid for a group of company specific models [6] [8]. In an attempt to pay special attention to the requirements of reference models, the following research work combines inductive and deductive elements during the development of the reference model. A first step is the evaluation of existing models found in GRC literature, which base on empirical cases and conceptual considerations. In a second step, a comparison of the model elements found with the strategic GRC requirements, briefly outlined in the following section, takes place.

3. Strategic GRC Requirements

The basis for this research work is an extensive literature search dealing with strategic GRC-Management and on that basis the structuring of relevant aspects by means of requirements. Requirements are conditions or abilities that are needed to solve a problem, respectively achieve an objective (see IEEE glossary).

The derivation of requirements for a strategic GRC-Management was shown in [16] and will, therefore, in the following only be briefly outlined. The method of von Brocke *et al*. [19] has been adapted for the literature search, which follows the recommendation to focus on high-quality publications. In a first step, leading scientific magazines and conference proceedings were chosen with the help of relevant rankings. Furthermore GRC-specific publications were identified.

We searched in scientific databases and, in addition, manually checked the tables of contents of GRC-related journals and conference proceedings. Articles about integrated GRC approaches as well as about specific individual aspects of GRC (conceptual or empirical) were analysed. An internet search in general search engines and library databases was made, too, by which relevant works about integrated GRC approaches, publications on actual GRC practice (standards and best practices, handbooks, white papers) and relevant doctoral theses were found. All in all 191 relevant publications were found and provide the basis of our literature review.

To derive the requirements of strategic GRC-Management a qualitative content analysis was performed [20]. With the help of this analysis, categories and sub-categories of requirements were derived. The individual categories of requirements were analysed on the basis of the associated theories in the GRC-literature.

The identified requirements were then consolidated by means of guidelines that are shown in **Table 1**. The guidelines derived are to deepen the already existing knowledge and give indications in terms of high-level recommendations for the creation and further development of strategic GRC-Management approaches.

Table 1. Requirements for a strategic GRC-Management (consolidated in the form of guidelines).

Category of requirement (relevant theories)	Guidelines
Strategic orientation (market-based-view, resource-based-view, stakeholder theory, shareholder theory)	1) GRC should focus on the strategic objectives of companies to secure the companies' survivability. 2) The resources constituting the GRC-Management should support the achievement of operational potentials of benefit. To create strategic advantage through well-managed GRC, though, is at least more difficult. 3) GRC should focus on the stakeholders' interests. The stakeholders' interests should be balanced out on the premise of the long-term maximisation of the companies' value.
Integration (transaction costs theory)	4) The management activities being relevant for GRC should be carried out by a central approach (including integrated information systems and methods). The operational activities of GRC should be integrated into the core business processes and IT systems (hybrid approach). 5) To avoid double works as well as gaps during the implementation, GRC should be integrated by different compliance requirements as well as by the GRC disciplines.
Business process orientation (transaction costs theory)	6) A process oriented point of view as well as procedures, methods and tools of business process management (BPM) should be adapted to reduce the transaction costs in GRC.
Management systems (transaction costs theory, institutional theory)	7) To harmonize management systems in the context of GRC appropriate procedures, methods and tools should be developed.
Automation (transaction costs theory, principle-agent theory, organisational control theory)	8) IT should be used as an enabler for GRC-Management and be supported by appropriate organizational concepts. 9) To increase the efficacy of organisational procedures of compliance and risk control as well as for reasons of cost reduction, controls should be automated to the largest extent possible. At the same time organisational procedures should complementarily support automated controls.
Flexible business processes and IT systems (principal-agent theory, stewardship theory)	10) The challenge of flexible business processes and IT systems originates from the conflict between strategic achievement of objectives and regulatory GRC needs. This conflict of objectives should be balanced out depending on the individual situation.
Human factors (e.g. theory of reasoned action/planned behaviour, principal-agent theory)	11) The determinants of compliance behaviour are dependent on the consideration of manifold forms of control. The control approach chosen should consider the relation between the controls as well as situation specific aspects.

4. Development of the Reference Model

4.1. Evaluation of Already Existing Models in GRC Literature

In the 191 publications of interest for strategic GRC-Management, 21 relevant models could be identified (**Table 2**).

The evaluation of the model elements was carried out as follows. First, equal elements were assigned to each other. Then model elements using different terms but on the basis of underlying definitions have the same meaning were assigned. This includes German and English terms, respectively term variations, too. After that, the different levels of abstraction of the models were taken into account. Model elements being a subset of another element and not urgently needed for the conceptual modelling of strategic GRC-Management, were assigned to that element (e.g. "business goal" and "IT goal" to information object "goal"). Missing generic terms for matching model elements were developed. In this step, it also had to be decided, which level of abstraction or specification the model should have. Specifically this reflects the decision, whether a model element is an individual information object (classification in UML language) or just an attribute. In the end, a standardization of language was carried out. **Table 3** shows the assignment of the information objects after language homogenization to the synonyms and the secondary terms resulting from the models evaluated (model numbers according to **Table 2** in brackets). In addition, the number of models with elements being assigned to the mentioned information object are shown (column "No.").

For the analysis of the relations between the information objects the existing models can only be used to a small extent, as with the exception of Menzies [4] none of the models explicitly looks at an integration of GRC. But possible relations can, nevertheless, be derived. For this, on the basis of a consolidation of the model ele-

Table 2. Overview of relevant conceptional models found in GRC literature.

