UNIVERSITY OF TARTU
Institute of Computer Science
Software Engineering Curriculum

Mihkel Vunk

A Framework for Assessing Organisational IT Governance Risk and Compliance

Master's Thesis (30 ECTS)

Supervisor(s): Raimundas Matulevičius
Nicolas Mayer

Tartu 2017

A Framework for Assessing Organisational IT Governance Risk and Compliance

Abstract:

Today, enterprises have reached to understanding that Information Technology (IT) is more than just a technical issue. Disciplines such as IT governance, (IT) risk management and (IT) compliance have been established to steer it. Though, there has been some improvements, these domains are usually focused separately in silos, which raises a problem of performance and efficiency, where less business value is created due to complexity of the process flows. In order to cure it, there has been an adoption from business world, referred as "GRC" which covers all the three disciplines of governance, risk management and compliance. The paper conducts a systematic review on the discipline of IT GRC, taking out best practices. Researching what has been done to integrate them and proposing an synthesized framework from the review results. The framework, unifying the disciplines is supposed to ease the adoption of IT GRC in an enterprise, providing a structure to manage the IT and business together, thereby improve business performance. In addition to proposing an IT GRC framework, the paper presents a web application to support the framework adoption. The proposed model is based on the scientifically proven best practices of the state of the art which would give a certainty of its value. The empirical study will help to contribute to improving the effectiveness IT GRC compared to traditional approach which is commonly practiced in enterprises.

Keywords:

IT GRC, IT Governance, IT Risk management and IT Compliance

CERCS: P170 - Computer science, numerical analysis, systems, control

Organisatsiooni IT juhtimise, riskihalduse ja vastavuse raamistik

Lühikokkuvõte:

Ettevõtted on hakanud mõistma, et infotehnoloogias (IT) ei ole vaid tehnilised aspektid. IT haldamiseks on vaja (IT) juhtimist, (IT) riskihaldust ja (IT) vastavust. Klassikalise lähenemise kohaselt on kõigiga eraldiseisvana tegeldud, mis aga ei ole väga efektiivne – äri toodab väärtust ning kõiki protsesse püütakse optimeerida. Probleemi lahenduseks on ärimaailmast üle toodud paradigma „*GRC*“ (*Governance* – juhtimine, *Risk management* – riskihaldus ja *Compliance* – vastavus), mis need kõik omavahel ühendaks. Käesolev magistritöö esitleb süstemaatilist kirjandusülevaadet IT *GRC*-teemal ning selle tulemustest koostatud IT *GRC* raamistikku, mille eesmärgiks on lihtsustada ettevõtete pingutusi oma IT protsesside kohandamisel. Lõppkasutaja abistamiseks on loodud raamistikule ka veebirakendus, mis on abiks raamistiku kasutamisel. Loodud raamistik põhineb teaduslikel artiklitel ning on läbinud ka esmase validatsiooni.

Võtmesõnad:

IT GRC, IT Governance, IT Risk management and IT Compliance

CERCS: P170 - Arvutiteadus, arvutusmeetodid, susteemid, juhtimine (automaatjuhtimisteooria)

Table of Contents

1 Introduction

1.1 Motivation and scope

Enterprises are facing challenges at governing their Information Technology (IT) resources and needs effectively. Due to instability of the markets and the global financial system, globalization-led competition pressure and corporate disasters in last decades, all corporations need to have focused on their governance, risk and compliance (Corporate GRC) activities. 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. Main problem of the topic is to have the domains activities as integrated as possible.

The scope of this paper is to define a framework for IT governance, risk management and compliance.

1.2 Research questions

To set clear goals of this paper, we hereby state the research questions, to which we seek answers. The main driving question, RQ is stated as following: "*How IT governance, IT risk management and IT compliance could be integrated?*".

In order to know, what it is and what has been done, try to find answer to the question SRQ1: "*What is the state of the art of IT GRC?*", thereby we conduct a systematic literature review. After finding out the state of the art methods, we try to combine them into one framework by finding answer to SRQ2: "*How IT GRC state of the art could be combined into the IT GRC framework?*". In order to support the accessibility and usability of the proposed framework for a potential end user, we need to find answer to SRQ3: "*How IT GRC assessment could be supported?*". This leads us to developing a web application.

As our work was initiated by similar research done based on ISO standards by [Mayer, 2011], it is important to know, differences between literature review-based framework and ISO standards based – question to answer is SRQ4: "*What are similarities and differences of our IT GRC framework to the Mayer et al ISO standards model?*". And lastly, the proposed framework is validated regarding completeness by conducting a focus group presentation and survey to answer SRQ5: "*What is completeness of IT GRC framework?*"

1.3 Summary of contribution

The paper presents a systematic review on the discipline of IT GRC, using *Guidelines for performing Systematic Literature Reviews in Software Engineering* by Kitchenham as an oracle. The review is done in two iterations – development of the protocol and following the protocol. During the protocol development, one digital library is used and all of the initial presumptions and rules are adapted to get the most relevant results. After approval of the protocol it is used in other libraries which are targeted with rules defined in the first iteration.

For contribution we propose a synthesis of the results from the literature review, resulting in an IT GRC framework proposal. To validate our developed framework, we have two steps: theoretical validation and usability/completeness testing. Theoretical validation is to map proposed framework with an analogue derived from ISO standards [Mayer, 2011]. Usability testing consisted of developing a web application and presenting it to the focus group to gather data and make conclusions based on that.

1.4 Structure

The paper is organised as follows: section 2 firstly, presents and describes the *review protocol*, and secondly, presents the *results of the review*. Section 3 presents our contribution in *improving IT-GRC framework.* In section 4, a web application for supporting the IT GRC framework is presented. In section 5 is a comparison of the proposed IT GRC framework against Mayer et al ISO standards model. Section 6 consists of the completeness validation process of the proposed framework and its results. Finally, section 7 concludes the papers results. All tables, referred with letter "a", for example Table a1, can be found under appendixes.

2 Systematic Review of IT GRC

In this chapter, we present a systematic literature review and its components regarding IT Governance, Risk and Compliance. The chapter aims to answer the question: SRQ1: "*What is the state of the art of IT GRC?*". Firstly, we describe the research method, secondly define the review protocol and thirdly, present the individual results from all the sources as proposals for the state of the art.

2.1 Systematic Review Method

The methodology used in this research is systematic literature review. "A *systematic literature review* (or systematic review) is a mean to identify, evaluate and interpret all available research relevant to a particular research question, topic area or phenomenon of interest" [Kitchenham, 2007]. In particular, we are using guidelines for systematic reviews, proposed by Kitchenham, which are designed for software engineering researchers [Kitchenham, 2007].

Most common reasons to take a systematic literature review are *to summarise* the existing empirical evidence, to *identify gaps in current research* or *to provide a framework or background* for new research activities. More deeply, the main rationale to undertake a systematic review is of its scientific value of being thorough and fair. This is achieved by the strict rules that the review must comply with [Kitchenham, 2007].

Systematic reviews start by defining a *review protocol* to embody rules and artefacts for the review. These artefacts usually consist of: ***background, research questions, search strategy, study selection criteria & procedures, study quality assessment checklists*** *& procedures, synthesis strategy of the selected data, dissemination strategy*. This protocol will help to execute the steps of a systematic review in a controlled manner.

Our followed review steps are split into three phases – "plan, conduct, report", which consist of tasks, involving the artefacts previously listed in bold. Phases of our review are presented in Figure 1 below. The last phase, reporting involves writing the report of the results and circulating them to potentially interested parties [Kitchenham, 2007].

Figure 1. Major steps for taking a systematic literature review. Three phases are expanded into tasks [Kitchenham, 2007].

2.2 Systematic Review Protocol

As in Figure 1, the first task in planning phase of conducting systematic review is to **specify the research questions**. In order to state them, we define the *background* in which context

the research questions shall be asked. The background section of the protocol confirms the need for the survey and supports the research questions. Research questions are divided as *main research question* and *sub-questions*.

The second task in the planning phase is to **develop the review protocol**. Artefacts from the first step are taken as a basis for developing the protocol. Then, a *search strategy* is defined to find as much relevant literature answering the research questions in an unbiased manner. The search strategy is documented for later possible assessment of the validity of results. After search strategy, *selection criteria and procedures* are defined as the rules for, and the way how to, include or exclude the search results in the systematic review. The studies included for the review should pass the quality assessment. *Quality assessment* section might give additional inclusion/exclusion criteria, help explaining differences in study results, allowing to weight the studies in synthesising step. Lastly, *data extraction strategy* defines how the information from each of the primary study will be obtained [Kitchenham, 2007].

Third task in planning phase, is to test run the developed review protocol in a restricted scope of conducting phase. This helps to validate whether the rules give results and allow to modify details of the protocol. After this task, the protocol remains intact.

Background. Today, enterprise processes have become so complex, Information Technology (IT) is more than just a technical issue. IT with its importance in an enterprise involves a governance layer which is steered by IT risk management and IT compliance. These disciplines (IT governance, IT risk management and IT compliance) are commonly dealt separately in silos. From the business world comes a paradigm, referred as „GRC“, covering all the three disciplines of governance, risk management and compliance. The challenge is to have an approach as integrated as possible to improve efficiency and effectiveness of the three disciplines in IT GRC [Mayer, 2015]. This review is conducted to find the state of the art of IT GRC based on scientific literature.

Research questions. For this review, we used PICOC method (*Population, Intervention, Comparison, Outcome* and *Context*) to create a frame for formulating research questions [Kitchenham, 2007].

For *population* we chose “Enterprises relying their processes on IT, tangling in complexity for governing, 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 efficiency of these domains in organisations”. *Context* for the research are: “Proceedings, Journals”.

Main research question, based on Intervention criteria was designed as RQ. In order to answer to this question, we break the domain apart into four sub-questions – SQ1, SQ2, SQ3 and SQ4, which are based on the frame of reference for GRC research [Racz, 2010].

- **RQ -** “How IT governance, IT risk management and IT compliance could be integrated?”;
- **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?”.

Search strategy – While planning the review it was agreed that the search will be done 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 research question RQ. The pseudo-query was formed as: "(IT or information technology) and ((governance and risk and compliance) or GRC)" which was modified for each library according to its search capabilities. Search queries for all three libraries are presented in table a2.

From this point the overall review process was split into two phases – firstly piloting the protocol on ACM Digital Library to get initial results, validate and modify the protocol. Second phase was to include IEEExplore and SpringerLink digital libraries and repeat the steps developed in phase one. Search result lists were downloaded as csv, imported to MS Excel and normalized to ease processing.

Selection Criteria and Procedures – The search query is constructed so that the main emphasis is on IT GRC variants either in title, abstract (ACM Digital Library) or without context constraint (IEEExplore and SpringerLink). It would be too broad to analyse each domain of IT GRC separately in given timeline for this project, therefore search query assures we should have a variant of IT GRC in resulting studies, but it still returns many irrelevant results.

To decide which studies to include or exclude, inclusion and exclusion criteria is applied to results in selection phase. Study was included if full IT GRC presence (all three domains, governance, risk and compliance) is captured in title. After going over the titles, studies not yet included nor excluded, were screened for GRC in abstracts. Results having only one or two domains present have no value to our review since they are not directly comparable. If the study does not coincide with any of the inclusion or exclusion criteria, it will be excluded.

The selection criteria checklist is presented in table a3. Firstly, 1.1. and 1.2. criteria are about the type of the study, which were agreed to include only journals, proceedings and chapters. Criterion 1.3. is about duplicate studies, which are not included twice. Criteria 2.1. and 2.2. are about GRC other meanings in titles, which stood out during developing the protocol. The same applies to abstract in selection criteria 3.1. and 3.2. Last criterion is 4.1., the final check which is done in data extraction step because it is about processing the papers content and contribution. Thereby after initial selection process, when data extraction reveals some exclusion criteria and no usable data can be found, the study is excluded.

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. After grouping, the evaluation is done according to table a4. If the study has no quality, it is harder to use it in extracting the results or id does not have anything to extract.

Data extraction strategy – Data is extracted using extraction forms. The initial forms were built using 4 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 (Racz, 2011a; Vicente & Silva, 2011a; Krey, 2010). Data extraction form is presented in table a5 in the appendixes and all the proceeding tables are filled data extraction forms for the individual studies.

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

2.3 Review results

Task 4 from Figure 1, *identify research*, results in search queries returning 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.

The tasks 6 and 7 were done together, more exclusions were made and finally 10 studies were included for the review out of which half were returned by more than one library. Due to small amount of studies found, the quality measure does not give an advantage in choosing sources of better quality amongst the 10 included studies any more. Papers found suitable for the review are listed below:

- **A. Shahim, R. Batenburg and G. Vermunt et al. „Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies“ [Shahim, 2012].**
- **D. Puspasari, M. Kasfu Hammi, M. Sattar and R. Nusa et al. „Designing a tool for IT Governance Risk Compliance: A case study“ [Puspasari, 2011].**
- **M. Krey et al. „Information Technology Governance, Risk and Compliance in Health Care - A Management Approach“ [Krey, 2010].**
- N. Racz, E. Weippl, A. Seufert et al.
    - „A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)“ [Racz, 2010].
    - **„Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives“ [Racz, 2011a].**
    - **„Integrating IT Governance, Risk, and Compliance Management Processes“** [Racz, 2011b].
- N. Mayer, B. Barafort, M. Picard and S. Cortina et al. „An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance)“ [Mayer, 2015].
- P. Vicente and M.M. da Silva et al.
    - **„A Business Viewpoint for Integrated IT Governance, Risk and Compliance“ [Vicente, 2011a].**
    - **„A Conceptual Model for Integrated Governance, Risk and Compliance“ [Vicente, 2011b].**

Information is extracted from the studies into 4 categories: *processes, roles, strategies* and *technologies*. During extraction, we excluded from the results (non-bold from previous list) Mayer et al (will be control model to compare the results with) and Racz 2010. et al (the approach for the research originated from this study) studies. The following sections present an overview of extractions of the studies included.

N. Racz, E. Weippl and A. Seufert et al. "Integrating IT Governance, Risk and Compliance Management Processes" [Racz, 2011b]

The study introduces a high-level model from individual domain components as an artefact for IT GRC research knowledge base. IT Governance process model is taken from *ISO/IEC 38500:2008 – Corporate governance of IT*; IT Risk process model is derived from *COSO ERM framework* and IT Compliance is covered by *process model suggested by Rath and Sponholz* book [Rath. M. & Sponholz, R, 2009]. The model proposed (Figure 2), is suitable answering processes sub question SQ1.

