A Framework for Assessing Organisational IT Governance, Risk and Compliance

Mikhel Vunk[1], Nicolas Mayer[2] and Raimundas Matulevičius[1]

[1] Institute of Computer Science, University of Tartu, Estonia
mihkel.vunk@gmail.com, rma@ut.ee
[2] Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux,
L-4362 Esch-sur-Alzette, Luxembourg
nicolas.mayer@list.lu

Abstract. Enterprises have reached to understanding that information technology (IT) is more than just a technical issue. Domains such as IT governance, risk management and compliance (GRC) have been established to steer it. Though there has been some improvements, these domains are usually considered separately, thus less business value is created due to complexity of the process flows. There has been little attempts to integrate all three aspects, however this was done using domain specific standard and not taking into account the existing state of the art. In this paper, we conduct a systematic literature review to understand the processes, roles, strategies, and technologies of IT GRC as well as their integration. Based on the results of the review, we propose an assessment framework, which could guide evaluation of the enterprise's IT GRC concerns.

Keywords: Governance, Risk Management, Compliance, IT GRC, Systematic review

1 Introduction

Enterprises are facing challenges while governing their Information Technology (IT) resources and needs. Due especially to instability of the markets in the global financial system, competition pressure and corporate disasters in last decades, all corporations need to have focused on their governance, risk and compliance (Corporate GRC) activities. Basically, according to Racz *et al.*, GRC can be defined as "an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization 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" [1]. Therefore, ensuring that their IT supports their current and future GRC-needs, IT GRC has been derived. IT GRC is not new but it is still a subject of research. The main challenge of IT GRC is to have an approach as integrated as possible to IT governance, IT risk management and IT compliance. The aim is to improve effectiveness and efficiency of the three disciplines, mainly compared to the traditional silo approach generally performed within organizations.

The scope of this study is to define a framework for IT GRC. Although there exist a number of studies that separately consider the IT governance, IT risk management and IT compliance challenges [2–4], little is done to integrate these domains together [5]. In this paper, the research question considered is *how IT governance, IT risk management and IT compliance could be integrated*.

To answer this research question, we have performed a systematic literature review, aiming at answering the following sub-questions: which processes have been defined for IT GRC, what roles of people are involved for IT GRC, what strategy is used for IT GRC, and what is considered as technology for IT GRC. Based on the review results, we proposed an integrated framework for assessing organisational IT GRC. The framework is supported by a web application, which could be used by organisations to assess their IT GRC practices.

The rest of the paper is organized as follows. In Section 2, we present the systematic literature review. Section 3 overviews the integrated framework for IT governance, IT risk management and IT compliance, including its implementation and validation aspects. Finally, Section 4 presents the concluding remarks and highlights the directions for future work.

2 Systematic Review of IT GRC

In this chapter, we present a systematic literature review and its components regarding IT governance, IT risk and IT compliance. Firstly, we describe the research method. Next we discuss the review protocol. Finally, we present the review results, thus constituting the state of the art for the integrated IT GRC framework.

2.1 Systematic Review Method

We have applied a systematic literature review method [6] to determine what is the state of the art in the IT GRC domain. The goal of our study is to understand how IT governance, IT risk management and IT compliance could be integrated. The review is executed through three stages – plan, conduct and report, as illustrated in Fig. 1. During the plan stage, we have specified the research question, developed and validated the review protocol. Second stage consists of the activities to conduct the research protocol. This included research identification, selection of the primary studies and assessment of their quality, and extraction and synthesis of the data. The final stage included preparation and validation of the report.

2.2 Review Protocol

Background: Enterprise processes are complex, involving IT not only as the technical issue but also including governance, risk management and compliance. However, IT governance, IT risk management and IT compliance are commonly dealt separately in silos. Hence the challenge is to integrate them to improve enterprises efficiency and effectiveness [7]. Typically, the integration of the three domains is referred as IT GRC, covering all the three disciplines. The literature review is conducted to find the state of the art of IT GRC based on scientific literature. It is worth to note that, in terms of scope, we clearly distinguish here (Corporate) GRC from IT GRC, the latter being the subset of Corporate GRC dealing with IT [5].

Before defining the research question, we have conducted a small exploration over the secondary studies. It revealed a framework [7] which integrates IT governance, IT risk management and IT compliance based on ISO standards. However we did not identify any other integrated framework, for instance, resulting from the literature review.