Model Focus	Topic Area	Source
1) Interrelationships of COBIT components	IT-Governance	[21] p. 8
2) Relationships between process modelling and control modelling concepts	Compliance	[22] p. 5
3) Selected correspondences between business process and risk	Risk management	[23] p. 24
4) Conceptual model of the compliance management problem	Compliance	[24] p. 5
5) A basic high level model for regulatory compliance	Compliance	[25] p. 180
6) Policy ontology	Compliance	[25] p. 187
7) Rule ontology	Compliance	[25] p. 188
8) A MOF/UML metamodel of a business protocol model	Compliance	[26] p. 562
9) A MOF/UML metamodel of an obligation	Compliance	[26] p. 563
10) A MOF/UML metamodel of a conditional commitment	Compliance	[26] p. 563
11) Rule ontology (constraints)	Compliance	[27] p. 794
12) The upper domain model of the internal controls compliance	Compliance	[28] p. 62
13) Relationship between an application control and a business process	Compliance	[28] p. 62
14) A semi-formalization of the control implementation	Compliance	[28] p. 63
15) IT risk reference model	Risk management	[29] p. 4
16) Meta-reference model for compliance management	Compliance	[30] p. 555
17) A classification model for automating compliance	Compliance	[31] p. 41
18) Exemplary excerpt from a corporate rule base	GRC	[4] p. 364
19) ISO 27001 metamodel	Risk management/Compliance	[9]
20) The oracle corporate analysis flow	Compliance	[32] p. 42
21) The regulatory mandate and compliance framework control domain relationship	Compliance	[32] p. 43

ments, relations within the models were identified, while the following restrictions apply. The focus, respectively the level of abstraction of the model in question has an important influence on the relations in the model. For instance, in the models evaluated the information object "role" (representing responsibility) has a relation to almost every other information object. In our case especially the responsibility for the GRC controls and business processes is relevant.

If no differentiation between the individual information objects in a source model was given, several relations were included. For instance, the information objects "control objective" and "control" were both put in relation to "business process", as there is not always a differentiation between the two in the literature. Partly, the source models differ in focus (company-wide vs. IT-related models), which had to be accounted for when transferring relations between information objects to the reference model.

Generally, it was not tried to show every possible relation, but to focus on those which lead to a consistent model and are very widespread. To achieve this, especially the analysis of strategic GRC requirements has made its contribution. Within the context of the presentation of the reference model (Section 5), the analysis has been seized in such a way that the relations identified in the already existing models are referenced at relevant passages to give reasons for the relations in the conceptual reference model developed.

4.2. Relation of Model Objects with Strategic GRC Requirements

In the following, the information objects for the reference model are derived from the requirements of strategic GRC-Management (as outlined in Section 3). **Table 4** summarizes the results.

Strategic orientation: The strategic orientation requires the orientation of GRC towards business strategies, the consideration of possible conflicts of objectives between the fulfilment of norms and the strategic achieving of objectives, the pursuance of potential benefits and the orientation towards stakeholders [16]. So information objects like "strategy", respectively "goal" are activated. GRC, meaning specifically the control objectives, should according to this be oriented towards the business goals. Governance should provide a framework for the

Table 3. Structured overview of model elements.

Information Object	Synonym Terms (As Used in Literature)	Secondary Terms	No
Control	Control Practices (1), Internal Control(s) (2, 5), Rule (4, 18), Procedures (5), Business Rule (11), Control (12, 19), Business Rule (20)	Risk Treatment Measure (3), Operational Business Rule (11), Declarative Business Rule (11), Company Level Control (12), IT Control (12), Application Control (12)	14
Role	Responsibility and Accountability Chart (1), Person Profile (3), Organisational Unit (3), Functional Entity (3), Actor (4), Business Function (6), Agent (11, 13), Authority (13), Organisational Chart (16), Responsible (18)	N/A	12
Business Process	Process (2), Process Model (6)	IT Processes (1), Key Activities (1), Task (2), Enterprise Activity (3), Process Structure (3), Activity (4, 6, 13), Process Fragment (6), Process Construct (6), Operation (11)	12
Control Objective	Requirement (4, 18, 19), Rule Goal (7), Measures & Directives (16), Directive (20)	Application Control Strategy (13, 14)	11
Guideline	Policy(ies) (4, 6, 11, 17), Standard Operating Procedure (18), Business Policy (20)	Meta-Policy (6)	7
Risk	Risk (2, 3, 4, 11, 12)	Event (3), Vulnerabilities (15), Threats (15, 19)	7
GRC Requirement	Source (4), Regulation (5, 6, 20), Authority (11), Laws and Regulations (17, 18)	N/A	7
Resource	Asset (3, 19), Enterprise Object (3), Business Subject (Sub-subject) (4), Subject (6)	Product Group (18)	5
Goal	Objective (3, 20), Desired Result (20)	Business Goals (1), IT Goals (1)	5
Application Area	Domain (3), Jurisdiction (6), Scope (6, 7), Scope (14)	Control Domain (21)	5
Documentation	Business Protocol (8), Business Document (13), Document Model (16)	N/A	5
Assessment	Audit (17)	Control Outcome Tests (1), Control Design Tests (1), Risk Assessment (12)	4
IT Component	IT Applications/IT Infrastructure (15, 21), IT-Architecture Model (16), Database Model (16), IT-System (17)	Packaged Service (21)	4
KPI	Performance Indicator(s) (1, 3)	Risk Indicator (3)	3
Stakeholder	Stakeholder (3, 18)	Indirect Stakeholder (18)	2
Strategy	Strategy Model (16)	N/A	2
Maturity Level	Maturity Model (1, 16)	N/A	2
Framework	Compliance Framework (21)	N/A	2
Performance	N/A	N/A	2
Monitor	N/A	N/A	2
Violation	N/A	Security Breach (19)	2
Implementation Logic	Rule Logic (7)	N/A	1