Processes

The proposed process model is vertically split into three separate GRC domains, where the processes and their flow has 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 & communication and Monitoring.* **IT Compliance** starts with *Requirements analysis, Deviation analysis, Deficiency management, Reporting/documentation and Deviation analysis.*

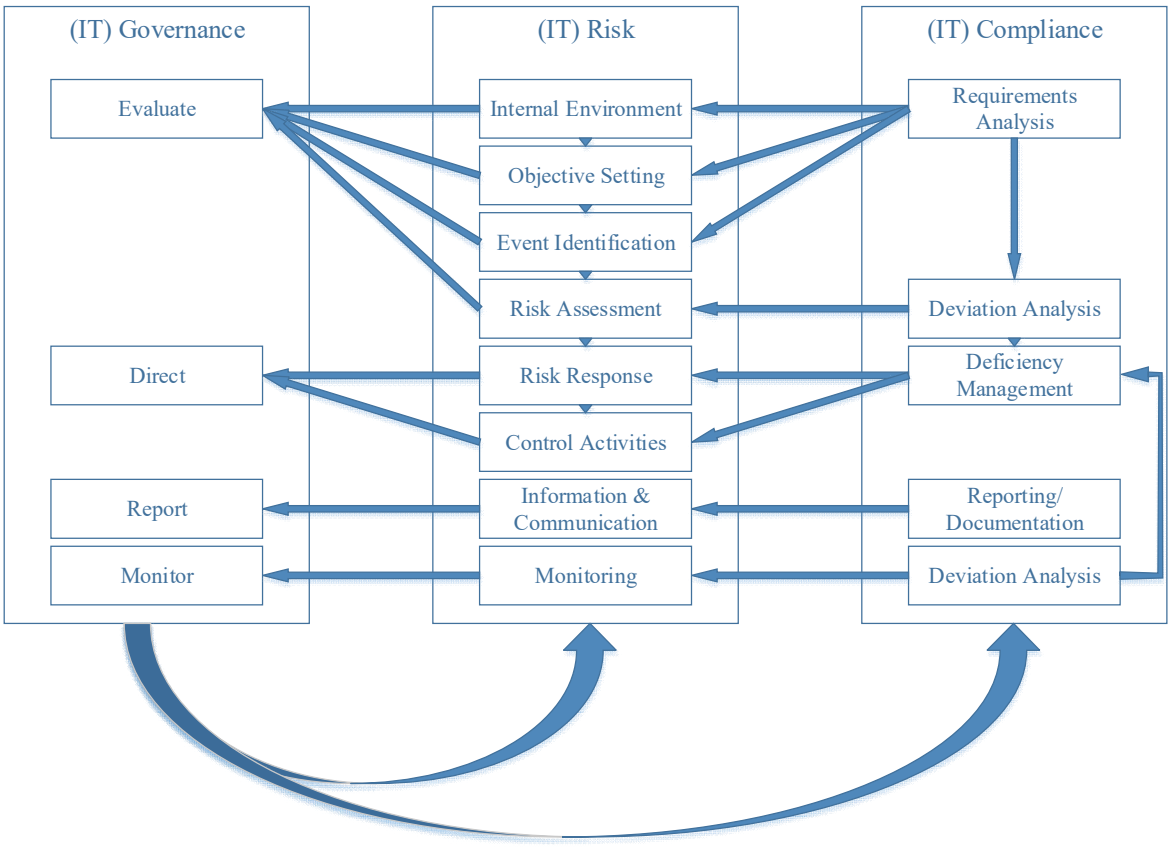

Figure 2. Process model for integrated IT GRC management [Racz, 2011]

N. Racz, E. Weippl and A. Seufert et al. „Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives“ [Racz, 2011a]

The study presents a survey from GRC software vendors on their perceptions of state-of-the-art IT GRC software. Since the survey was designed with open-ended questions, which were clarified afterwards, some inaccuracies might be introduced while interpreting the results. The survey might provide us some answers about technology sub-question SQ4. They recommend to base the future research on scientifically applied software engineering rather than purely on results they found.

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:

Governance involves using *surveys, reporting/dashboards/analytics*, conducting *controls testing and – management* and *workflow management.*

Risk Management consists of *risk management, case/issue/event/remediation/loss management* and *operational risk management.*

Compliance involves *policy management, audit management* and *compliance management.*

P. Vicente and M.M. da Silva et al. „A Business Viewpoint for Integrated IT Governance, Risk and Compliance“ [Vicente, 2011a]

The paper researches GRC state of the art and constructs a Business Viewpoint by combining Racz et al. “A Frame of Reference for Research of Integrated GRC”, Racz et al. “A Process Model for Integrated IT GRC Management” and Vicente & Silva et al. “A Conceptual Model for Integrated GRC”. They reach to a conclusion that there is a strong relation between IT GRC and enterprise GRC i.e., the described high level process can be used for both of the domains.

Since our research includes all three references, this paper uses for constructing the Business Viewpoint, we are not using the model, but examples of some GRC roles described, could answer to roles’ sub question **SQ2**.

Roles

Authors chose not to represent the actors and roles within ArchiMate language and include them into a viewpoint. They brought out just some examples of actors, roles and categories without assigning them to the parts of the model:

- Leadership and champions
- Oversight personnel
    - Board of Directors
- Strategic personnel
    - C-suite - 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

- Operational personnel
  - Key-users
  - Governance, risk, audit, controls, legal and compliance managers.

P. Vicente and M.M. da Silva et al. „A Conceptual Model for Integrated Governance, Risk and Compliance“ [Vicente, 2011b]

The paper presents developing individual conceptual models for governance, risk and compliance, integrating them into one model and evaluating it against OCEG Capability Model. The model is quite extensive and thereby we extract only the parts overlapping the most in the domains, answering to the review sub question SQ1.

Processes

Although the initial, individual domain models of GRC included monitoring, dashboards and reporting, authors, opted to leave these out from the integrated model. We also leave out detailed information which is not overlapping through all three domains. Resulting extracted model is presented in Figure 3.

The rectangular concepts, coloured orange, stand for what they propose to be the GRC main functionalities: audit management, policy management, issues management and risk management. The concepts, in green rectangles, represent information that is managed by these functionalities or are presented as a responsibility of the G, R or C areas.

Authors did not assign any roles to the activities, thereby after establishing the structure from the model, the responsibilities need to be divided and properly associated roles present in enterprise [Vicente, 2011b].

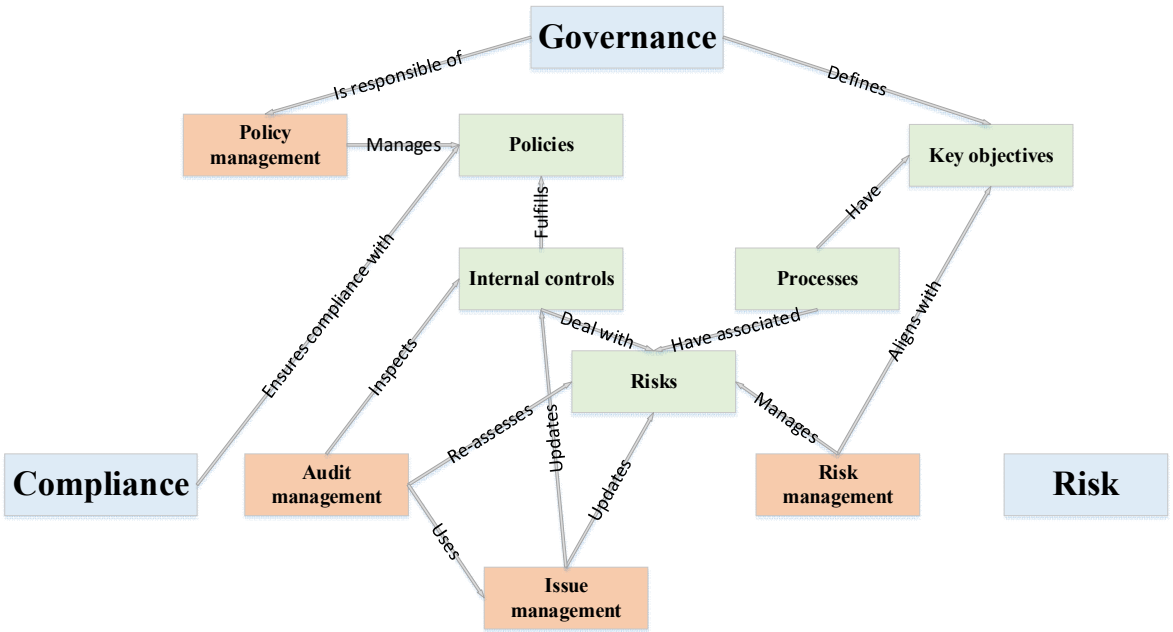

Figure 3. Generalization of Integrated GRC Conceptual Model by Vicente et al.

M. Krey et al. „Information Technology Governance, Risk and Compliance in Health Care - A Management Approach“ [Krey, 2010]

The paper presents results of a survey comapring Swiss hospitals' environments against CobiT Maturity Model. CobiT framework is taken as a GRC approach (Figure 4). Since risk and compliance processes are not explicitly described, only activities regarding governance are extracted as processes. For compliance some general recommendations are mentioned. This study contributes answering review sub question SQ1.

Processes

IT governance is covered by four focus areas. *Strategic alignment* (Business-IT-Alignment) ensuring the linkage of business and IT plans (aligns operations between IT and enterprise). It defines, maintains and validates the IT value propositions. *Value delivery* makes sure 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 – *identifying of good practices* of dealing with laws and regulations and *improving personnel awareness* in regulatory requirements thereby *increasing process performance of* an enterprise *and compliance* with **laws and regulations [Krey, 2010].**

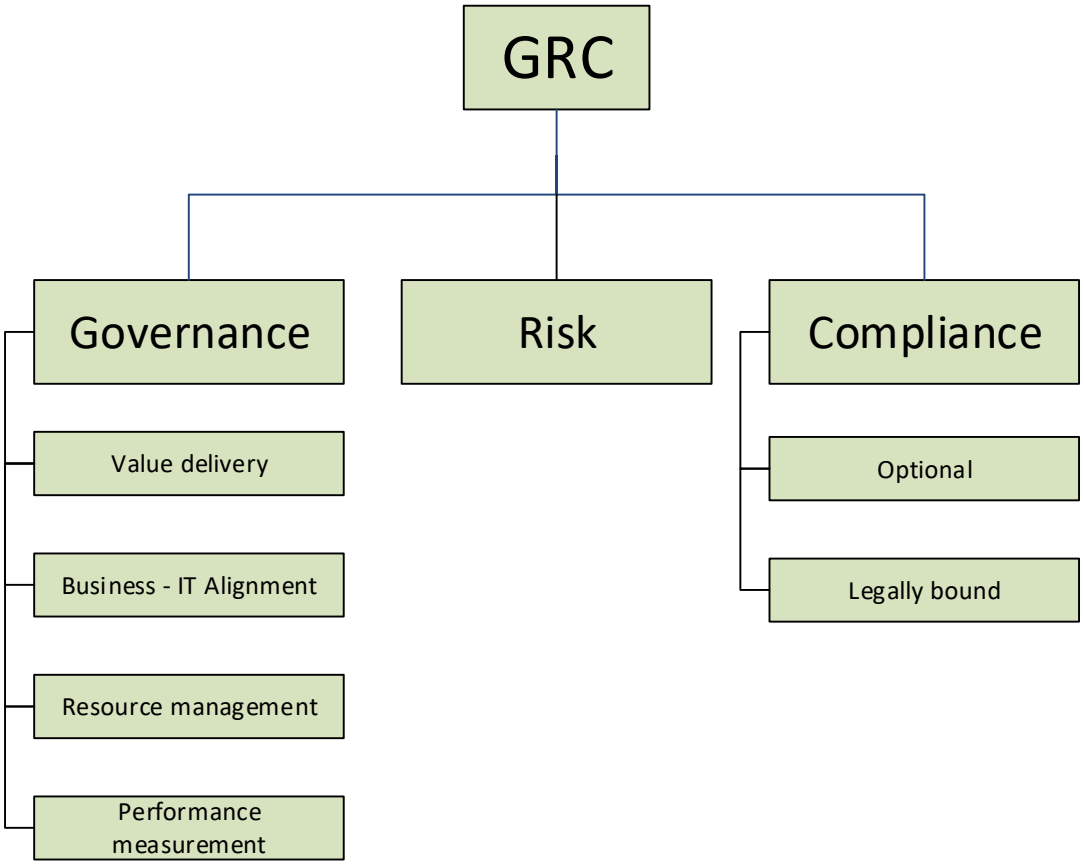

Figure 4. GRC approach based on CobiT framework [Krey, 2010]

D. Puspasari, M. Kasfu Hammi, M. Sattar and R. Nusa et al. „Designing a tool for IT Governance Risk Compliance: A case study“ [Puspasari, 2011]

The paper defines IT GRC domain and reviews studies about IT GRC frameworks. The results of the review are used to develop a bank's GRC application. Although the contribution part of the study is out of our scope and too specific, we can extract some data from the review results to answer our review sub question SQ1.

Processes

Firstly, some functionalities regrading 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 (Figure 5) from senior management is given. Although it is poorly decribed, but from where some interactions between the domains have been captured.