Research questions. Task 1 of the systematic literature review process is about specifying the research questions (see Fig. 1). For this review, we used PICOC method (i.e., population, intervention, comparison, outcome and context) to create a frame for formulating research questions [6]. For population we chose “Enterprises relying their processes on IT, tangling in complexity for IT governance, IT risk management and IT compliance”. Intervention to improve them would be “Integration of IT GRC”. For comparison we are “Comparing IT GRC state of the art studies done so far”. The outcome of this paper is ought to be “Integrated framework for IT GRC, leading to a better effectiveness and efficiency of these domains in organisations”. Context for the research are: Proceedings and Journals.

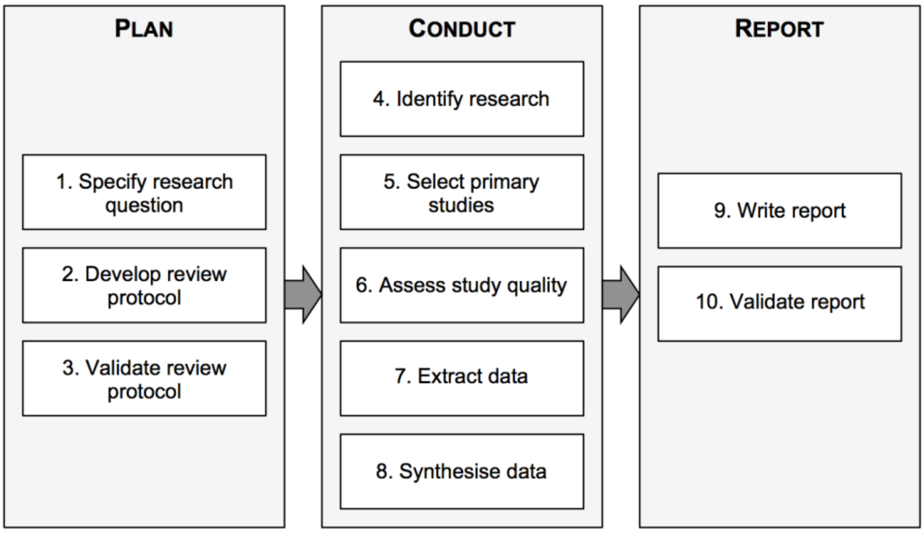

Fig. 1. Major steps for taking a systematic literature review. Three phases are expanded into tasks [6].

The main research question is *how IT governance, IT risk management and IT compliance could be integrated?* Based on the frame of reference for GRC research [10], we have broken it into four sub-questions:

SQ1. Which processes have been defined for IT GRC?

SQ2. What roles of people are involved for IT GRC?
SQ3. What strategy is used for IT GRC?
SQ4. What is considered as technology for IT GRC?

The review protocol has been designed as follows (task 2):

Search strategy. The search was performed over three libraries – *ACM Digital Library*[1], *IEEExplore*[2] and *SpringerLink*[3]. Search queries for these libraries were based on an initial pseudo-query, which was formed from the main research question: "(*IT or information technology*) *and* ((*governance and risk and compliance*) *or GRC*)". This query, however, was modified for each library according to its search capabilities.

Selection Criteria and Procedures. The search query is constructed so that the main emphasis is on IT GRC variants either in title, abstract (e.g., ACM Digital Library) or without context constraint (i.e., IEEExplore and SpringerLink). To decide which studies to include (or exclude), inclusion (and exclusion) criteria are applied. Regarding inclusion criteria, we have included the study if the study is reported as a journal, proceeding or book chapter publication, and if its title or abstract contained *GRC* (or *governance, risk* and *compliance*). At the opposite, we excluded studies that contained discussions over only one or two domains (e.g., COBIT [2], De Smet and Mayer [8], etc.) as they are not directly comparable and because our objective is to survey the specific topic of IT GRC as a whole. However, we acknowledge that some relevant input can be found in domain-specific studies. Papers with different meanings for the GRC acronym (e.g., ground response curve) were obviously not included in the study, as well as studies already included earlier. Finally, we excluded the studies, which were relevant to the IT GRC domain, but that does not contain the information needed to answer our research questions.

Quality checklists. To measure the quality, the resulting studies are divided into two groups – 1) method, approach or framework presentation and 2) empirical study, such as survey, case study or experiment. Following guidelines of the systematic research method, we have applied a list of quality evaluation criteria, which help us to assess quality of the selected studies. Sample of the evaluation criteria includes presence of (*i*) the problem statement, (*ii*) the research questions, (*iii*) the research method description, (*iv*) illustrative example or related work, (*v*) discussion, (*vi*) conclusion and similar.