definition of strategy and goals and make the integrated management of "performance" and "conformance" [33] possible by means of assessments and key performance indicators. Better controls may lead to the improvement of the business process performance and to the achievement of business objectives by means of GRC, being equivalent to the requirement to pursue potential benefits. The stakeholder orientation requires an alignment of the strategy and of the goals and by this indirectly an alignment of the control objectives to the interests of the stakeholders.

Integration: The integration of GRC is discussed in literature with view to content-related, methodical, re-

Table 4. Information objects and relations from the requirements of strategic GRC-Management.

Category of requirement	Relevant information objects	Derived relation
Strategic orientation	Strategy, Goal, Guideline, Control, Key Performance Indicator, Stakeholder	(B1) Control objectives are adjusted to the goals. (B2) Business processes support goals being measured by key performance indicators. (B3) Strategy and goals are oriented on stakeholders.
Integration	Control Objective, Risk, GRC Requirement, Key Performance Indicator, Assessment, Business Process, Control	(B4) Control objectives result from risks and GRC requirements. (B5) Assessments measure through performance indicators conformance and performance of business processes. (B6) Controls are realised during core business processes (operative integration).
Business process orientation	Control, Business Process, Implementation Logic, Role	(B7) Controls are implemented into business processes and with the help of an implementation logic are automated within the business process. (B8) The responsible role (ownership) is determined by business processes.
Management systems	Assessment, Key Performance Indicator, Business Process	(B9) Business processes are controlled by assessments and through key performance indicators with view to GRC.
Automation	Control, Business Process, IT Component, Implementation Logic	(B10) IT components are directly affected by controls. (B11) Controls are automated by an implementation logic.
Flexibilisation	All, especially Business Process, IT component, GRC Requirement, Risk	(B12) A direct relation between IT components and risks is necessary to make a control of the risks during IT-related adjustments possible.
Human factors	Control, Business Process, Role	(B13) Controls have a direct relation to the information object “role”.

spectively information technical aspects. Content aspects are the integrated fulfilment of several GRC requirements and the integration of GRC disciplines. In addition, an integration of GRC-activities into core business processes is demanded [16]. For the research objective pursued by this reference model, both integration aspects are highly relevant. There are two points of views concerning the relation of compliance management and risk management. On one hand, compliance is seen as a sub-area of risk management, in which the non-compliance-risk is considered as a risk category [34] [35]. On the other hand, risk management is seen as a sub-area of compliance. Risk management and in relation to that the establishment of an internal control system, therefore, is a GRC requirement, its realisation being supported by control models like the ones used for IT processes, e.g. COBIT, ITIL or ISO 27001/2 [36]. But it is also possible to define control objectives for risk controlling measures out of risk analyses. Control objectives, therefore, can be derived from risks as well as from GRC requirements.

Concerning the obeying of regulatory requirements [2] there is an overlapping between corporate governance and compliance. In addition the term corporate governance is associated with a value-based leadership strategy of companies [2] which is backed up by the IT governance term as well [30]. According to Racz *et al*. [6] corporate governance as well as risk and compliance management support themselves mutually by delivering important information from risk and compliance management to governance and by taking over the control of risks and compliance management by governance.

Business process orientation: In the literature a business process-oriented approach is demanded due to the importance of business processes for GRC as well as the importance of a business process-oriented approach for the automation of compliance safe-guarding [16]. This results in the demand to integrate GRC and business process management. Business processes have a direct connection to risks [29] and in terms of an operative integration (see requirement category “integration”) should include the controls. As business processes are the starting point of automation, there is also a relation to the implementation logic. Following a business process-oriented approach, the business process is a central element of GRC-Management. The responsibility (ownership, information object “role”) for business processes, thus, determines ownership to a number of further in-

formation objects, such as "controls", and, consequently, the responsibility for the fulfilment of GRC-requirements. Risk minimizing measures should be carried out by the employees working within the associated business process.

Management systems: A harmonization of GRC with other management systems in the company is required, as today GRC contents are often distributed over several organizational units and management systems. Relevant management systems that have to be coordinated with GRC are those that can be subsumed under a certain GRC topic area (e.g. internal revision, data protection, quality management) and others that in the context of GRC are more generally relevant (e.g. controlling, IT management) [37] [38]. Management systems being subsumed under GRC mainly deal with the control of the spheres of responsibility they were entrusted to. This is very much underlined in the scope of tasks for the internal revision, providing independent control and council services [39]. Controlling has a similar task, which supports the management by planning, controlling and the provision with information and uses performance measurement systems. It must be pointed out that adjustment and coordination of GRC with related management systems generates costs that could partially be avoided with a more centralized GRC-approach.

Next to business process management also IT management concerning the introduction and operation of information systems and quality management as well as the internal revision often pursue business process-oriented approaches. As a conclusion, next to "assessments" and "key performance indicators" also "business processes" are relevant information objects here.