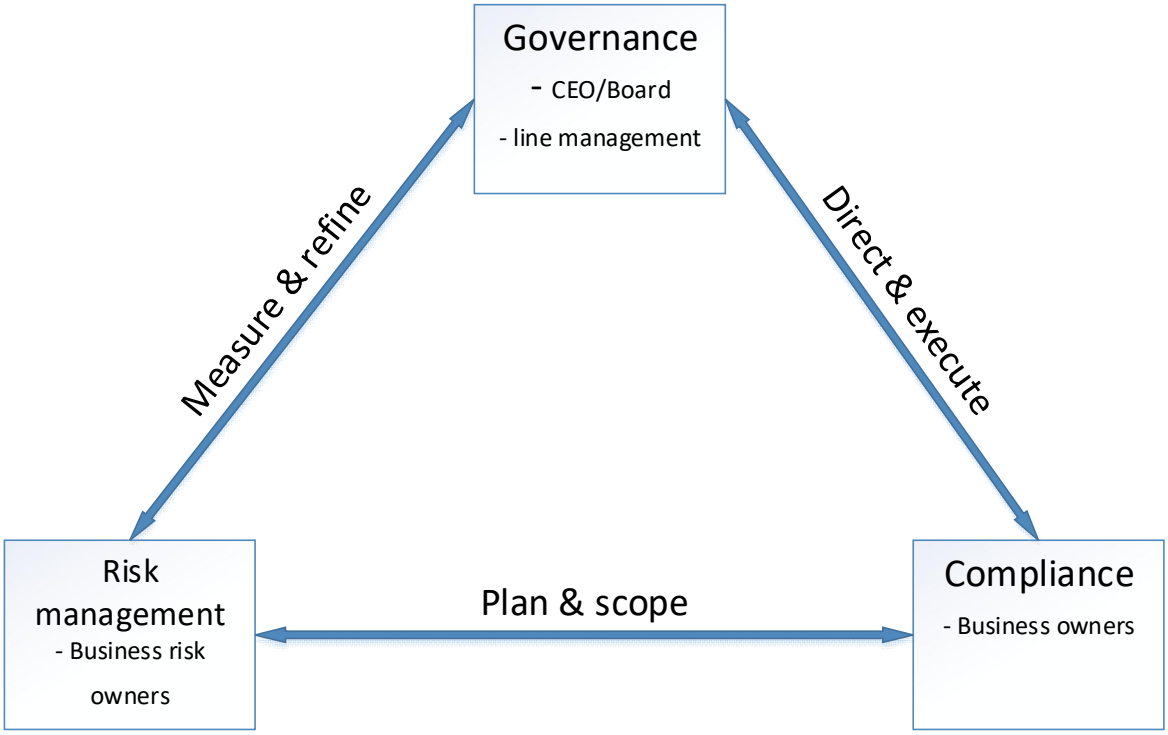

Figure 5. Governance guidelines

A. Shahim, R. Batenburg and G. Vermunt et al. “Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies” [Shahim, 2012]

The paper defines integrated GRC, then positions GRC into an integrated strategic perspective allowing to assess the GRC maturity and its alignment paths. Two case studies are presented to explain the issue more thoroughly.

The drivers for this paper are the studies dedicated to measuring the effect of business-IT alignment has on performance. Those studies reveal that the companies which align their business with their IT strategies effectively, have an advantage over companies which do not. The authors provide guidelines to assess company GRC-maturity and define paths to achieve strategic alignment. The study answers our review's strategy sub question **SQ3**.

Strategy

The strategic alignment model is divided into external and internal domains, both have business and IT domain – so altogether 4 domains. While strategic fit integrates the external and internal domains, functional integration connects business and IT domains. The model is presented on Figure 6. Integration and functional fit is presented with bold arrows.

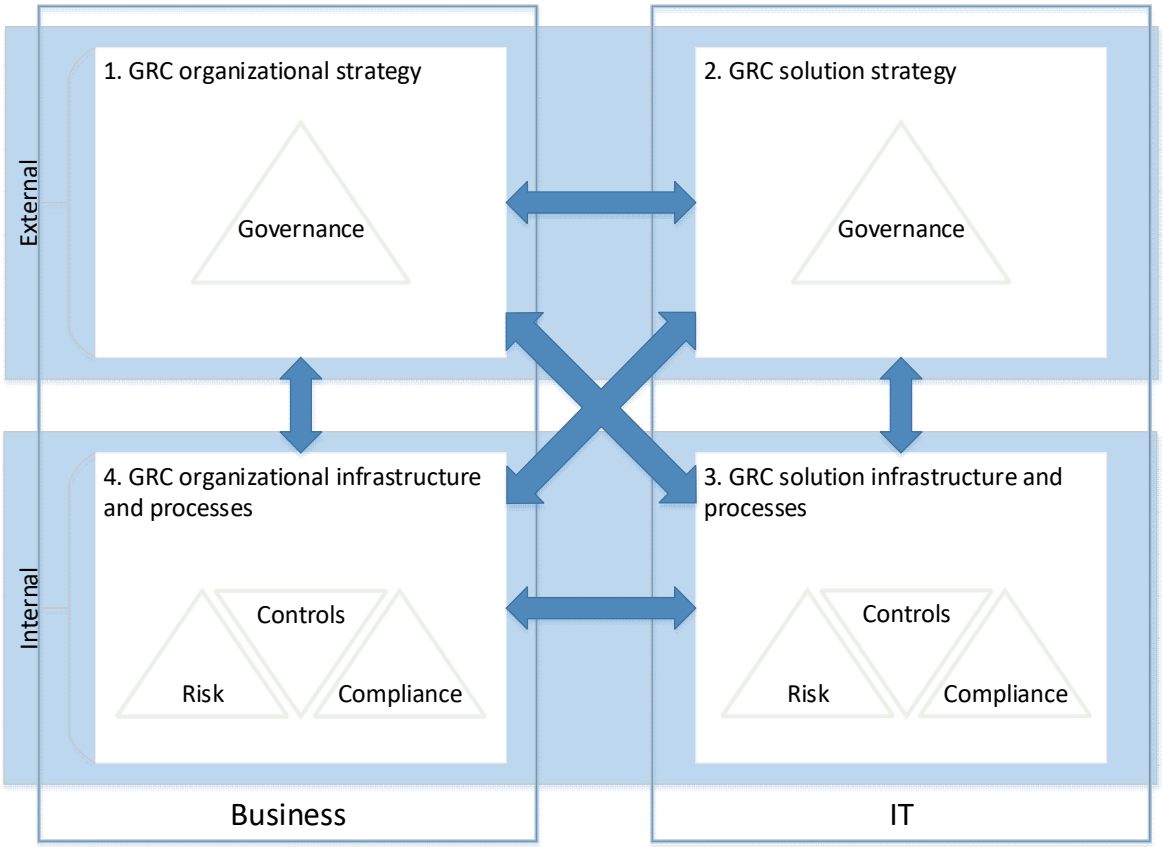

Figure 6. The GRC strategic alignment model [Shahim, 2012]

Authors defined four paths to reach strategic alignment in GRC. The paths are presented in Figure 7. Path A, **strategy execution**, indicates that GRC *strategy and infrastructure in business domain* are a basis for choosing, in *IT domain, a GRC solution* suitable *between business and IT domain infrastructure*. Path B, **technology transformation** shows a scenario where *GRC strategy is developed in business domain* and *GRC solution in IT domain* is chosen which concurs this strategy. The GRC solution infrastructure is embedded in the organization. Path C, **competitive potential**, lets the *GRC solution strategy* lead the *GRC strategy and infrastructure in the business domain*. Path D, **service level** lets the vision of *GRC strategy, adopted in the GRC solution*, to be *integrated in the GRC organizational infrastructure* [Shahim, 2012].

Figure 7. Paths to reach strategic alignment in GRC strategic alignment model [Shahim, 2012].

2.4 Summary

First to notice, there was quite small amount of studies qualifying 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 processes category – four studies and one study for all the rest. The answer to systematic review protocol's main research question, a driver for this research, will be adressed in the paper's forecoming chapters as the literature review part captured answers regarding state of the art of IT GRC.

3 Framework for integrated IT GRC

In this chapter, we aim to answer the question SRQ2: "How IT GRC state of the art could be combined into the IT GRC framework?". Last task in conducting phase of the review is to synthesize data (Figure 1) into one model. This chapter begins by defining purpose and audience for the framework then collects the definitions for GRC and then explains the structure of our proposed IT GRC framework.

3.1 Purpose and audience of framework

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.

3.2 Definitions

Here we conclude the definitions different papers have taken as a basis for the GRC research.

GRC *"GRC is 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."* [Racz, 2011a].

GRC (OCEG) *"a system of people, processes and technology that enables an organization to understand and prioritize stakeholder expectations, set business objectives congruent with values and risks, achieve objectives while optimizing risk profile and protecting value, operate within legal, contractual, internal, social and ethical boundaries, provide relevant, reliable and timely information to appropriate stakeholders, and enable the measurement of the performance and effectiveness of the system"* [Shahim, 2012].

Corporate Governance of IT *„the system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the plans for the use of IT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organisation"* [ISO/IEC 38500:2008].

Governance *"governance is the culture, values, mission, structure, layers of policies, processes and measures by which organizations are directed and controlled"* [Vicente, 2011b].

Risk management *"the systematic application of processes and structure that enable an organization to identify, evaluate, analyse, optimize, monitor, improve, or transfer risk while communicating risk and risk decisions to stakeholders"* [Vicente, 2011b].

Enterprise Risk Management *„a process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"* [Racz, 2011a].

Compliance *"compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies"* [Vicente, 2011b].

3.3 Integrated IT GRC model

Regarding other components, technology findings are merged to corresponding processes due to small number of results in technology components. We assume that strategies are meant to 1) be managed mainly by governance, 2) be established outside of given processes and thereby are not explicitly separate component in our model. According to second assumption, our model should be aligned to support business and IT strategies as shown in Figure 6 and 7, accomplished with alignment path A or B [Shahim, 2012].

As a base, we use the frame of reference GRC-triangle for integrated GRC by Racz et al (Figure 7). In literature review, we tried to extract all four basic components of the frame of reference – 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.

Our integrated IT GRC model is presented on Figure 8, where we put GRC **main functionalities** the same as [Vicente, 2011b] took as the starting point for the conceptual model. These GRC main functionalities – *audit-*, *policy-*, *issue-* and *risk management* have been placed in the aforementioned GRC triangle. Yellow arrows are, pointing to the **ordered process flows** of four groups – *direct*, *evaluate*, *monitor* and *report.* The processes were mapped to functionalities and process flows one by one, ttrying to find best match for each process.

The process flow grouping comes from governance standard [ISO/IEC 38500:2015] and was adopted to all of the domains in order to have the governance viewpoint. To remove noise we left out groups which did not have any processes in. This means that the functionality either does not have this group processes or they weren't captured in our review sources. These flows are assumed to be in continuous loops and consist of processes described in next 4 sections.

For the next sections we use following notation for presenting processes – the processes are displayed in a class diagram-like box as presented in Figure 9, where process name is class name, proposed roles above the line and possible subprocesses 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.

Audit management

Audit management consists of more evaluating, reporting and monitoring tasks, since from the review results, its main tasks seem to be more of overseeing whether the compliance is obeyed. Following, is the list of audit management processes and their definitions, if adequate one was found. Audit management proposed processes and roles are presented on Figure 10.

Audit management processes are:

- Evaluate
    - **Re-assess risks** – **risk assessment** – overall process of risk identification, risk analysis and risk evaluation [ISO 31000:2009].

- **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“ [ISO 19600:2014].
- **Evaluate heatmaps** – evaluating current status of the auditable subject according to reported heatmaps.
- **Measure KPI** (Key Performance Indicators) – measuring organization/IT/department performance using its agreed KPIs.

- Report
  - **Report compliance (-findings)** – **compliance reporting** – „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 noncompliances, in a timely manner..“ [ISO 19600:2014].
- 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” [Krey, 2010].

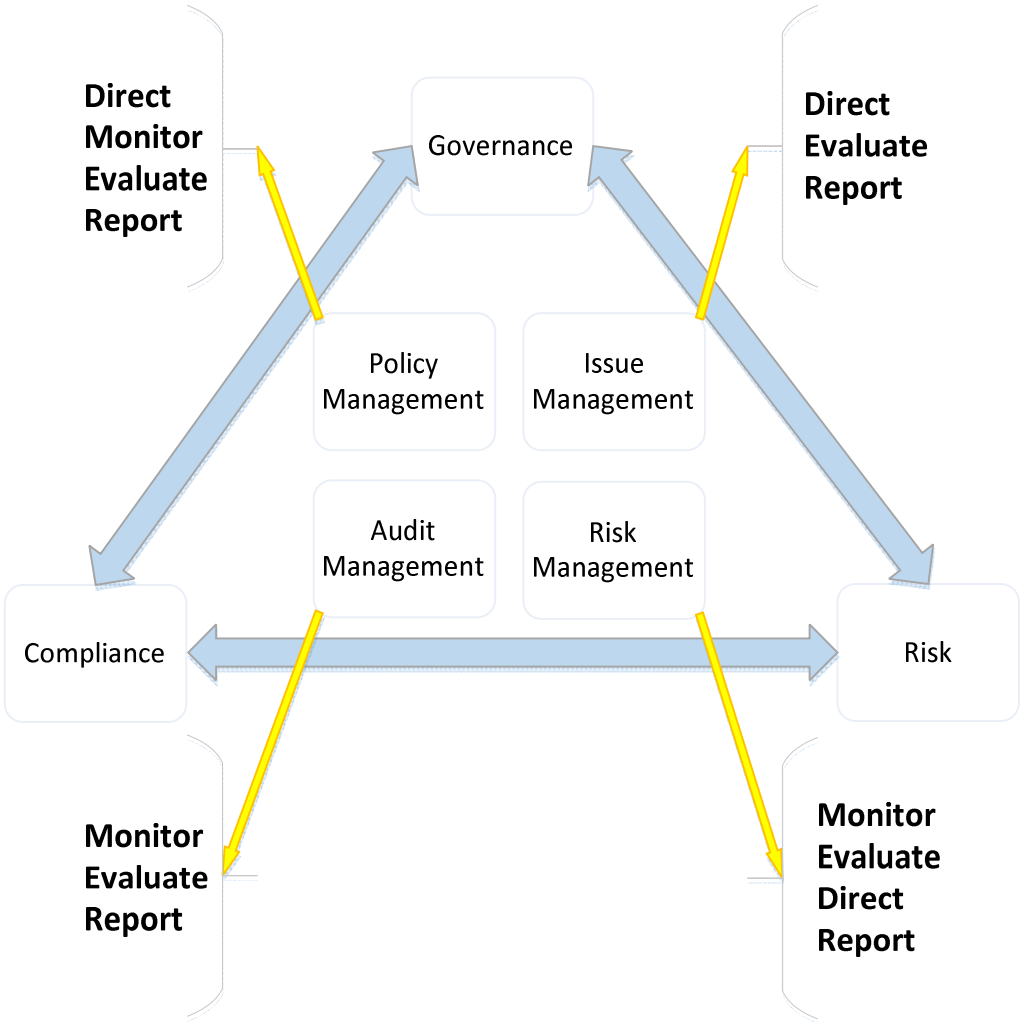

Figure 8. Integrated IT GRC model with clarified high-level GRC management processes