Data extraction strategy. Data is extracted using extraction forms. The initial forms were built using four initial studies, out of which one turned out to use another's results for the basis of integration standard. Thereby current forms are based on three studies [9–11]. The data extraction form consists of two parts. Firstly, we gather factual information about the paper (e.g., date of extraction, extractor, paper title, authors, short overview and quality score). Secondly we extract the contextual information regarding (*i*) the processes defined for the IT GRC, (*ii*) roles of people involved in IT GRC, (*iii*) strategy used for IT GRC, and (*iv*) technology applied for IT GRC.

[1] http://dl.acm.org/
[2] http://ieeexplore.ieee.org/
[3] http://link.springer.com/

Finally, regarding protocol validation (task 3), the review protocol was basically created by the first author of this paper and validated in the iterative discussion among all the authors (i.e., in the manner of student and supervisor discussion as mentioned in [6]).

2.3 Systematic Literature Review Result

Task 4 from Fig. 1, *identify research*, results in search queries returning a total of 1444 results out of which were 168 from ACM, 105 from IEEE and 1171 from SpringerLink. After applying inclusion/exclusion criteria – task 5 – *select primary studies* to these results, 36 were included out of which 27 unique studies were left for *quality assessment (task 6)* and *data extraction (task 7)*. Main reasons for excluding the papers were: wrong acronym of GRC, not all domains were present or the scope of paper did not match with our corporate/IT GRC scope, or the quality indicators did not capture any required aspects.

After *quality assessment*, we have selected 7 primary studies. Due to small amount of studies found, the quality measure does not give an advantage in choosing sources of better quality amongst the seven included primary studies any more. Papers found suitable for the review are listed below:

- N. Racz, E. Weippl and A. Seufert, "Integrating IT Governance, Risk and Compliance Management Processes" [12].
- N. Racz, E. Weippl and A. Seufert, "Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives" [9].
- P. Vicente and M.M. da Silva, "A Conceptual Model for Integrated Governance, Risk and Compliance" [13].
- P. Vicente and M.M. da Silva, "A Business Viewpoint for Integrated IT Governance, Risk and Compliance" [10].
- M. Krey, "Information Technology Governance, Risk and Compliance in Health Care - A Management Approach" [11].
- D. Puspasari, M. Kasfu Hammi, M. Sattar and R. Nusa, "Designing a tool for IT Governance Risk Compliance: A case study" [14].
- A. Shahim, R. Batenburg and G. Vermunt, "Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies" [15].

Information is extracted from the studies into 4 categories: *processes, roles, strategies* and *technologies*. During extraction, we excluded from the results Mayer *et al.* [7] study. Although relevant, this study was firstly also reported as the secondary source in background study (see Section 2.2). Also we use this study to validate result of the current literature study (see Section 3.5). We have also excluded the paper by Racz *et al.* [16], since its results were recaptured in other two later papers by the same authors (see the list of selected papers).

The following sections present an overview of the extracted data from the included studies.

"Integrating IT Governance, Risk and Compliance Management Processes" [12], **"Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives"** [9]

The first paper introduces a high-level model from individual domain components as an artefact for IT GRC research knowledge base. IT governance process model is based on the ISO/IEC 38500:2008 standard for the corporate governance of IT. Its IT risk process model is derived from the COSO ERM framework. The IT Compliance is covered by the process model suggested by Rath and Sponholz [17]. This way the developed model helps answering the *SQ1*.

In the second publication the author's study presents a survey from GRC software vendors on their perceptions of state-of-the-art IT GRC software. The survey potentially contributes with some description on the technology aspects, thus contributing to the *SQ4*.

Processes: The proposed process model is vertically split into three separate GRC domains, where the processes and their flow have been captured. Main flows are going from compliance to risk and from risk to governance. *IT Governance* tasks are evaluating, directing, reporting and monitoring. *IT Risk* domain holds internal environment, objective setting, risk assessment, risk response, control activities, information and communication, and monitoring. *IT Compliance* starts with requirements analysis, and continues with deviation analysis, deficiency management, reporting/documentation, and deviation analysis.