Automation: IT is object and supporter of GRC [2]. From the point of view of IT as a supporter of GRC, especially the automation of compliance safeguarding and of risk control is relevant. Thereby, the manual control effort and risk of human errors are reduced. IT as an object of GRC, respectively in the context of information security, is directly an object of compliance requirements and risks. Relevant information objects are "controls", "business processes", "IT components" and "implementation logic". In addition, not every control can be automated, but partly has to be carried out manually [29].

Flexibilisation: In literature flexible business processes and IT systems are presented as a grand challenge for GRC. Consequences of regulatory changes to the organisation, respectively effects of organisational adjustments on compliance have to be looked at [40]. Furthermore, it is necessary to supervise continuously the risks [31]. Menzies [4] identifies pushers of GRC-management such as new processes and products, M & A activities and IT systems.

Flexibilisation may have consequences to nearly all information objects of the reference model, especially to "strategies", "goals", "business processes" and "resources", "risks" as well as "controls". Sackmann [31] puts emphasis on the relations between risks and IT components as well as business processes. The direct relation between IT components and risks is necessary, as changes among the IT components may have direct consequences for the risk situation, which do not necessarily affect the running of business processes.

Factors concerning human behaviour: The demand to consider human behaviour refers to the behaviour of employees [41] [42], the company culture [5] [43] as well as the communication in terms of the "tone at the top" [4] [5] [35]. The responsible employee who in his position carries out business processes and the controls included, is therefore of high importance. For this reason, controls such as trainings and awareness campaigns should be offered to make employees competent for their roles in GRC and to encourage them. As a conclusion, "controls" have a direct relation to the information object "role".

5. Presentation of the Reference Model

The reference model shown in **Figure 1** bases on the analyses made in the sections before. In addition, the presentation already anticipates the results of the evaluation in Section 6. Information objects that could not be confirmed during evaluation are left out. The relations between the information objects are derived by the already existing models (1 - 21, according to **Table 2**) as well as by relations derived from the strategic GRC requirements (No. B1 - B13 according to **Table 4**). Due to the complexity of the model, a further subdivision into a strategic, conceptual and operative level has been made, which only is to improve the readability of the model and is not subject of the derivation, respectively evaluation.

On the strategic level, GRC should start at the results of strategic management, use these for governance and for the strategic orientation of risk and compliance management and furthermore support the strategy process by means of relevant information. Starting point are the stakeholders whose interests have overall economical in-