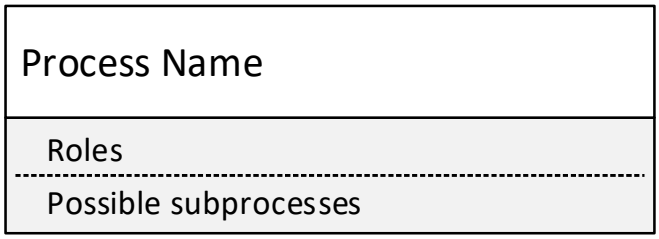

Figure 9. Process notation for the model

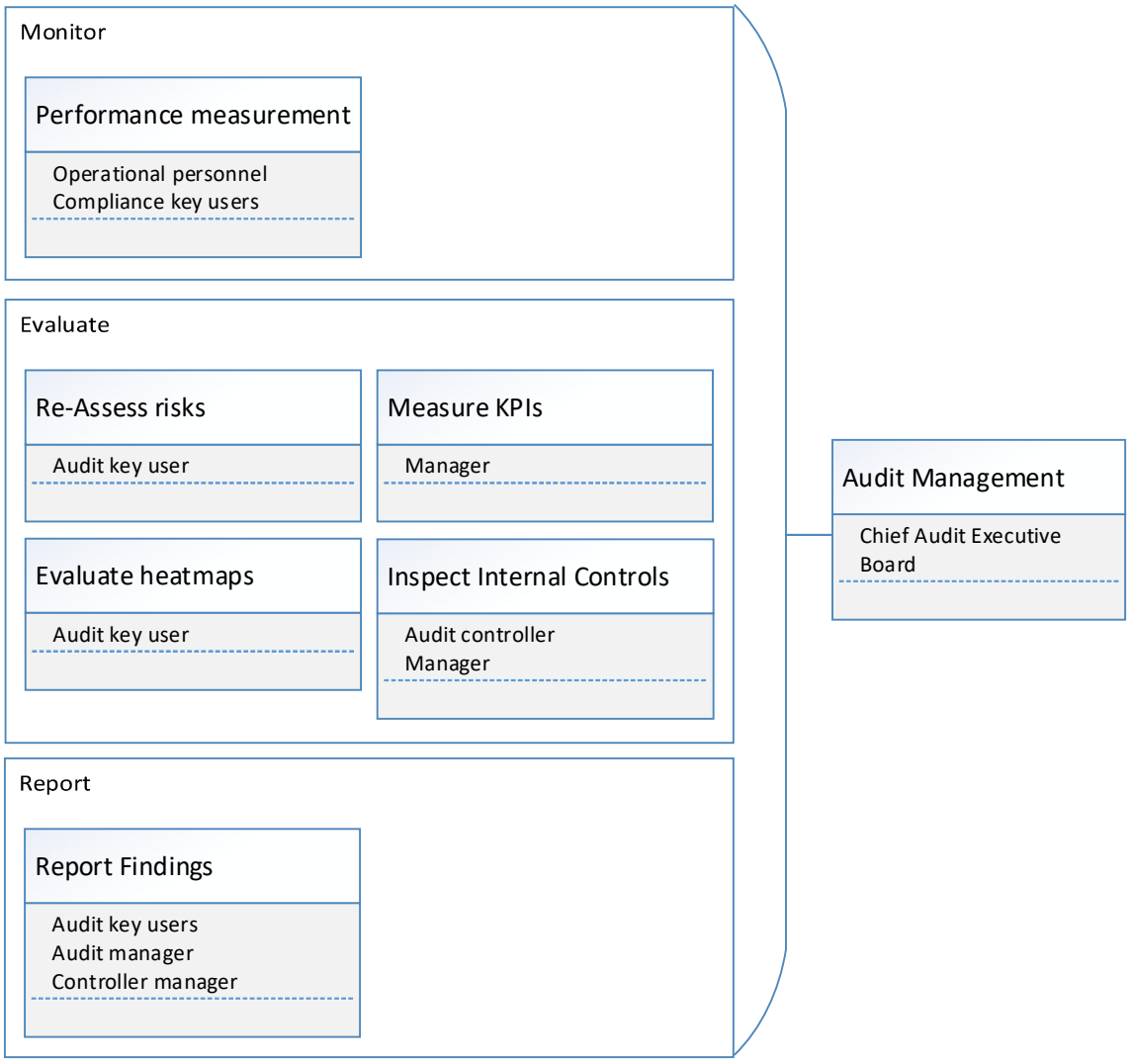

Figure 10. Audit Management processes and roles

Policy management

Policy management is more about directing the IT towards exploiting the strategy. To be more precise, the processes should go through a feedback loop and have presence in evaluation, reporting and monitoring also. Policy management and its proposed processes with roles is presented on Figure 11.

Policy management processes are:

- Direct
  - **Strategic alignment/define strategy** – „(Business-IT-Alignment) – focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations“ [Krey, 2010].
  - **Deficiency management** – „Results from deviation analysis are taken as requirements for deficiency management. Deficiencies are eliminated through improving, creating new controls or modifying parts of the control system“ [Racz, 2011b].
  - **Manage policies** – from the definition of management system, „set of interrelated or interacting elements of an organization to establish policies ...“ where policy is „intentions and direction of an organization as formally expressed by its top management“ [ISO19600:2014].
  - **Support policy life-cycle** – measures to help establishing managing policy life-cycle phases.
  - **Controls & policy mapping** – each policy should have controls to execute it. These need to be mapped for ensure consistency and ensuring that policies are followed.
  - **Manage procedures** – **procedure** – „specified way to carry out an activity or process“ [ISO19600:2009].
  - **Define risk appetite** – **risk attitude** – „organization’s approach to assess and eventually pursue, retain, take or turn away from risk“ [ISO 31000:2009].
- Evaluate
  - **Requirements analysis** – „Requirements analysis comprises the identification od regulatory, legal, contractual, and other obligations that affect the organization’s IT operations.“ [Racz, 2011b].
  - **Deviation analysis** – „after requirements analysis, adherence is examined with internal and external audits“ [Racz, 2011b].
- Report
  - **Reporting/documentation** – „All actions are documented and relevant information is reported to stakeholders“ [Racz, 2011b].
  - **IT compliance reporting** – „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 its continuing adequacy, including all relevant noncompliances..“ [ISO 19600:2014].
- Monitor
  - **IT control self-assessment and measurement** – „Control self-assessment is a methodology used to review key business objectives, risks involved in achieving the objectives, and internal controls designed to manage those risks“ [Institute of Internal Auditors. 1998. A Perspective on Control Self-Assessment. The Institute of Internal Auditing, Florida.].

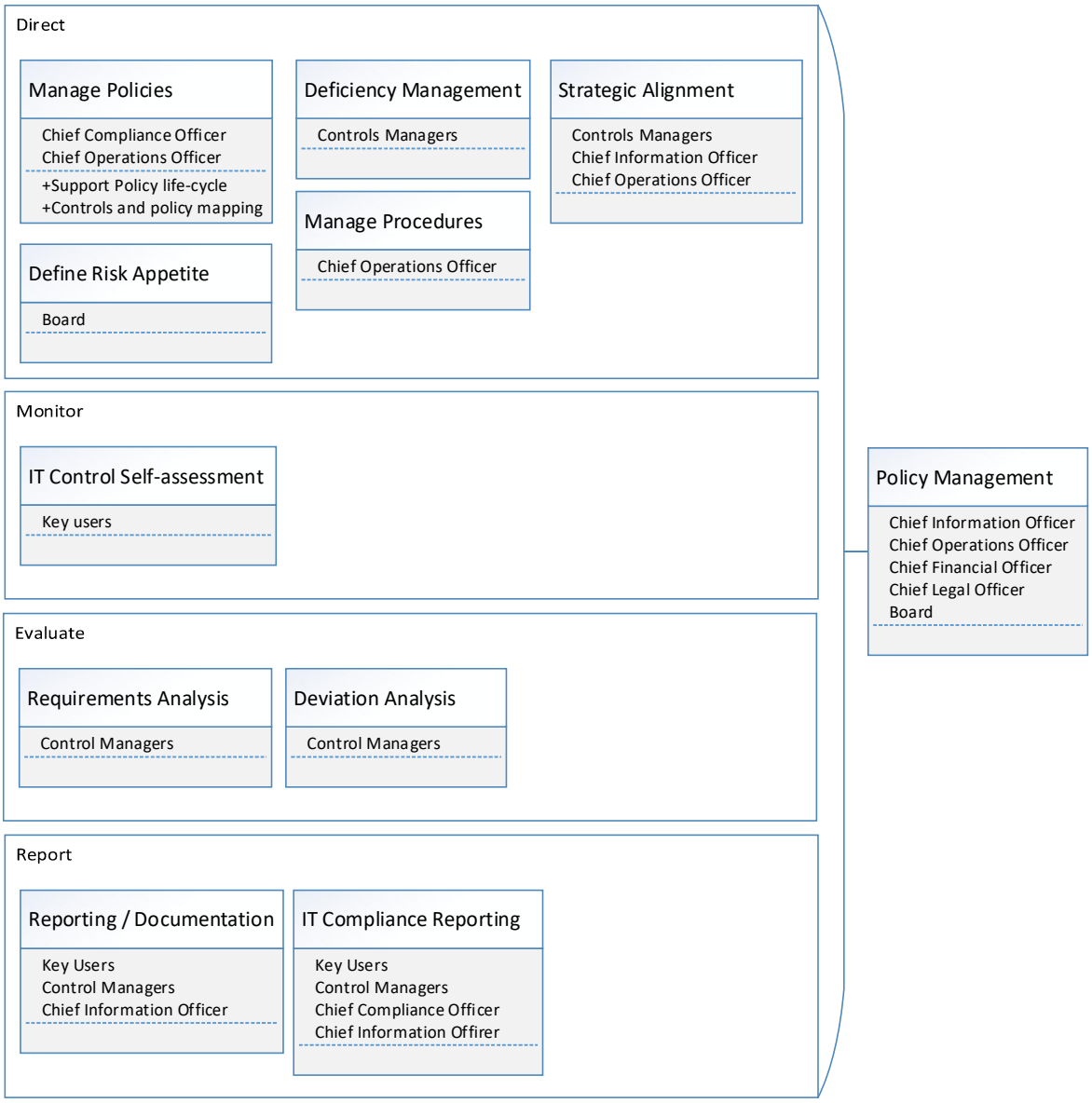

Figure 11. Policy management processes and roles

Issue management

The less captured functionality is issue management (case, issue, event, remediation, loss). Altough there have been captured some processes, the roles have not been assigned. The main question for us would be whether issues management could be a part of risk management or should it remain separately? Issue management processes model proposal is presented on Figure 12.

Issue management processes are:

- Direct
  - **Manage issues** – dealing with cases/issues/events which have not been declared as a risk/involving a risk.
  - **Update risks** – issue that turned out to be risk has to be described for risk management to be able to deal with (identify, mitigate, etc) this in the future.

- **Update internal controls** – internal controls as a main driving force in a system, need to be up to date and relevant.
- **Value delivery** – „is about executing the value proposition throughout the delivery cycle, concentrating on optimizing costs and providing the intrinsic value of IT" [Krey, 2010].
-

- Evaluate
  - **Value delivery** – „ensuring that IT delivers the promised benefits against the strategy" [Krey, 2010].
- Report
  - **Produce Prioritized Matrix/Heatmaps** – reporting the situation of the system/department etc using heatmaps.

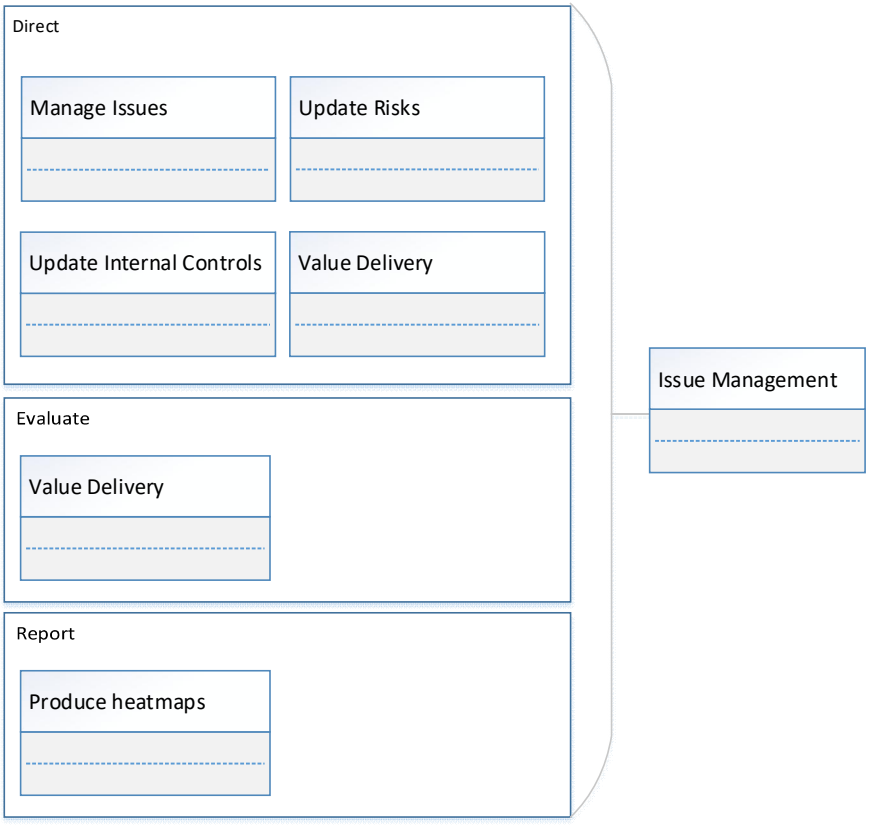

Figure 12. Issue Management processes

Risk management

For risk management (risk management, enterprise risk management) we assume that before directional processes, we need to do some monitoring and evaluation so the order of processes follows this idea. Following is the unordered list of definitions in risk management functionality, grouped by directing, evaluating, reporting and monitoring. Risk management processes model proposal is presented on Figure 13.