Technology: GRC software vendors have different perspectives on which functionality should be delivered by GRC software. The paper did not specify technology or tools, but listed their functionalities without domain affiliation. We extracted the functionalities proposed from survey as following: (*i*) *governance* should be supported with surveys, reporting, dashboards, analytics, conducting controls testing and management, and workflow management; (*ii*) *risk management* should be performed through case, issue, event, remediation, loss management, and operational risk management; finally (*iii*) *compliance* should be supported by functions for policy, audit, and compliance management.

"A Conceptual Model for Integrated Governance, Risk and Compliance" [13], **"A Business Viewpoint for Integrated IT Governance, Risk and Compliance"** [10]

The first paper presents conceptual models for governance, risk and compliance. The proposed model is assessed against the OCEG Capability Model. The newly developed model is rather extensive but basically it contributes to answering the *SQ1*.

In the second paper authors continue developing the integrated model. Thus they align it with the GRC state of the art and enforce it with the approach introduced by Racz *et al.* [9, 12] (see above). The new contribution is focussed on the *business viewpoint*. The study concludes that there exists a strong relation between the IT GRC and enterprise/corporate GRC, where the high level processes can be executed in both domains. The second paper contributes with the GRC role description, thus potentially gives an answer to the *SQ2*.

Processes: The major functionalities of the integrated GRC model are *audit management*, *policy management*, *issues management* and *risk management*.

Roles: In the study, a sample of actors, their roles and categories are presented. This includes: (*i*) *leadership and champions*, (*ii*) *oversight personnel* (e.g., board of directors), (*iii*) *strategic personnel*, like C-suite (e.g., chief information officer, chief compliance officer, chief audit executive, chief financial officer, chief risk officer, chief operations officer), information systems and system owners, process owners, and (*iv*) *operational personnel* (e.g., key-users, governance, risk, audit, controls, legal and compliance managers).

"Information Technology Governance, Risk and Compliance in Health Care - A Management Approach" [11]

This paper presents results of a survey where Swiss hospitals' environment was assessed using the CobiT Maturity Model. Here, however, the risk and compliance processes are not explicitly described and only activities regarding governance are explicitly extracted as processes. The study contributes with some generic recommendations to achieve compliance, thus also contributing to the answer of *SQ1*.

Processes. IT governance is described through strategic alignment, value delivery, resource management, and performance measurement. *Strategic alignment* (Business-IT-Alignment) ensures the linkage of business and IT plans (aligns operations between IT and enterprise). It defines, maintains and validates the IT value propositions. *Value delivery* guarantees that the value proposition is executed throughout the delivery cycle to ensure that IT delivers the promised benefits, concentrating on cost optimization. *Resource management* ensures the proper investment in and management of critical IT resources such as information, infrastructure, applications and people. *Performance measurement* tracks strategy implementation, process performance, resource usage, etc.

Compliance is initiated (not covered) by three steps: (*i*) identifying good practices of dealing with laws and regulations, (*ii*) improving personnel awareness in regulatory requirements and, thereby, (*iii*) increasing process performance of an enterprise and compliance with laws and regulations**.**

"Designing a tool for IT Governance Risk Compliance: A case study" [14]

This paper defines the IT GRC domain and reviews studies about IT GRC frameworks. The results of the review are used to develop some GRC application used in the bank domain. The paper contributes with few data to answer the *SQ1*.

Processes. Firstly, some functionalities regarding GRC management are presented such as policy and controls library, IT control self-assessment and measurement, IT asset repository, remediation and control management, basic compliance reporting, IT compliance dashboard, IT risk assessment and controls, and policy mapping. Secondly, a high level top-down perspective is presented from the senior management point of view.

"Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies" [15]

This study defines an integrated GRC approach, where it positions GRC to the integrated strategic perspective. This allows assessing the GRC maturity and its alignment paths. Two case studies are presented to explain the drivers to measure the effect of business-IT alignment on performance. Those examples reveal that the companies, which align their business with the IT strategies, have an advantage over other companies. The authors provide guidelines to assess company GRC-maturity and define paths to achieve strategic alignment. This study contributes to the answers of the *SQ3* question.

Strategy: The strategic alignment model is divided into external and internal domains, which both are split to the business and IT domains. While strategic fit integrates the external and internal domains, the functional integration connects business and IT domains.

Authors also define four paths to reach strategic alignment in GRC. For instance, the *strategy execution* indicates that GRC organisational strategy and infrastructure (in business domain) are the basis for choosing the IT domain infrastructure. Another path describes *technology transformation*, which shows scenarios to develop GRC strategy in the business domain and GRC solutions in the IT domain. The *competitive potential* path lets the GRC solution lead the GRC strategy and infrastructure in the business domain. Finally, the *service level* path describes how the GRC strategy is adopted to the GRC solution and then integrated in the GRC organizational infrastructure.