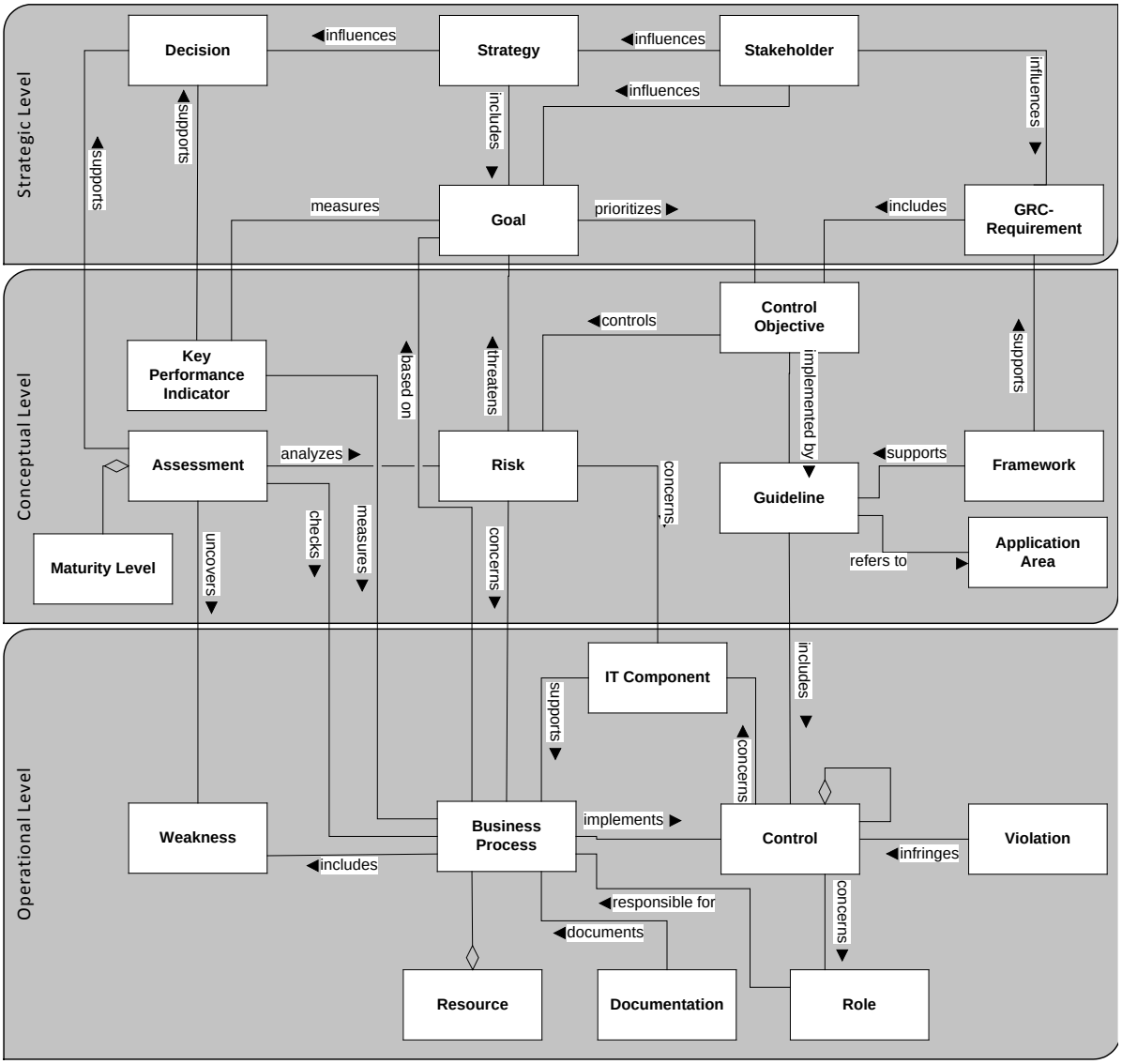

Figure 1. Data-centred conceptual reference model for strategic GRC-Management.

fluence on the GRC requirements (18) and company-related, as shown in the analysis of the requirement category "strategic orientation", have influence on strategy and goals (B3). Strategies support the achievement of objectives (6, 16) and influence the decision-making (see evaluation).

It should be differentiated between the strategic level and the conceptual level, which includes the management activities of GRC. Here the control objectives resulting from the GRC requirements (4, 5, 17, 18, B4) and the risks (2, 4, 12, B4) have to be developed. The requirement category "strategic orientation" also suggests that the control objectives should be adjusted to the business goals of the strategic level (1, B1). The guidelines are derived from the control objectives (4, 5, 17, 18, 20), which have a limited application area (6).

To derive company-specific guidelines, frameworks like established standards and best practices can be taken (4, 18), which support the fulfilment of GRC requirements (18). Business processes have to be adjusted to company goals (3, 20, B2, B9). The focus of this model suggests to carry out assessments with view to risks (12) as well as to "conformance" and "performance" (B5) on the business process level (1, 12, B5, B9). In this context, maturity models can be used, which are a special form of assessment. Assessments support decisions on the strategic level. Business processes are again connected to controls (2, 3, 5, 6, 11, 12, 13, 18, B6, B7) and risks (3, 12, 15, 19). Risks still can result directly from IT components (15, B12) without business processes being

changed. Risks threaten the achievement of objectives (11). Performance indicators measure business processes (1, B5, B9) concerning the achievement of goals (1, 3, 16, B2) and herewith support, as well as assessments, decisions on the strategic level (see evaluation).

On the operative level, controls being formulated in the form of guidelines (4, 5, 6, 11, 18, 20) are implemented in terms of an operative integration into the core business processes (2, 3, 5, 6, 11, 12, 13, 18, B6, B7). There may be dependencies between the controls themselves (6, 11, 19). Controls still can be infringed by violations (4, 19) and, next to business processes, directly concern those IT components (B10) which support the business processes (15). In addition, IT components serve for the automation of controls (B11). Business processes are seen as company resources, whereby further objects like products, projects and information are relevant for GRC (3, 6, 18). IT components and controls have to be documented within the context of business processes (13). The model defines the responsibilities by means of the roles being part of the business processes (1, 4, 6, 11, 13, 18, B8). Controls may directly concern employees (11, B13). Eventually, weaknesses of business processes can be found within the context of assessments on the conceptual level (see evaluation).

6. Evaluation

It is possible to evaluate reference models with view to different criteria like e.g. the principles of modelling [44] and by using different methods of evaluation [45]. Here the usefulness of the reference model during the data modelling process for a strategic GRC-Management is to be evaluated. This includes the adequacy of the information objects, e.g. with view to the level of abstraction and the terms used, the completeness of the information objects and the correct modelling of the relations between the information objects. Furthermore, it is planned to further specify the information objects with view to practice requirements e.g. by attributes. As until now the GRC integration on the strategic level has been rarely looked at by research [46], practical case studies found in literature dealing with GRC sub-aspects were taken for evaluation. These refer to successful implementations and make it possible to integrate a relatively broad range of cases with a sufficient depth of content. Further evaluations, e.g. concerning the correct syntax, and an application of the model in practice are desirable. However, the success of the application depends also on further factors such as the maturity of the business process management of the company, the availability of appropriate GRC-Management methods and the information systems used.

The procedure of evaluation is as follows. First, implementation examples were identified by looking for case studies in the literature [16] and through the search in general search engines as well as practical publication organs. Altogether 21 relevant practical examples were included and used for evaluation.

On a general level, the evaluation shows that a standardised GRC-terminology is missing in practice. Partly different terms for the same matters are used, respectively differentiated only insufficiently from each other. In the case studies, differences between the GRC sub-areas and industries with reference to the information objects could hardly be found. Rather, common core terms such as “control”, “business process”, “risk” and different terms dealing with GRC requirements were found. Due to the great significance of the Sarbanes-Oxley-Act across all business fields, financial reporting on the whole is of high importance. The involvement of the top management into many GRC-tasks is still seen as important. Explicitly, the uncertainty concerning the management methods for GRC was pointed out [4]. Frameworks such as COSO and COBIT were judged to be too abstract and cannot always clearly be distinguished from the actual regulatory GRC requirements.