Risk management processes are:

- Direct

    - **Resource management** – "is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure" [Krey, 2010].
    - **Risk response** – **risk treatment** – „process to modify risk" [ISO 31000:2009].
    - **Control activities** – **control** – „measure that is modifying the risk" [ISO 31000:2009].
    - **Manage risks** – „systematic application of management policies, proceduresand practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk" [ISO 31000:2009].
    - **Develop KRI** – **establish the context** – „defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy" [ISO 31000:2009].
    - **Remediation & control management** – **Remediation risk management (RRM)** – „is the process for managing uncontrollable project activities or circumstances that may result in negative consequences to remediation system performance" [Interstate Technology & Regulatory Council (ITRC)].
    - **Objective setting** – „Derivation of IT compliance and IT compliance reporting objectives from business requirements" [Racz, 2011b].
    - **Align with key-objectives** – Process of aligning RM with organisational objectives.
- Evaluate
    - **Internal environment** – **internal context** – „internal environment in which the organization seeks to achieve its objectives" [ISO 31000:2009].
    - **Event identification** – **risk identification** – „process of finding, recognizing and describing risks" [ISO 31000:2009].
    - **(IT) Risk assessment** – „overall process of risk identification, risk analysis and risk evaluation" [ISO 31000:2009].
    - **Identify risks in proccesses using inquiries/surveys** – part of **risk identification** – „process of finding, recognizing and describing risks" [ISO 31000:2009].
    - **Determine risk appetite** – **risk attitude** – „organization's approach to assess and eventually pursue, retain, take or turn away from risk" [ISO 31000:2009].
- Report
    - **Information & communication** – **communication and consultation** – „continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk" [ISO 31000:2009].
- Monitor
    - **Monitoring** – „continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected" [ISO 31000:2009].

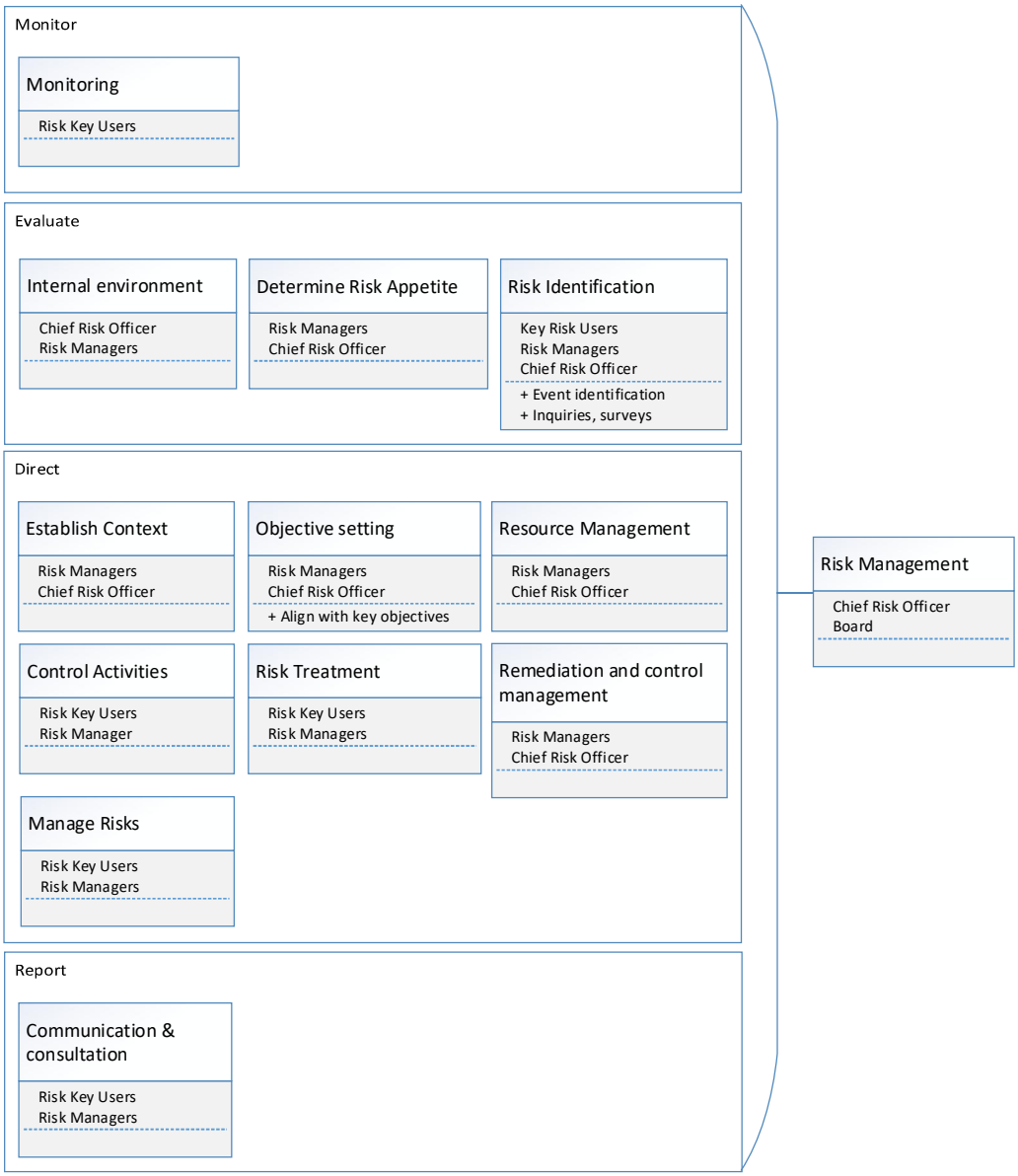

Figure 13. Risk Management processes and roles

3.4 Summary

This chapter's goal, an IT GRC framework proposal was presented on Figures 8-13. Questionable for us was that some processes were mapped with a hesitation such as "manage risks" and the lack of processes in issue management functionality. Those doubts need some further validation which shall be done in proceeding chapters.

4 Framework based application

To better visualise the IT GRC framework and help to assess companies' maturity regarding IT GRC, a web application [4]was developed. The same components presented in previous chapter are presented interactively. This chapter is intended to answer the question SRQ3: "*How IT GRC assessment could be supported?*". The chapter is divided into two parts, firstly the web application is introduced, secondly explanation how to assess a company's IT GRC maturity by using this application.

4.1 Main screen

The main screen of the web application (Figure 14) has the GRC-triangle in top of the screen. Clickable, ordered process flow lists, pointed by the yellow arrows, are around the triangle in bold. Users can explore processes in the framework by clicking on these process flow elements. Grey feedback panel in the bottom of the screen is for maturity assessment.

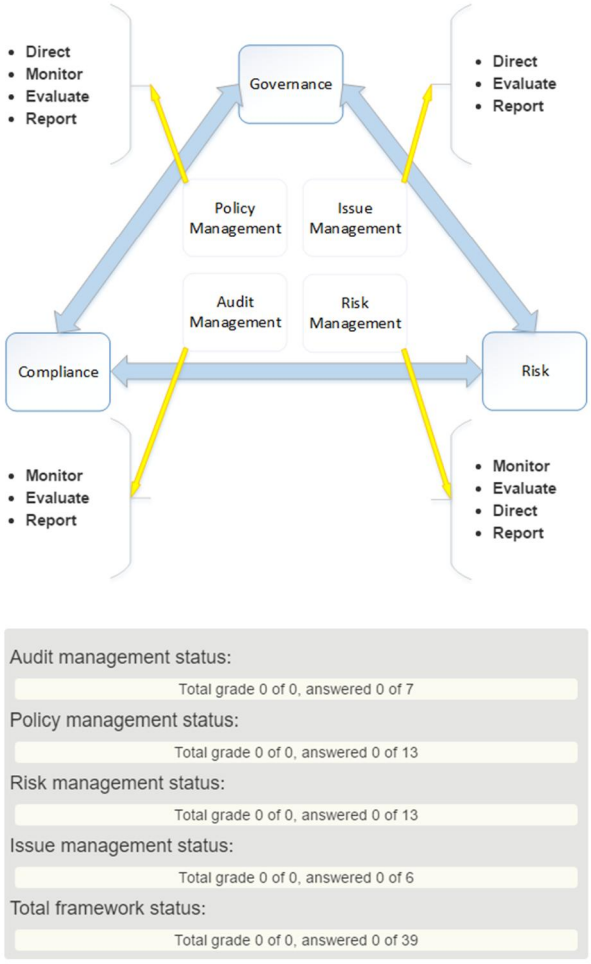

Figure 14. IT GRC web application main view

After clicking on a process flow title, the functionality rectangle and the arrow pointing to the process flow will turn grey and a grey panel either on the left or on the right (depending on which side process flow was clicked) appears. The appearing panel displays the underlying processes involved in this (clicked) process flow. The processes are displayed

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

using the same class diagram-like notation, including roles that are possibly involved with them, subprocesses and if hovering the cursor over the process-box definitions for the processes are shown in a tooltip (Figure 15).

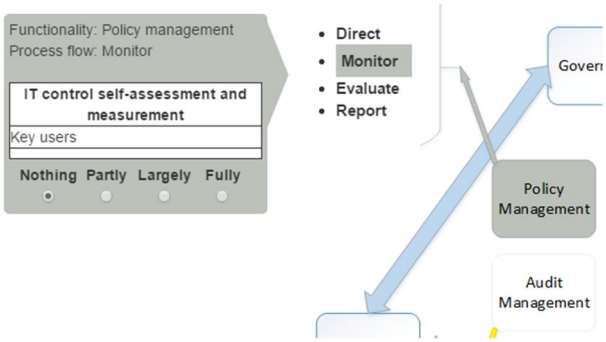

Figure 15. Policy management's process flow „monitor"

4.2 Maturity assessment

While exploring the framework's processes, one can see under each process box, there are four radio buttons with labels „Nothing", „Partly", „Largely" and „Fully". For example, in Figure 15, *policy management*, *monitor* process flow was clicked and a grey panel on the left opened, showing „*IT control self-assessment and measurement*" process. These can be used to assess a company's maturity regarding IT GRC. The meaning of those buttons should present the status of this process alignment in the company. For example, in the Figure 15, one can form a sentence: „Our company has ***nothing*** aligned in *policy management, monitoring* process flow's process *IT-control self-assessment aligned with the presented framework*".

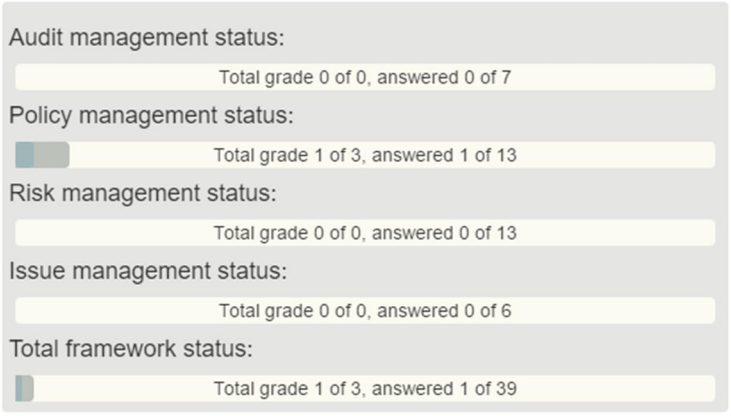

Figure 16. Feedback panel, one process under policy management graded with „partly"

During assessment of the individual processes, the feedback panel in the bottom of the screen is updated according to the maturity grades entered (Figure 16). Information is shown on two levels – *amount of processes assessed* (policy management status, answered 1 of 13 or grey indicator in Figure 16), and *maturity regarding assessed processes* (policy management status, grade 1 of 3 or green indicator in Figure 16). First of which indicates how many processes are assessed from total and second allows to have overview of the status for the assessed processes without needing to go over assessing all of them in case

one does not need all of the processes implemented. Grades are calculated based radio input values, where „Nothing“ has value 0, „Partly“ has value 1, „Largely“ has value 2 and „Fully“ has value 3. The goal is to have as many proccesses as fully in aligned as possible.

4.3 Summary

In this chapter, a web application to support assessment of IT GRC maturity in a company was created. Next chapters are about presenting the resulting IT GRC framework to domain specialists and thus validating the framework.

5 Comparison of the frameworks

The goal of this chapter is to compare our proposed IT GRC framework against IT GRC ISO standards compliant framework [Mayer, 2011]. This chapter answers to question SRQ4: "*What are similarities and differences of our IT GRC framework to the Mayer et al ISO standards model?*". The chapter begins with describing Mayer's results, the methodology, how the comparison is done, then comparison results are presented and the improvement ideas for our framework are addressed.

Mayer constructed an ISO-compliant IT GRC integ.rated model from the ISO standards related to the GRC individual domains by combining the common activities in them. As there were no dedicated ISO standards, they based their study on reference documents as following – for risk, they based their study on ISO 31000:2009 „Risk management – Principles and guidelines", for compliance, they based their study on ISO 19600:2014 „Compliance management systems – Guidelines." and for governance, they based their study on ISO/IEC 38500:2015 „Governance of IT for the organization".

The first step for them was to identify common activities in risk and compliance management processes as seen on the Figure 17, marked with orange. Secondly, they extracted the common elements involving the governance component on which their integration strategy was based on. Mayer's governance tasks are presented in Table 1. Their objective was to identify only the integrating activities rahter than exhaustively describe all processes.