2.4 Summary

First to notice, there was quite small amount of studies qualified for the review at hand. Although we planned to identify the state of the art in four categories (processes, roles, technology and strategy), the main emphasis was found on the *process* category – four studies address process aspects while roles, technology and strategy are each addressed by only one study. The answer to systematic review protocol's main research question, a driver for this research, will be addressed in the next section as the literature review part captured answers regarding state of the art of IT GRC.

3 A Framework for Integrated IT GRC

In this section, we aim to define a framework for integrated IT GRC based on the state of the art performed. The proposed framework shall be an instrument to adopt the IT GRC activities within a company. It is meant to help in establishing the needed processes and to assess the maturity of IT GRC activities in a company that already has some. The main target group for this framework would be companies, which need integrated IT GRC approach.

3.1 Integrated IT GRC model

To structure our proposed IT GRC framework, the approach is to synthesize data obtained during the systematic literature review into one model. As a base, we use the **frame of reference for integrated GRC** by Racz *et al.* [16] that is largely adopted according to the state of the art. In literature review, we tried to extract all four basic components of this frame of reference, i.e., strategy, processes, technology and people/roles. Since the review yielded results mostly in processes and extremely vaguely other components, we decided to use others as much as possible but main emphasis is on aligning processes to this triangle. As a consequence, we put the focus rather on GRC **main functionalities** as used by Vicente *et al*. [13] as the starting point for their conceptual model. These GRC main functionalities – *audit*, *policy*, *issue* and *risk management* – have been placed in the aforementioned GRC triangle. Finally, each main functionality is organized in our model around the **IT governance process flows** – *direct*, *evaluate*, *monitor* and *report* established by Racz *et al.* [18]. According to Racz *et al.*, "IT governance provides the frame for IT risk management and IT compliance decisions". To remove noise we left out groups which did not have any processes in (e.g. no *Direct* activities are related to *Audit management*). The resulting model is presented in Fig. 2.