As far as adequacy and completeness of the information objects are concerned, **Table 5** shows the number of practice examples using terms that can be assigned to the information objects of the reference model. The result is an overlapping and a similar distribution of terms as in the evaluation of the existing GRC-models in literature. But it has to be said that none of the examples confirms all information objects. The models found in GRC literature have often been developed with the objective of automating controls, which is not at the centre of the practice examples. The information objects “monitor” and “implementation logic”, therefore, could not be confirmed. The information object “execution” was only confirmed in one case and is, thus, merged with “business process”.

The level of abstraction of the reference model seems to be appropriate, but needs further specification concerning the shaping of the attributes of the information objects. Controls are relevant on different levels and are differentiated into company level, business and IT controls [4]. In addition, the focus in practice is put on key controls with the objective to achieve a concentration towards critical areas. Business processes are mentioned

Table 5. Information objects and number of practice cases in support.

Control	16
Role	16
Business Process	21
Control Objective	13
Guideline	11
Risk	1
Resource	2
Goal	11
Application Area	5
Business Document	15
Assessment	13
IT Component	14
Key Performance Indicator	7
Stakeholder	6
Strategy	9
Maturity Level	3
Framework	7
Execution	1
Monitor	0
Violation	2
Implementation Logic	0

in every example including also management processes of GRC. The processes are divided into core and supporting processes in the practice examples, responsibilities are relevant on all hierarchy levels. Business documents are cited concerning the documentation of controls and the reporting system. It is proposed to classify risk into risk categories [47]. The examples show that financial performance indicators for profitability and costs are of importance for GRC. The value respectively the value creation of GRC is relevant as well.

A number of further terms are of high relevance in the practice examples, but cannot directly be assigned to the information objects in the reference model and, therefore, are discussed here in more detail. Terms like “group”, “division” and “national company” show the complexity of international groups. The reference model is basically able to show this by means of several models on different levels of hierarchy. The term “project” in the examples refers to projects dealing with the realisation of GRC requirements. But also business initiatives, especially in the IT sector, are realised by means of projects and are, hence, object of GRC-Management.

A number of case studies mention the carrying out of trainings, which are a kind of control having a direct relation to the information object “role”. The term “control” is of high importance in the examples. It refers to the term “governance” and shows the task of GRC concerning the management of “performance” and “conformance”. Several times the term “weakness” is mentioned, which is used in the sense of weakness in control and has to be added to the reference model. Further terms being cited in connection with financial reporting are “financial data” and “account”. Both terms are objects of control and are subsumed under “resources” in the reference model.

GRC has the function to support decisions on the strategic level. To support decision making, especially information coming from assessments and performance indicators is relevant. Also a meeting structure, which includes a management board responsible for decision-making, is necessary. Therefore, “decision” is added to the model as an information object. The terms “service level agreement” and “service” are cited, too, but are especially of relevance for IT governance and were not taken over into the generic reference model. They point out the importance of services as a subject of controls and the importance of contracts as a source of GRC requirements.

With respect to the relations of the information objects, it can be stated that relations are rarely looked at in the practical case studies and their analysis is further complicated by an inexact terminology. For instance, several times scoping is mentioned (information object, application area), but it is not clear, whether this refers to GRC requirements, control objectives, controls, risks or GRC guidelines. Partly, the relations themselves are described very generally. For instance, departments are to be oriented towards goals [48].

Only the practice example in [49] discusses explicitly the integration of GRC, but does not focus on the information level but on organizational structures and reporting. The difference between the information objects "control objective" and "control" is not explicitly made clear in all practice examples. Therefore, controls like e.g. in [4] are not always assigned to the control objectives, but partly directly to risks. Relations between controls [4] [50], controls and processes [4], risks and objectives [47] as well as processes and assessments [48] [51] are confirmed in the practical cases.

7. Conclusions

In this article, a data-centred conceptual reference model for a strategic GRC-Management was developed, which shows the relevant information objects and structural connections. Only insignificant adaptations and a few indications for further specification of the model resulted from the practice-based evaluation of case studies in the literature. The kind of evaluation chosen seems appropriate, as the research concerning GRC integration is in its infancy. Moreover, the examples we looked at have a sufficient depth of content.

However, the evaluation of the relations between the information objects was only possible to a limited extent by means of the case studies. Although a reason for the connection of the model elements was given by the models found in literature and by the strategic GRC requirements, the relations should be subject of further research.

The objective of the research project presented here was the development of a specific conceptual reference model. To implement it in the context of an information system for strategic GRC-Management will require further refinement, such as adding attributes to the information objects. Moreover, it makes sense to further specify the information objects following the organizational company hierarchy in big groups. More research needs still exist, e.g. with view to the applicability of the model in different lines of business.

Finally, it can be said that by the majority of the case studies evaluated still a great uncertainty became visible concerning the realisation of GRC approaches. The GRC requirements found within the context of our examination, the guidelines and the reference model, which aims at the data level, represent only first steps towards the strategic alignment and integration as well as towards the terminological standardization of GRC. Herewith, the implementation of a strategic GRC-Management in companies is supported. But with view to the management methods and IT-based tools in GRC-Management, deficits can be identified that will have to be solved in future research projects. The reference model may give important indications to companies to better classify methods and tools, to choose them accordingly or, if needed, to develop them themselves.