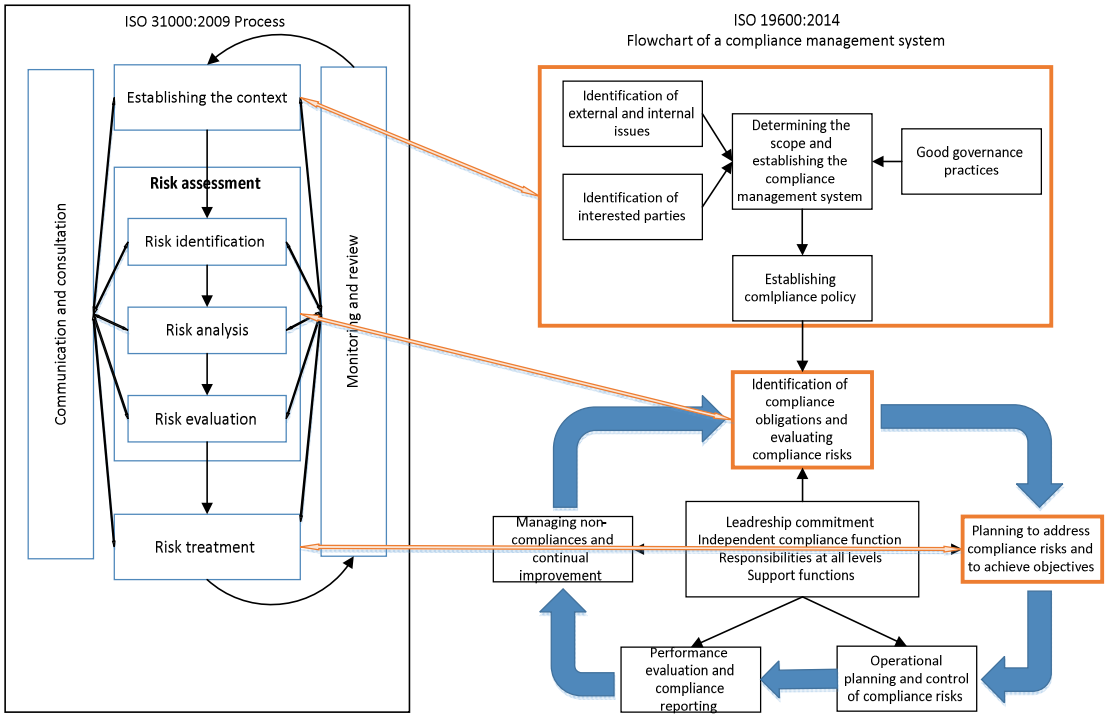

Figure 17. Common activities between risk management and compliance management [Mayer, 2011]

Table 1. Compliance and risk activities in governing body [Mayer, 2011]

	Direct	Evaluate	Monitor
Compliance	Demonstrate leadership and commitment with respect to the compliance management system	Review and approve strategy based on regulatory demands	Review the reporting on the compliance management system performance
	Establish and endorse a compliance policy		Supervise the compliance management system
	Define roles and responsibilities		Escalation, where appropriate
	Active involvement in the compliance management system		
	Commit to the development of a compliance culture		
Risk management	Define the risk appetite relating to the use of IT and specific control requirements	Review and approve strategy based on risks	Ensure that there is an adequate audit coverage of IT related risk management
		Approve key risk management practices such as those relating to security and business continuity	
		Evaluate what is an acceptable risk to the organization	

5.1 Methodology

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 are 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. The comparison table is presented in table a13 and explained below in this chapter.

5.2 Correspondence

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.

5.2.1 Corresponding elements

1) *Defining risk appetite (attitude)* is complete match in both models. – **Complete match.**
2) *Strategic alignment / definition of strategy* from our model is containing processes from Mayer et al model such as *evaluation of strategy based risks* and *evaluation of strategy based on regulatory demands.* – **Partial match.**
3) In the context of IT GRC, we align (compliance) *objective setting* from our model with *establishment of a compliance policy* from Mayer et al model. – **Partial match.**
4) *Compliance reporting* process in our model is by its definition suitable to be aligned with *reviewing the reporting on the CMS performance* from Mayer et al model, since the context of the processes is to ensure effective compliance reporting. – **Complete match.**
5) *Producing* and *evaluating heatmaps* from our model are part of the *supervision of the CMS* from Mayer et al model. – **Partial match.**
6) *Managing policies*, *monitoring*, *evaluation of internal/external context*, *supporting policy life-cycle* and *controls & policy mapping* are part of *monitor, review strategies and associated policies* from Mayer et al model. – **Partial match.**
7) *Evaluation of requirements* and *aligning with key objectives* from our model is part of *evaluation of acceptable risk for the organization* from Mayer et al model. – **Partial match.**
8) *Inspecting internal controls* from our model is overlapping with *monitoring adequate audit coverage for IT RM* from Mayer et al model. – **Partial match.**

5.2.2 Mayer et al has, our model does not have

Processes in Mayer et al model which **our model did not have** (blue background in the table a13) are:

1) *active involvement in compliance management system,*
2) *escalation where appropriate,*
3) *application of governance to the management system,*
4) *commitment to developing of a compliance culture,*
5) *definition of roles and responsibilities,*
6) *evaluation of key risk management practices,*
7) *demonstration of leadersip and commitment with respect to compliance management system.*

5.2.3 Our model has, Mayer et al does not have

Processes **in our model which we did not find equivalence** (red background in table a13) in Mayer et al model are:

1) *Resource management,*
2) *direct & evaluate value delivery,*

3) *manage procedures,*
4) *performance measurement,*
5) *deviation analysis,*
6) *deficiency management,*
7) *remediation & control management,*
8) *IT risk assessment,*
9) *manage issues,*
10) *develop key risk indicators,*
11) *event/risk identification,*
12) *identification of risks in processes using surveys,*
13) *IT control self-assessment and measurement,*
14) *managing risks,*
15) *risk response,*
16) *control activities,*
17) *updating risks,*
18) *updating internal controls,*
19) *reporting documentation.*

5.2.4 How our framework should be updated?

We improve our model by adding the processes from Mayer et al model as following:

Under **policy management's** process flow **direct**, we:

a) combine the actions, such as *active involvement in compliance management system*, *application of governance to the management system* and *demonstration of leadersip and commitment with respect to compliance management system* as a description for ***Establish compliance management system*** process.
b) add separate processes: c*ommitment to developing of a compliance culture*, and *definition of roles and responsibilities.*

Under **audit management's** process flow **report**, we:

a) add process *escalation where appropriate*.

Under **risk management's** process flow **evaluate**, we:

a) add process *evaluation of key risk management practices*.

5.3 Summary

As there are different number of corresponding elements in our model – 14 to Mayer et al model – 9, Mayer had more compliance related elements, our 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 assumption could be that as Mayer's study based the framework on reference documents, not 1:1 ISO standards for the domains of IT risk management and IT compliance, the processes for their model are more general and thereby have less details.

6 Completeness of the framework

The goal of this chapter is to evaluate the completeness of proposed IT GRC framework and the question SRQ5 is "*What is completeness of IT GRC framework?*". The chapter begins by describing the instruments, used to evaluate completeness and evaluation process. Then results and implications are presented, afterwards, threats to validity and future validation activities are discussed.

6.1 Instruments

In addition to help visualise and assess companies IT GRC maturity, the **IT GRC framework web application**[5] can be used to assess the proposed framework's completeness. To better understand the framework without reading the paper at hand, **a screencast**[6] was prepared. This briefly explains the structure and functionalities of the IT GRC framework and the web application. To collect as much feedback as possible, a web form[7] was created. This was designed to be as comfortable as possible, as there were many questions, which might scare respondents from answering at all. The feedback form consists of 4 pages split by main functionalities, grouped by process flows which could be commented and processes in the flows which could be assessed in the scale of "definitely include" as 1, "maybe include" as 2, "maybe exclude" as 3 and "definitely exclude" as 4.

6.2 Process

The process of assessing the completeness of the IT GRC framework depends on the feedback by a specially selected focus group. The focus group was formed from the authors of the papers from the references of 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, all the relevant studies which were excluded by some reasons, those authors were also included to the focus group.

The focus group was sent an invitation letter with aforementioned links and explanations to the framework web application and screencast video to collect the feedback. The letter was sent initially to 11 persons, then reminder letter after 7 days. As a result, one of 11 respondents had filled the survey. After such low response rate, studies which were excluded from the review in later stages after which, the focus group was 25 persons. Finally, 4 out of 25 persons answered the questionnaire.

6.3 Results

The results of IT GRC framework completeness assessment were captured as following – a comment per each process flow and a grade per process, where grades were from 1 to 4 (from definitely include to definitely exclude). The response in total was 13 comments and 151 grades. To conclude the results, we average the grades and try to answer the comments, conclusion of results is presented in table 2. The raw data is presented in tables a14 - comments and a15 - grades.

[5] http://mihkel.joulukiri.ee
[6] https://www.youtube.com/watch?v=uKHUKxTICxI
[7] http://mihkel.joulukiri.ee/evaluate/renderform

Table 2. Results of IT GRC framework completeness survey

Definitely include	**Maybe include**	**Maybe exclude**	**Definitely exclude**	**Suggested by respondents**
21 processes	17 processes	1 processes	0	8 processes
Inspect internal controls Report findings Strategic alignment Manage policies Manage procedures Define risk appetite Deviation analysis IT compliance reporting Risk response - Risk treatment Control activities *Manage risks* Develop KRI - establish the context Remediation & control management Internal environment - internal context Risk identification Determine risk appetite – risk attitude	Performance measurement Re-assess risks Evaluate heatmaps Measure KPIs Deficiency management Requirements analysis Reporting /documentation IT control self-assessment and measurement Manage issues Update risks Update internal controls Value delivery Value delivery Produce prioritized matrix/heatmaps Resource management Objective setting Commitment to developing of a compliance culture	Escalation where appropriate		Manage risks could be main functionality risk management's description instead of process. Add under risk management's evaluate: • control activities, • risk response/risk treatment. • external environment - external context Copy under audit management monitoring: • IT control self-assessment and measurement Add under policy management evaluate: • translation of external regulations into operational compliance measures. Move under audit management evaluate • deviation analysis (from policy management)

Information & communication Monitoring Establish compliance management system Definition of roles and responsibilities Evaluation of key risk management practices				• Translation of laws and regulations into operational compliance measures

6.3.1 Risk management

Risk management got the most grades as 1 – definitely include, also suggestions to include elements from other functionalities to risk component.

Direct process flow – *resource management* and *objective setting* processes got average grade of 1.75 which we consider "maybe include". *Remediation & control management* process got average grade of 1.25 which we translate as "definitely include", the same goes with all other processes in this flow, that got average grade of 1. This process flow did not receive any comments under it, but its process, *manage risks* got a question under report process flow – this process could be taken out as it encapsulates all the processes under the main functionality *risk management*.

Evaluate process flow – all processes got average between 1 to 1.25 which we translate to "definitely include". Comment suggests adding "external environment" and some of the processes from the "direct" process flow. This is agreeable, since the mapping of the processes into the process flows was done by finding the best suitable process flow to each process and second round might be needed.

Report process flow has only one process of *information & communication* it got average grade of 1.25, meaning "definitely include".

Monitor process flow – it has only one non-split process called *monitoring*, which got average grade of 1 – "definitely include". Also the comment indicates that there could be more details. What concerns to all details proposed in the comment, they did not fit the scope of this study, but might be separate goal in some future research.

6.3.2 Policy management

Policy management seems to have many things in common with audit management, thereby some details might have been mixed up between those functionalities.

Direct process flow – all processes under this flow got the average of 1 or 1.25 (definitely include), except for *deficiency management* and *Commitment to developing of a compliance culture* which got 1.75 and 1.67 accordingly (maybe include). From comments, a question regarding *deficiency management*, whether it is issue management is raised. Answer to it –

might be, as issue management is open for discussion, whether it is needed to exist as a separate functionality or included into others. Second question regarding relationship between G, R and C, firstly second round of mapping would help identify which processes are partial – left out from some process flows.

Monitor process flow – only process for this flow was *IT control self-assessment and measurement* which got the average grade of 1.5 – maybe include. The comments revealed again the need for second round of mapping, since the process might be part both, policy and audit management.

Evaluate process flow – there are two processes, *deviation analysis*, which got average of 1.5 – maybe include and *requirements analysis,* which got 1.3 – definitely include. From comments, there is one proposal for new process: "translation of external regulations into operational compliance measures" and mentioning the audit management, which could have the deviation analysis process but not certain whether instead or as well.

Report process flow – two processes under this flow are *reporting/documentation* which got average of 1.5 – maybe include and *IT compliance reporting,* which got 1.25 – definitely include. Comment seems to indicate that putting together *reporting/documentation* might have been a wrong step.

6.3.3 Audit management

Monitor process flow – one and only process performance measurement got the average of 1.5 – maybe include.

Report process flow – one of processes, *report findings* got average of 1.25 – maybe include and *escalation where appropriate* got 2.67 – maybe exclude, also from comments, first comment could be agreed with – *escalation, where appropriate* could be merged into/mapped to *report findings* as escalation is a form of reporting. Second comment, seems slightly out of scope of this research, but if taken in scope, there was too little input from the literature review results to decide this – maybe additional future research activity option.

Evaluate – two out of four processes *re-assess risks* and *measure KPIs* got grade 1.5 and *evaluate heatmaps* got 2 – both cases maybe include. Last process, inspect internal controls got 1 – definitely include. Comments reveal proposal for a new process – "*connection of risks and compliance requirements translation of laws and regulations into operational compliance measures*".

6.3.4 Issue management

The author of this paper hesitates, whether issue management should be a part of this model. Same kind of indications could be found from the feedback as well.

Direct process flow – all processes are near average of 2 – maybe include. Comment raise question regarding difference between issues and risks which has been questionable from the

Evaluate process flow – one and only process *value delivery* got average of 2 – maybe include. Comments also reveal that there is no clear certainty, whether issue management should be here.

Report process flow – one and only process *produce prioritized matrix* got the average of 2 – maybe include.

6.4 Threats to validity

Since some comments showed, that the introduction for the framework completeness assessment step was not thorough enough (respondents did not seem to know the scope), there might be more details missing in this communication and thereby some aspects might have left unnoticed. Secondly, as there were not many responses, there might not be enough opinions.

6.5 Future validation activities

After the model is retouched, taking into account the first round of feedback, more feedback from domain specialists might be needed. After that, comparison in real life could be conducted by validating the details of the model with industry best practices.

6.6 Summary

In general, the grades for completeness showed, that the processes captured in this paper shall be part of the framework (definitely include and maybe include). There were some comments regarding shortcomings of current setup and improvement ideas, some of which we agreed to apply.

7 Final remarks

In this paper, there are quite many gaps in the definitions of the processes and the process flows themselves in GRC main functionalities. This might refer to either still having not enough primary studies done about the domain or the review itself restrained us to reach such a little amount of applicable results.