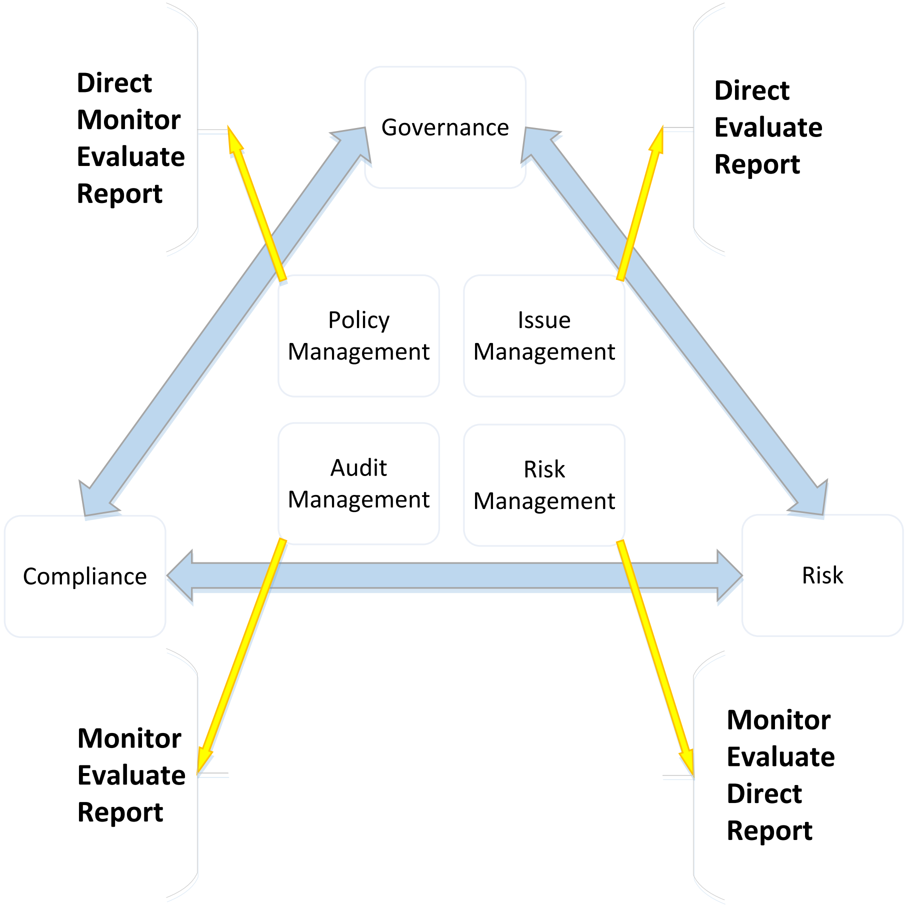

Fig. 2. The Integrated IT GRC model

3.2 Management processes of the four GRC main functionalities

Our main task to build our integrated IT GRC model is then to map the main findings obtained during the systematic review to the functionalities and process flows adopted. For each of the four GRC main functionalities (Audit, Policy, Issue and Risk management), we identify based on the systematic review the involved processes, associated roles and possible subprocesses. These processes are classified according to the process flow: *direct*, *evaluate*, *monitor* and *report*. Because of space limitation, only *Audit management* is detailed in this paper. The other GRC main functionalities are detailed in a technical report [19].

Audit management. Audit management consists in evaluating, reporting and monitoring tasks, since from the review results, its main tasks are focused on overseeing whether the compliance is obeyed. Following is the list of audit management processes and their definitions, as found in the literature. Audit management proposed processes and roles are presented in Fig. 3.

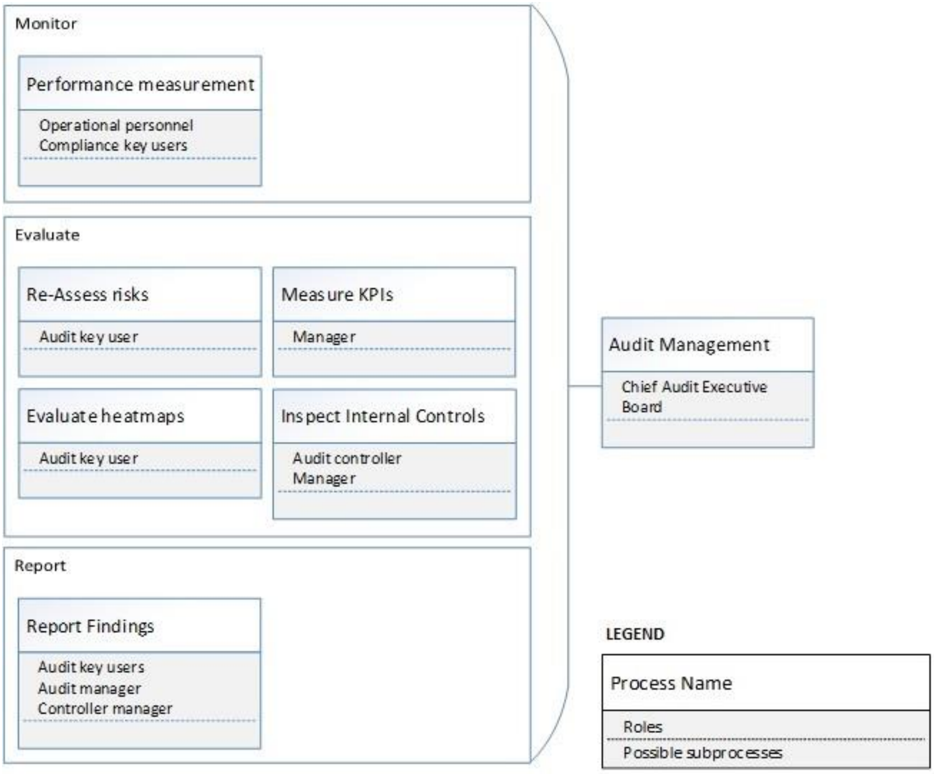

Fig. 3. Audit Management processes and roles

Audit management processes are:

- Evaluate
    - **Re-assess risks** – **risk assessment** – overall process of risk identification, risk analysis and risk evaluation [20].

    - **Inspect internal controls – (internal) audit** – “systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled” [21].
    - **Evaluate heatmaps** – evaluating current status of the auditable subject according to reported heatmaps [13].
    - **Measure KPI** (Key Performance Indicators) – measuring organization/IT/department performance using its agreed KPIs [13].
- Report
    - **Report compliance (-findings)** – “The governing body, management and the compliance function should ensure that **they** are effectively informed on the performance of the organization’s compliance management system and of its continuing adequacy, including all relevant non-compliances, in a timely manner” [21].
- Monitor
    - **Performance measurement** – “track and monitor strategy implementation, project completion, resource usage, process performance and service delivery, using, for example balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting” [7].