References

[1] Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, **24**, 45-77. http://dx.doi.org/10.2753/MIS0742-1222240302

[2] Teubner, A. And Feller, T. (2008) Informationstechnologie, Governance und Compliance. *Wirtschaftsinformatik*, **50**, 400-407. http://dx.doi.org/10.1007/s11576-008-0081-6

[3] Open Compliance & Ethics Group (2012) 2012 GRC Maturity Survey. http://www.oceg.org/event/the-2012-grc-maturity-survey-report/

[4] Menzies, C. (2006) Sarbanes-Oxley und Corporate Compliance—Nachhaltigkeit, Optimierung, Integration. Schäffer-Poeschel, Stuttgart.

[5] Mitchell, S.L. and Switzer, C.S. (2009) GRC Capability Model. Red Book 2.0. Open Compliance & Ethics Group, Phoenix.

[6] Racz, N., Weippl, E. and Seufert, A. (2010) A Process Model for Integrated IT Governance, Risk & Compliance Management. *Proceedings of the Ninth Baltic Conference on Databases and Information Systems* (*DB&IS* '10), Riga, 155-170.

[7] Racz, N., Weippl, E. and Seufert, A. (2010) A Frame of Reference for Research of Integrated GRC. In: De Decker, B.

and Schaumüller-Bichl, I., Eds., *Communications and Multimedia Security. Proceedings of CMS*, Springer, Berlin, 106-117.

[8] vom Brocke, J. (2003) Referenzmodellierung. Gestaltung und Verteilung von Konstruktionsprozessen. Logos, Berlin.

[9] Milicevic, D. and Goeken, M. (2010) Konzepte der Informationssicherheit in Standards am Beispiel der ISO 27001. In: Fähnrich, K.P. and Franczyk, B., Eds., *Proc. Informatik* 2010, LNI Vol. 176, Köllen, Bonn, 305-310.

[10] Zelewski, S. (1999) Ontologien zur Strukturierung von Domänenwissen—Ein Annäherungsversuch aus betriebswirtschaftlicher Perspektive. Technical Report No. 3, Institut für Produktion und Industrielles Informationsmanagement, Essen.

[11] Scheer, A.-W. (2002) ARIS—Vom Geschäftsprozeß zum Anwendungssystem. 4th Edition, Springer, Berlin. http://dx.doi.org/10.1007/978-3-642-56300-3

[12] OMG (2010) Unified Modelling Language: Infrastructure, Version 2.3. OMG, Needham.

[13] Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004) Design Science in Information System Research. *MISQ*, **28**, 75-105.

[14] Hevner, A.R. and Chatterjee, S. (2010) Design Research in Information Systems: Theory and Practice. Springer, Berlin.

[15] Becker, J., Delfmann, P., Knackstedt, K. and Kuropka, K. (2002) Konfigurative Referenzmodellierung. In: Becker, J. and Knackstedt, R., Eds., *Wissensmanagement mit Referenzmodellen. Konzepte für die Anwendungssystem-und Organisationsgestaltung*, Physica, Heidelberg, 25-144. http://dx.doi.org/10.1007/978-3-642-52449-3_2

[16] Marekfia, W. and Nissen, V. (2012) Anforderungen an ein strategisches GRC-Management. *Proceedings of Informatik*, 731-745.

[17] Verhoef, T.F., Hofstede, A.H.M.T. and Wijers, G.M. (1991) Structuring Modelling Knowledge for CASE Shells. In: Andersen, R., Bubenko, J. and Soelvberg, A., Eds., *Advanced Information Systems Engineering*, CAiSE'91, Trondheim, Norway, 13-15 May 1991, Lecture Notes in Computer Science 498, Springer, Berlin, 1991, 502-524..

[18] Chen, P.P.-S. (1976) The Entity-Relationship Model—Toward a Unified View of Data. *ACM Transactions on Database Systems*, **1**, 9-36. http://dx.doi.org/10.1145/320434.320440

[19] vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Newell, S., Whitley, E., Pouloudi, N., Wareham, J. and Mathiassen, L., Eds., *Proceedings of the ECIS* 2009, 17*th European Conference On Information Systems*, Verona, 2206-2217.

[20] Bohnsack, R., Marotzki, W. and Meuser, M. (2006) Hauptbegriffe Qualitativer Sozialforschung. 2nd Edition, Budirch, Opladen.

[21] The IT Governance Institute (ITGI, Hrsg.) (2007) COBIT 4.1. http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

[22] Sadiq, S., Governatori, G. and Naimiri, K. (2007) Modeling Control Objectives for Business Process Compliance. *Proceedings of the* 5*th Conference on Business Process Management*, Lecture Notes in Computer Science 4714, 149-164. http://dx.doi.org/10.1007/978-3-540-75183-0_12

[23] Sienou, A., Lamine, E. and Pingaud, H. (2008) A Method for Integrated Management of Process-Risk. *Proceedings of GRCIS*, Springer, Berlin, 16-30.

[24] Silveira, P., Rodriguez, C., Casati, F., Daniel, F., D'Andrea, V., Worledge, C. and Taberi, Z. (2009) On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management. *Proceedings of ICSOC Workshops*, **6275**, 208-217.

[25] El Kharbili, M., Stein, S. and Pulvermüller, E. (2008) Policy-Based Semantic Compliance Checking for Business Process Management. *Proc. MobIS Saarbrücken* 2008, LNI Vol. P 141, Köllen, Bonn, 178-192.

[26] Goedertier, S. and Vanthienen, J. (2006) Business Rules for Compliant Business Process Models. *Proceeding of International Conference on Business Information Systems* (BIS 2006), Klagenfurt, 31 May-2 June 2006, 558-572.