The framework we constructed tries to give some guidelines about aligning IT GRC in an enterprise, though the issue needs more thorough research and practical experimenting.

7.1 Limitations

First of all, the author of this paper feels that more competence regarding all domains would be needed to have the study more thorough. For example, some processes which were mapped or not mapped during constructing the model and comparison between models, would be mapped differently now after the results are fixed.

The framework was intended to have 4 components – processes, roles, technology and strategy, but it has mostly processes which makes it quite loose to interpret. Secondly, some processes might have lost context or some important details as the focus was poor as research stretched longer as planned.

7.2 Answers to RQ

We started our research with a question **SRQ1**: "*What is the state of the art of IT GRC?*". To answer this, a systematic literature review was conducted, gathering its results for proceeding work.

Then, our driving question **SRQ2** was: "How IT GRC state of the art could be combined into the IT GRC framework?", which led us to proposing an IT GRC framework.

For question **SRQ3**: "*How IT GRC assessment could be supported?*", a web application was created to present the proposed framework. The web application is at the same time an instrument to assess the maturity regarding IT GRC.

To start validation of our proposed IT GRC framework, we tried to find answer to **SRQ4**: "*What are similarities and differences of our IT GRC framework to the Mayer et al ISO standards model?*".

SRQ5: "*What is completeness of IT GRC framework?*" - All in all, the framework has some processes in place, some to modify and add. Additionally, it would need more 'who', 'what' and 'how'.

Finally, this research intended to answer the question **RQ**: "How IT governance, IT risk management and IT compliance could be integrated?", for which, we proposed this IT GRC framework.

7.3 Conclusion

The proposed framework and its supporting web application is intended to assist companies to integrate their IT GRC processes. Regarding feedback from the completeness assessment, there is some details missing to complete the integrated model. Application of the framework in real life could help assessing maturity of IT GRC according to the the framework. Completeness of the framework could be said to be partial – which can be both

positive and negative at the same time. On the positive side, it is more flexible to different industries needs, but the loose architecture might cause important details to be missed.

7.4 Future work

Firstly, current research completeness assessment feedback shall be included to the framework. Also, as it came out from completeness assessment, the framework could be overlooked regarding mapping of the processes. Next step could be to include domain (G, R or C) specialists to oversee the details and answer the questions of “who?”, “what?” and “how?”.

8 References

1. Mayer, N., Barafort, B., Picard, M., Cortina, S. (2015). An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance). In Systems, Software and Services Process Improvement Volume 543 of the series Communications in Computer and Information Science (pp. 87-99). Springer International Publishing.
2. Kitchenham B., Guidelines for performing Systematic Literature Reviews in Software Engineering, EBSE Technical report, Keele University 2007.
3. Racz, N., Weippl, E., Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In Communications and Multimedia Security (pp. 106-117). Springer Berlin Heidelberg.
4. Racz, N., Weippl, E., Seufert, A. (2011a). Governance, Risk & Compliance (GRC) Software - An Exploratory Study of Software Vendor and Market Research Perspectives. In proceedings of the 2011 44th Hawaii International Conference on System Sciences (pp. 1-10). IEEE Kauai, HI.
5. Racz, N., Weippl, E., Seufert, A. (2011b). Integrating IT Governance, Risk, and Compliance Management Processes. In proceedings of the 2011 conference on Databases and Information Systems VI (pp. 325-338). IOS Press Amsterdam, The Netherlands, The Netherlands.
6. Krey, M. (2010). Information Technology Governance, Risk and Compliance in Health Care - A Management Approach. In proceedings of the 2010 Developments in E-systems Engineering (pp. 7-11). IEEE Computer Society Washington, DC, USA.
7. Vicente, P., Silva, M. M. (2011a). A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In proceedings of the 2011 IEEE World Congress on Services (pp. 422-428). IEEE Computer Society Washington, DC, USA.
8. Vicente, P., Silva, M. M. (2011b). A Conceptual Model for Integrated Governance, Risk and Compliance. In Advanced Information Systems Engineering (pp. 199–213). Springer Berlin Heidelberg .
9. Shahim, A., Batenburg, R. and Vermunt, G. (2012). Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies. In ICT Critical Infrastructures and Society Volume 386 of the series IFIP Advances in Information and Communication Technology (pp. 202-212). Springer Berlin Heidelberg.
10. Puspasari, D., Kasfu Hammi, M., Sattar, M., Nusa, R. (2011). Designing a tool for IT Governance Risk Compliance: A case study. In International Conference on Advanced Computer Science and Information System (ICACSIS). (pp. 311-316). IEEE, Jakarta.
11. Institute of Internal Auditors. 1998. A Perspective on Control Self-Assessment. The Institute of Internal Auditing, Florida.
12. ISO/IEC 38500:2015: Information technology – Governance of IT for the organization. International Organization for Standardization, Geneva (2015).
13. ISO 31000:2009: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2009).
14. ISO 19600:2014: Compliance management systems – Guidelines. International Organization for Standardization, Geneva (2014).
15. Interstate Technology & Regulatory Council (ITRC). Retrieved 10.05.2016, from http://www.itrcweb.org/Team/Public?teamID=43

Appendix

I. Review protocol

Table a1. Systematic review protocol

<table>
<tr><td rowspan="5">Research questions</td><td rowspan="1">Main RQ</td><td colspan="2">How IT governance, IT risk management and IT compliance could be integrated?</td></tr>
<tr><td rowspan="4">Sub-questions</td><td colspan="2">Which processes have been defined for IT GRC?</td></tr>
<tr><td colspan="2">What roles of people are involved for IT GRC?</td></tr>
<tr><td colspan="2">What strategy is used for IT GRC?</td></tr>
<tr><td colspan="2">What is considered as technology for IT GRC?</td></tr>
<tr><td>Search terms</td><td colspan="3">ACM Library:
1) acmdlTitle:((grc OR (governance AND risk AND compliance)) AND (it "information technology"))
2) recordAbstract:((grc OR (governance AND risk AND compliance)) AND (it "information technology"))
IEEExplore:
1) ((governance AND risk AND compliance AND "information technology" AND NOT granular) OR (governance AND risk AND compliance AND IT AND NOT granular) OR (GRC AND IT AND NOT granular) OR (GRC AND "information technology" AND NOT granular))
SpringerLink:
1) ((governance AND risk AND compliance) OR GRC) AND (IT OR "information technology")</td></tr>
<tr><td>Resources to be searched</td><td colspan="3">ACM Digital Library, IEEExplore, SpringerLink</td></tr>
<tr><td rowspan="5">Selection strategy, procedures, criteria</td><td>1.1.</td><td colspan="2">Include if type is journal or proceeding.</td></tr>
<tr><td>1.2.</td><td colspan="2">Exclude if type is magazine paper, doctoral dissertation, preface for conference/workshop, book, poster.</td></tr>
<tr><td>2.1.</td><td colspan="2">Include if title includes GRC, OR governance AND risk management AND compliance.</td></tr>
<tr><td>2.2.</td><td colspan="2">Exclude if title includes granular computing or network.</td></tr>
<tr><td>3.1.</td><td colspan="2">Include if abstract includes governance, risk AND compliance.</td></tr>
</table>

	3.2.	Exclude if abstract has wrong acronym of GRC or the abstract indicates the paper is not about GRC integration.	
Quality assessment	Method/approach/framework presentation		
		Quality criteria	**Points**
	1.1.	Problem statement presented	0.5
	1.2.	Research question(s) presented	0.5
	2.	Research method presented	1
	3.	Theoretical grounding	1
	4.	Illustrative example, case study	1
	5.	Discussion/analysis	1
	6.	Related work	1
	7.1.	Conclusion	0.5
	7.2.	RQ are answered	0.5
	8.	Limitations / advantages	1
	Empirical study (survey, case study, experiment)		
		Quality criteria	**Points**
	1.1.	Problem statement presented	0.5
	1.2.	Research question(s) presented	0.5
	2.	Research method presented	1
	3.	Discussion / analysis	1
	4.	Related work	1
	5.1.	Conclusion	0.5
	5.2.	RQ are answered	0.5
	6.1.	Results presented	0.5
	6.2.	Result analysis presented	0.5
	7.	Threats to validity presented	1

Data extraction	Data extraction form presented in paragraph 2.3.
Data synthesis	Data synthesis described in paragraph 2.4.

II. Search Queries

Table a2. Search queries

Library	**Search queries**
ACM Digital library	1) acmdTitle:((grc OR (governance AND risk AND compliance)) AND (it "information technology")) 2) recordAbstract:((grc OR (governance AND risk AND compliance)) AND (it "information technology")) **Note:** Search The ACM Guide to Computing Literature was used.
IEEExplore	((governance AND risk AND compliance AND "information technology" AND NOT granular) OR (governance AND risk AND compliance AND IT AND NOT granular) OR (GRC AND IT AND NOT granular) OR (GRC AND "information technology" AND NOT granular))
SpringerLink	((governance AND risk AND compliance) OR GRC) AND (IT OR "information technology") **Note:** Additionally, “SWE” and “English” filters were used.

III. Study Selection Criteria

Table a3. Study selection criteria

1.1.	Include if type is journal, proceeding or chapter.
1.2.	Exclude if type is magazine paper, doctoral dissertation, preface for conference/workshop, book, poster.
1.3.	Exclude if study is already included earlier.
2.1.	Include if title includes GRC or GOVERNANCE and RISK and COMPLIANCE.
2.2.	Exclude if title includes GRANULAR COMPUTING or NETWORK.
3.1.	Include if abstract includes GRC or GOVERNANCE, and RISK and COMPLIANCE.
3.2.	Exclude if abstract includes contextually wrong acronym of GRC – paper is not about IT GRC.
4.1.	Exclude if further reading reveals the paper not to be about IT GRC or the study can not answer to data extraction form questions otherwise consult with other researchers (include if applicable).

IV. Quality checklist

Table a4. Study Quality checklists

Method/approach/framework presentation			**Empirical study (survey, case study, experiment)**		
#	Criterion	Pts	#	Criterion	Pts
1.1.	Problem statement presented	0.5	1.1.	Problem statement presented	0.5
1.2.	Research question(s) presented	0.5	1.2.	Research question(s) presented	0.5
2.	Research method presented	1	2.	Research method presented	1
3.	Theoretical grounding	1	3.	Discussion / analysis	1
4.	Illustrative example, case study	1	4.	Related work	1
5.	Discussion/analysis	1	5.1.	Conclusion	0.5
6.	Related work	1	5.2.	RQ are answered	0.5
7.1.	Conclusion	0.5	6.1.	Results presented	0.5
7.2.	RQ are answered	0.5	6.2.	Result analysis presented	0.5
8.	Limitations / advantages	1	7.	Threats to validity presented	1

V. Data Extraction Form

Table a5. Data extraction form

Data item	**Value**	**Note**
Statistic info		
Date of extraction		
Extractor		
Title		
Author(s)		
Short overview		
Quality score		
Contextual info		
Which processes have been defined for IT GRC?		
What roles of people are involved for IT GRC?		
What strategy is used for IT GRC?		
What is considered as technology for IT GRC?		

VI. Data extraction forms with data

Table a6. [Racz, 2011b]

Data item	Value	Note
Statistic info		
Date of extraction	30.01.2016, 07.03.2016	
Extractor	Mihkel	
Author(s)	Racz N, Weippl E, Seufert A.	
Title	Integrating IT Governance, Risk and Compliance Management Processes	
Quality score	5/8	1.1. Research problem statement 0.5 2. Research method presentation 1 3. Theoretical grounding 1 5. Discussion/analysis 1 6. Related work 1 7.1. Conclusion 0.5
Short overview	The study introduces a high-level model from individual domain components as an artefact for IT GRC research knowledge base. IT Governance process model is taken from *ISO/IEC 38500:2008 – Corporate governance of IT*; IT Risk process model is derived from *COSO ERM framework* and IT Compliance is covered by *process model suggested by Rath and Sponholz* book.	
Contextual info		
Which processes have been defined for IT GRC?	The proposed process model is vertically split into three separate GRC	Risk and compliance support governance and

	domains, where the processes and their flow has 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 & communication and Monitoring.* **IT Compliance** starts with *Requirements analysis, Deviation analysis, Deficiency management, Reporting/documentation and Deviation analysis*.	governance governs R and C processes.
What roles of people are involved for IT GRC?	Management	
What strategy is used for IT GRC?	Not mentioned	
What is considered as technology for IT GRC?	Not mentioned	

Table a7. [Racz, 2011a]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	20.01.2016, 31.01.2016	
Extractor	Raimundas, Mihkel	
Author(s)	Racz, N., Weippl, E., Seufert, A.	
Title	Governance, Risk & Compliance (GRC) Software – An Exploratory Study of	

	Software Vendor and Market Research Perspectives	
Short overview	The study presents a survey results received from GRC software vendors on their perceptions of IT GRC software tools. Since the survey was designed with open-ended questions, some inaccuracies might be introduced while interpreting the results.	
Quality score	7/7	
Contextual info		
Which processes have been defined for IT GRC?		
What roles of people are involved for IT GRC?		
What strategy is used for IT GRC?		
What is considered as technology for IT GRC?	Vendors have different perspectives on which functionality should be delivered by GRC software. Study extracted following functionalities: **Governance** Reporting/dashboards/analytics; Controls testing and management; Financial controls; Surveys; Workflow management; Corporate governance; **Risk** Risk management (RM, ERM); Case / issue / event / remediation / loss management; Operational risk management **Compliance** Policy management; Audit management;	Not specific technology or tools, but their functionalities studied.

	Compliance management; IT audits and compliance.	