For each GRC main functionality, we use the following notation for presenting processes: the processes are displayed in a class diagram-like box as presented in Fig. 3, where process name is class name, proposed roles are above the line and possible sub-processes under the line in class members’ area. These processes are positioned in groups represented by rectangles with the group name in upper left corner. These groups are all connected by brace and form together the main functionality process put on the right side of the brace.

3.3 Implementation

To better visualise the IT GRC framework and help to assess companies’ maturity regarding IT GRC, a web application was developed[4]. The same components introduced in previous section are presented interactively. The main screen of the web application has the GRC-triangle in top of the screen including main functionalities and associated processes. Users can explore processes in the framework by clicking on these process flow elements. When clicking on the processes, a panel appears in the screen allowing performing a maturity assessment for each process related to the functionality. The maturity assessment of processes is performed on a scale of four items extracted from process assessment best practices: *Not achieved*, *Partially achieved*, *Largely achieved*, or *Fully achieved* [22].

[4] http://mihkel.joulukiri.ee

3.4 Validation

We have established a 2-step validation protocol aiming at validating the completeness and soundness of our proposal. First, we compared our framework with the ISO-specific one proposed by Mayer *et al.* [7]. In this work, Mayer *et al.* constructed an ISO-compliant IT GRC integrated model from the ISO standards related to the GRC individual domains. This framework has been chosen because its scope is equivalent to ours (i.e. IT GRC as a whole). Some more specific/focused ones, but better established, could also have been chosen in this validation step (e.g., COBIT for IT governance [2]). However, it would have only given a partial validation in terms of scope. The comparison is focused on processes, the ISO-compliant model of Mayer *et al.* being process-based. Then, as second step, the completeness and soundness of our model will be evaluated by a focus group composed of experts in the field, selected based on the systematic review results.

Comparison with the ISO-compliant IT GRC integrated model from Mayer *et al.* [7]. To compare the models, all the processes need to be processed in a comparable state. The comparison is done in a two-column table, both models being placed in columns and their functionalities/processes in rows accordingly. While detecting equivalence in the models, similar functionalities are grouped together in the same row or row-group (if several processes in one framework correspond to one in the second framework) and if no equivalence was found, an empty cell is on this row for the framework lacking the process. Details of this table can be found in a technical report [19].

In total we extracted 16 elements from Mayer *et al.* model and our model has 34 elements out of which 9 elements of Mayer *et al.* model corresponds to 14 elements in our model. 20 elements in our model have no direct correspondence in Mayer *et al.* model and 7 elements of Mayer *et al.* model have no correspondence in our model. As there are different numbers of corresponding elements in our model (14) to Mayer *et al.*'s model (9), Mayer *et al.*'s one had more compliance related elements, ours more risk management related elements. One assumption would be that the level of abstraction of the elements is not equal. In order to have them at the same abstraction level, more domain specific knowledge would be needed. Another finding is that, as Mayer *et al.*'s study based its framework on some non-IT specific reference documents (for the domains of risk management and compliance), the processes for their model are more generic and thereby have less details.

Validation with a focus group of experts. Second, we will assess the completeness and soundness of our model through a focus group. This focus group will be composed of authors of the papers selected during the literature review, as those authors were mainly in research groups dealing with the issue at hand and would be able to give the most relevant feedback. In addition to studies finally selected to be used in the review, the authors of all the relevant studies, which were excluded by some reasons, were also included to the focus group. This focus group will be asked to assess the proposed framework by going through the IT GRC framework web application (see Section 3.3) and complete a web form[5] associated to the framework. The feedback form consists of 4 pages split by main functionalities of the IT GRC framework (i.e. *Policy management, Issue management, Audit management and Risk management*), organized by process flows (i.e. *Direct, Monitor, Evaluate, Report*). Each process associated to functionality can be commented and assessed on the following scale: "definitely include", "maybe include", "maybe exclude" and "definitely exclude". This validation work is still in progress.