[27] Weigand, H., van den Henvel, W.J. and Hiel, M. (2011) Business Policy Compliance in Service-Oriented Systems. *Information Systems*, **36**, 791-807.

[28] Namiri, K. and Stojanovic, N. (2007) A Semantic-Based Approach for Compliance Management of Internal Controls in Business Process Management. In: *Advanced Information Systems Engineering*, 19*th International Conference CAiSE* 2007, Trondheim, Norway, 11-15 June 2007, Proceedings. Springer, Berlin, 61-64.

[29] Sackmann, S. (2008) A Reference Model for Process-Oriented IT Risk Management. In: Golden, W., Acton, T., Conboy, K., Heijden, H.V.D. and Tuunainen, K., Eds., *Proceedings of ECIS*, GITO-Verlag, Berlin, 1137-1148.

[30] Teuteberg, F. and Freundlieb, M. (2009) Compliance Management mit betrieblichen Umweltinformationssystemen.

Wisu—Das Wirtschaftsstudium, **4**, 550-557.

[31] Sackmann, S. (2008) Automatisierung von Compliance. *HMD—Praxis der Wirtschaftsinformatik*, **45**, 39-46.

[32] Pohlman, M. (2008) Oracle Identity Management: Governance, Risk, and Compliance Architecture. 3rd Edition, CRC Press, Boca Raton. http://dx.doi.org/10.1201/9781420072488

[33] International Organization for Standardization and International Electro Technical Commission (ISO, IEC Hrsg.) (2008) Corporate Governance of Information Technology. Geneva.

[34] Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW, ed.) (2010) Entwurf IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen. (IDW EPS 980) Stand: 11.03.2010. Düsseldorf.

[35] Withus, K.H. (2010) Sicherstellung der Compliance durch wirksame Managementsysteme. *Zeitschrift für Interne Revision*, **7**, 99-108.

[36] Johannsen, W. and Goeken, M. (2006) IT-Governance—Neue Aufgaben des IT-Managements. *HMD—Praxis der Wirtschaftsinformatik*, **250**, 7-20.

[37] Bhimani, A. (2009) Risk Management, Corporate Governance and Management Accounting. Emerging Interdependencies. *Management Accounting Research*, **20**, 2-5. http://dx.doi.org/10.1016/j.mar.2008.11.002

[38] Klotz, M. (2009) IT-Compliance: Ein Überblick. Dpunkt, Heidelberg.

[39] Deutsches Institut für Interne Revision (2011) Internationale Standards für die berufliche Praxis der Internen Revision 2011. Frankfurt am Main.

[40] Müller, G. (2007) Für Sie gelesen. *Wirtschaftsinformatik*, **49**, 107-109.

[41] Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009) If Someone Is Whatching, I'll Do What I'm Asked: Mandatories, Control, and Information Security. *European Journal of Information Systems*, **18**, 151-164.

[42] Herath, T. and Rao, R. (2009) Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems*, **18**, 106-125.

[43] Abdullah, S.N., Indulska, M. and Sadiq, S. (2010) Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In: Hutchinson, *et al*., Eds., *Advanced Information Systems Engineering*, 22*nd International Conference*, *CAiSE* 2010, Hammamet, Tunisia, 7-9 June 2010. Proceedings, Springer, Berlin, 251-265.

[44] Schütte, R. (1997) Die neuen Grundsätze ordnungsmäßiger Modellierung. *Paper Presented at Forschungs Forum*, Leipzig, 1997, 16.09-20.09.97. http://www.econbiz.de/archiv/e/ue/produktion/ordnungsmaessige_modellierung.pdf

[45] Fettke, P. and Loos, P. (2004) Entwicklung eines Bezugsrahmens zur Evaluierung von Referenzmodellen. In: Loos, P., Ed., *Working Papers of the Research Group Information Systems & Management*, Vol. 20, ISYM—Information Systems & Management, Mainz.

[46] Gericke, A., Fill, H.G., Karagiannis, D. and Winter, R. (2009) Situational Method Engineering for Governance, Risk and Compliance Information Systems. *Proc. DESRIST* 2009, ACM Press, New York, Article No: 24. http://dx.doi.org/10.1145/1555619.1555651

[47] Kley, W.D. (2011) Risiko-und Chancenmanagement der MAN SE. *Zeitschrift für Controlling & Management*, **55**, 105-110.

[48] Fröhlich, M. and Glasner, K. (2007) IT Governance. Leitfaden für eine praxisgerechte Implementierung. Gabler, Wiesbaden.

[49] Tüllner, J. (2012) Integration von Governance, Risikomanagement und Compliance. Erfahrungsbericht über ein Projekt zur Optimierung der Unternehmenssteuerung und einen ganzheitlichen Lösungsansatz. *Zeitschrift für Corporate Governance*, **7**, 118-121.

[50] Gigerl, T., Unger, C. and Baumgartner, C. (2007) Umsetzung eines integrierten IT-Compliance-Frameworks—am Beispiel ALTANA Pharma. *Information Management & Consulting*, **22**, 70-77.

[51] Just, D. and Tami, F. (2007) Praxisbeispiel: Bewertung von Applikationsportfolios und IT-Prozessen. In: Johannsen, W. and Goeken, M., Eds., *Referenzmodelle für IT-Governance. Strategische Effektivität und Effizienz mit COBIT, ITIL & Co*, Dpunkt.verlag, Heidelberg, 225-242.