4 Concluding Remarks

In this paper, we described how we developed a framework for integrated IT GRC. The approach chosen was to perform first a systematic literature review of the IT GRC field. Following the systematic review protocol established, seven studies compose the results of our review. Then a proposal for the integrated IT GRC framework is made, based on a consolidation of the research results identified during the systematic review. This framework is implemented in a web application, to be used primarily as validation artefact. The proposed framework and its supporting web application are intended to assist companies to integrate their IT GRC processes. Application of the framework in real life could especially help assessing maturity of IT GRC according to the framework. Regarding future work, we first need to finish the validation work involving a focus group of experts and improve our model based on the conclusions drawn. Then, the use of our framework in an organization with a purpose of assessing IT GRC of this organisation will help us to check the adequacy and relevance of our approach.

Acknowledgments. Supported by the National Research Fund, Luxembourg, and financed by the ENTRI project (C14/IS/8329158).

References

1. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: Decker, B.D. and Schaumüller-Bichl, I. (eds.) Communications and Multimedia Security. pp. 106–117. Springer Berlin Heidelberg (2010).
2. ISACA: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. (2012).
3. ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management. International Organization for Standardization, Geneva (2011).
4. ISO/IEC 38500:2015: Information technology - Governance of IT for the organization. International Organization for Standardization, Geneva (2015).
5. Racz, N.: Governance, Risk and Compliance for Information Systems: Towards an Integrated Approach. Sudwestdeutscher Verlag Fur Hochschulschriften AG, Saarbrücken (2011).

[5] http://mihkel.joulukiri.ee/evaluate/renderform

6. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature Reviews in Software Engineering. School of Computer Science and Mathematics, Keele University (2007).
7. Mayer, N., Barafort, B., Picard, M., Cortina, S.: An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance). In: Systems, Software and Services Process Improvement: 22nd European Conference, EuroSPI 2015, Ankara, Turkey, September 30 – October 2, 2015. Proceedings. pp. 87–99. Springer International Publishing, Cham (2015).
8. De Smet, D., Mayer, N.: Integration of IT Governance and Security Risk Management: A Systematic Literature Review. In: 2016 International Conference on Information Society (i-Society). pp. 143–148 (2016).
9. Racz, N., Weippl, E., Seufert, A.: Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives. In: 44th Hawaii International Conference on System Sciences. pp. 1–10 (2011).
10. Vicente, P., da Silva, M.M.: A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In: 2011 IEEE World Congress on Services (SERVICES). pp. 422–428 (2011).
11. Krey, M.: Information Technology Governance, Risk and Compliance in Health Care - A Management Approach. In: 2010 Developments in E-systems Engineering. pp. 7–11 (2010).
12. Racz, N., Weippl, E., Seufert, A.: Integrating IT Governance, Risk, and Compliance Management Processes. In: Proceedings of the 2011 Conference on Databases and Information Systems VI: Selected Papers from the Ninth International Baltic Conference, DB&IS 2010. pp. 325–338. IOS Press, Amsterdam, The Netherlands, The Netherlands (2011).
13. Vicente, P., Silva, M.M. da: A Conceptual Model for Integrated Governance, Risk and Compliance. In: Mouratidis, H. and Rolland, C. (eds.) Advanced Information Systems Engineering. pp. 199–213. Springer Berlin Heidelberg (2011).
14. Puspasari, D., Hammi, M.K., Sattar, M., Nusa, R.: Designing a tool for IT Governance Risk Compliance: A case study. In: 2011 International Conference on Advanced Computer Science and Information Systems. pp. 311–316 (2011).
15. Shahim, A., Batenburg, R., Vermunt, G.: Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies. In: ICT Critical Infrastructures and Society. pp. 202–212. Springer, Berlin, Heidelberg (2012).
16. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: Decker, B.D. and Schaumüller-Bichl, I. (eds.) Communications and Multimedia Security. pp. 106–117. Springer Berlin Heidelberg (2010).
17. Rath, D.M., Sponholz, R.: IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Erich Schmidt Verlag GmbH & Co, Berlin (2009).
18. Racz, N., Weippl, E., Seufert, A.: A process model for integrated IT governance, risk, and compliance management. In: Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010. pp. 155–170 (2010).
19. Vunk, M.: A Framework for Assessing Organisational IT Governance Risk and Compliance, http://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=57229&year=2017, (2017).
20. ISO 31000:2009: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2009).
21. ISO 19600:2014: Compliance management systems — Guidelines. International Organization for Standardization, Geneva (2014).
22. ISO/IEC 33020:2015: Information technology – Process assessment – Process measurement framework for assessment of process capability. International Organization for Standardization, Geneva (2015).