Table a8. [Vicente, 2011a]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	23.01.2016, 05.04.2016	
Extractor	Mihkel	
Author(s)	Vicente, P., Silva, M. M.	
Title	Business Viewpoint for Integrated IT Governance, Risk and Compliance	
Short overview	The paper researches GRC state of the art and constructs a Business by following Racz et al. "A Frame of Reference for Research of Integrated GRC" and combining Racz et al. "A Process Model for Integrated IT GRC Management" and Vicente & Silva et al. "A Conceptual Model for Integrated GRC". They reach to a conclusion that there is a strong relation between IT GRC and enterprise GRC i.e., the described high level process can be used for both of the domains.	
Quality score	4.5/8	Research problem statement 0.5 Background 1 Research method presentation 1 Theoretical grounding 1 Discussion/analysis 1

Contextual info		
Which processes have been defined for IT GRC?	Study presents a business process viewpoint, composed by processes (in italic) and objects (named after each process) as following: **Governance** *Evaluation* of policies, risk appetite, culture, strategies, key objectives. *Directing* of Key Risk Indicators, Risk reports and Key Performance Indicators. *Reporting* Risk reports. *Monitoring* Key Risk Indicators, Key Performance Indicators **Risk** *Internal environment* Policies, Risk Appetite, Culture, Strategies. *Objective setting* Risk Appetite and Key Objectives. *Event identification* enquiries / Surveys, Issues, Risks. *Risk assessment* Risks and Key Risk Indicators. *Risk response* Key Risk Indicators, Risk Reports, Risks, Action Plans, Internal Controls. *Control activities* Risk reports, Internal Controls, Control Objectives. *Information & communication* Risk Reports, Dashboards.	

	Monitoring **Compliance** *Requirements analysis* Policies. *Deviation analysis* Inquiries / Surveys, Issues, Risks, Findings. *Deficiency management* Findings, Action Plans, Internal Controls. *Reporting / Documentation* Dashboards. *Monitoring*	
What roles of people are involved for IT GRC?	Authors chose not to represent the actors and roles within ArchiMate language and include them into a viewpoint. They brought out just some examples of actors, roles and categories without assigning them to the parts of the model: • Leadership and champions • Oversight personnel – Board of Directors • Strategic personnel – C-suite - 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 • Operational personnel – Key-users	

	– Governance, risk, audit, controls, legal and compliance managers.	
What strategy is used for IT GRC?	Not mentioned.	
What is considered as technology for IT GRC?	Not mentioned.	

Table a9. [Vicente, 2011b]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	28.02.2016, 23.03.2016	
Extractor	Mihkel	
Title	A Conceptual Model for Integrated Governance, Risk and Compliance	
Author(s)	Pedro Vicente, Miguel Mira da Silva	
Short overview	The paper presents developing individual conceptual models for governance, risk and compliance, integrating them into one model and evaluating it against OCEG Capability Model. The model is quite extensive and thereby we extract only the parts overlapping the most in the domains.	
Quality score	4/8	1.1.Research problem statement 0.5 2.Research method presentation 1 3.Theoretical grounding 1 7.1.Conclusion 0.5 8.Limitations/advantages 1
Contextual info		

Which processes have been defined for IT GRC?	Processes scattered in Figure 3.	The authors did not include monitoring, dashboards and reporting to remove complexity.
What roles of people are involved for IT GRC?		
What strategy is used for IT GRC?	No strategy defined	
What is considered as technology for IT GRC?	No technology defined	

Table a10. [Krey, 2010]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	20.01.2016	
Extractor	Raimundas	
Author(s)	Krey, M.	
Title	Information Technology Governance, Risk and Compliance in Health Care – A Management Approach	
Short overview	The paper presents a survey results from the health care sector in Switzerland.	
Quality score	4.5/7	Identified criteria: research problem statement; research question(s); research method description; discussion/analysis; result presentation; result analysis.
Contextual info		

Which processes have been defined for IT GRC?	Activities taken from CobiT framework, these are: **Governance** *Strategic alignment* (Business-IT-Alignment) – "focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations" [Krey, 2010]. *Value delivery* – "is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and providing the intrinsic value of IT" [Krey, 2010]. *Resource management* – "is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure." [Krey, 2010]. *Performance measurement* – "tracks and monitors 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	Activities defined but specific processes are not.

	beyond conventional accounting." [Krey, 2010]. **Risk** No specific activities defined. **Compliance** "Identification of good practices for dealing with laws and regulations." [Krey, 2010]. "Improving personnel awareness for regulatory requirements." [Krey, 2010]. "Increasing process performance and compliance with laws and regulations and improved corporate performance." [Krey, 2010]	
What roles of people are involved for IT GRC?	**Governance** IT Strategy board, management	Only mentioned in general, but not specific definitions of roles given.
What strategy is used for IT GRC?	Not mentioned	
What is considered as technology for IT GRC?	Not mentioned	

Table a11. [Puspasari, 2010]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	11.02.2016, 27.03.2016	
Extractor	Mihkel	
Title	Designing a Tool for IT Governance Risk Compliance: A Case Study	

Author(s)	Dewi Puspasari, M. Kasfu Hammi, Muhammad Sattar, and Rein Nusa	
Short overview	The paper analyses the process of creating a GRC tool for XYZ Bank in Indonesia.	
Quality score	3/7	Problem statement 0.5 Research method presentation 1 Discussion/analysis 1 Conclusion 0.5
Contextual info		
Which processes have been defined for IT GRC?	In addition to Racz proposed IT GRC process framework, more high level processes were presented: Governance <-> **Direct & execute** <-> Compliance Governance <-> **Measure & Refine** <-> Risk Risk <-> **Plan & scope** <-> Compliance	
What roles of people are involved for IT GRC?	**Governance** CEO/Board and line management **Risk** Business risk owners **Compliance** Business owners	
What strategy is used for IT GRC?		
What is considered as technology for IT GRC?		

Table a12. [Shahim, 2012]

Data item	**Value**	**Note**
Statistic info		
Date of extraction	28.02.2016, 23.03.2016	
Extractor	Mihkel	
Title	Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies	
Author(s)	Abbas Shahim, Ronald Batenburg, Geert Vermunt	
Short overview	The paper reports development of a **strategic alignment perspective for the GRC domain** which is to assess the GRC maturity and alignment paths for organizations.	
Quality score	5/8	1.1.Research problem statement 0.5 1.2.Research question 0.5 2.Research method presentation 1 3.Theoretical grounding 1 4.Illustrative example/case study 1 7.1.Conclusion 0.5 7.2.RQ answer 0.5
Contextual info		
Which processes have been defined for IT GRC?		
What roles of people are involved for IT GRC?		
What strategy is used for IT GRC?	"The vision of GRC from a strategic alignment perspective is plotted on the	

	four domains from the strategic alignment model, based on the two building blocks: strategic fit and functional integration. The strategic fit dimension represents the integration of the external and internal domain" [Shahim, 2012]. "The external domain, on a business level, addresses the arena in which corporate decisions are made concerning strategy and distinctive strategy attributes which distinguish the firm from competitors. The element 'Governance' is positioned in this domain because it is concerned with the GRC strategy in the organization. The internal domain, on a business level, pertains to the organizational structure and the critical business processes that are available in the organization. The elements of 'Risk', 'Control' and 'Compliance' are positioned in this domain because these elements relate to the structure of GRC and the processes involved with GRC, e.g. the risk control structure in the organization. The fit between the external and internal domain in the business domain is argued to be critical when maximizing economic performance. This relation can be reflected in the IT domain, resulting in a proposition that in the IT domain a similar separation between the external and internal domains can be	

	made and that a fit between these domains is critical for IT in an organization." [Shahim, 2012]. "Integrating the business and the IT domain is coined by Henderson and Venkatraman as functional integration. In the GRC perspective, the IT domain represents the GRC solution which forms a system of record for GRC in the organization." [Shahim, 2012]. "The strategic alignment model distinguishes two kinds of functional integration between the business and IT domain: strategic integration (i.e. attempts are made to align both business and IT strategy) and integration of organization and processes (i.e. operational integration concerned with aligning infrastructure and processes on both business and IT level). Following the strategic alignment model of Henderson and Venkatraman, four alignment paths can be applied to the GRC domain: 1. The "strategy execution" path, translated to a GRC perspective, is displayed as "A". This path indicates that GRC strategy and GRC infrastructure are constructed in the business domain. A GRC solution is selected which could form a fit between the GRC infrastructure on both business and IT domain.	

	2. The “technology transformation” path for GRC is displayed as “B”. In this perspective a GRC strategy is developed in a business domain and a GRC solution is selected which concurs with this strategy. The infrastructure from the GRC solution is embedded in the organization. 3. The “competitive potential” path, translated to a GRC perspective, is displayed as “C”. In this path the strategy from the GRC solution is the driver. The GRC strategy and infrastructure in the business domain are geared towards the strategy which is adopted in the GRC solution. 4. The “service level” path for GRC is displayed as “D”. In this case the vision of GRC adopted in the GRC solution is integrated in the GRC organizational infrastructure.” [Shahim, 2012].	
What is considered as technology for IT GRC?		

VII. Comparison table

Table a13. Comparison between models

	Mayer et al.		Our model	
	Activity/process	**Description**	**Activity/process**	**Description**
1	Define risk appetite	Defining risk appetite related to the use of IT and specific control requirements.	Define risk appetite/risk attitude	Organization's approach to assess and eventually pursue, retain, take or turn away from risk.
2	Evaluation of strategy based risks	The governing body should approve the organization's business strategy for IT taking into account the implications of the strategy for achieving business objectives and any associated risks that might arise.	Strategic alignment, define strategy	Business-IT-alignment, focusing on ensuring the linkage of business and IT. Defining maintaining and validating the IT value proposition. Aligning IT operations with enterprise operations.
3	Evaluation of strategy based on regulatory demands			
4	Establishment and endorsing of a compliance policy	The governing body and top management, preferably in consultation with employees, should establish a compliance policy that: […] and should be endorsed by the governing body	Objective setting	Derivation of IT compliance and IT compliance reporting objectives from business requirements
5	Reviewing the reporting on the CMS performance	The governing body […] should ensure that they are effectively informed on the performance of the organization's compliance management system and of its continuing adequacy	Report compliance (-findings) / compliance reporting	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 noncompliances, in a timely manner..
6	Supervision of the CMS	The governing body and top management should assign the responsibility and authority to the compliance function for […] b) reporting on the performance of the compliance management system to the governing body and top management	Produce heatmaps	
7			Evaluate heatmaps	

8	The governing body should ensure that the organization's external and internal environment are regularly monitored and analysed to determine if there is a need to review and, when appropriate, revise the strategy for IT and any associated policies.		Manage policies	From the definition of management system, „set of interrelated or interacting elements of an organization to establish policies ...“ where policy is „intentions and direction of an organization as formally expressed by its top management
9			Monitoring	continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
10			Evaluate internal/external environment	Environments in which the organization seeks to achieve objectives
11			Support policy life-cycle	
12			Controls & policy mapping	
13	Evaluation of what is an acceptable risk to the organization	The governing body should set policies on internal control taking into account what is an acceptable risk to the organization. This should include the risk appetite relating to the use of IT and specific control requirements	Evaluate requirements	Requirements analysis comprises the identification of regulatory, legal, contractual, and other obligations that affect the organization’s IT operations.
14			Align with key objectives	Process of aligning risk management with organisational objectives.
15	Monitoring adequate audit coverage for IT related RM	For example, the governing body should ensure that there is adequate audit coverage of IT related risk management, control, and governance processes as part of the audit approach.	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
16			Resource management	“is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure”
17			Direct Value delivery	„is about executing the value proposition throughout the delivery cycle, concentrating on optimizing costs and providing the intrinsic value of IT”

18			Evaluate value delivery	„ensuring that IT delivers the promised benefits against the strategy”
19			Manage procedures / procedure	specified way to carry out an activity or process
20			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
21			Deviation analysis	After requirements analysis, adherence is examined with internal and external audits
22			Deficiency management	Results from deviation analysis are taken as requirements for deficiency management. Deficiencies are eliminated through improving, creating new controls or modifying parts of the control system
23			Remediation & control management	Is the process for managing uncontrollable project activities or circumstances that may result in negative consequences to remediation system performance
24			(IT) risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
25			Manage issues	
26			Develop KRI	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.
27			Event/risk identification	Process of finding, recognizing and describing risks.
28			Identify risks in processes using inquiries/surveys	Part of risk identification – „process of finding, recognizing and describing risks“
29			IT control self-assessment and measurement	Control self-assessment is a methodology used to review key business objectives, risks

				involved in achieving the objectives, and internal controls designed to manage those risks
30			Manage risks	„systematic application of management policies, proceduresand practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk“
31			Risk response/treatment	Process to modify/minimise the risk.
32			Control activities	Measure that is modifying the risk.
33			Update risks	
34			Update internal controls	
35			Reporting documentation	All actions are documented and relevant information is reported to stakeholders
36	Active involvement in CMS	The active involvement of, and supervision by, governing body and top management is an integral part of an effective compliance management system		
37	Escalation, where appropriate	Where appropriate, escalation should be to top management and the governing body, including relevant committees		
38	Application of governance to the management system	The strategies and policies for the use of IT (set by the governing body (and communicated to managers)) should provide the basis for the application of governance to the management systems of the organization. […] They may include: ─ Risk appetite relating to the use of IT and specific control requirements		
39	Commitment to developing of a compliance culture	The development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body		

40	Definition of roles and responsibilities	The governing body and top management should: […] c) include compliance responsibilities in position statements of top managers d) appoint or nominate a compliance function […]		
41	Evaluation of key risk management practices	In respect of IT, the governing body typically retains involvement in such things as: approval of key risk management practices such as those relating to security and business continuity.		
42	Demonstration of leadership and commitment with respect to the CMS (compliance management system)	The governing body and top management should demonstrate leadership and commitment with respect to the compliance management system		

VIII. Completeness survey results

Table a14. Completeness assessment feedback comments

Functionality	Process flow	Comments
Risk management	Monitor	"I think there should be more detailed framework not only ""who"" but also including what and how to monitor IT risk management. In advance there should be tools, technique and resources required/ needed. This apply for all your process flow (evaluate, direct, monitor, report)."
	Evaluate	"There should be external factor also included in the process of risk identification and evaluation. Evaluation focus on measuring changes in of risk residual, risk profile and what lesson learned (or what to improve regarding risk controls). some process name, i.e.: manage risks, control activities, risk response/ risk treatment - should not exclusively owned by Direct process flow. Evaluate process flow can be contained above process name."
	Report	What is the difference between risk in the triangle and the risk management process? Why are there no processes for governance and compliance management?
Policy management	Direct	Deficiency management = issue management? or two separate things?
		what about the relationship between governance, risk and compliance (e.g. risk measures and fulfilment of compliance requirements)
	Monitor	"what is exactly the difference between monitoring as part of policy management and audit management. IT control self-assessment could also be a methodology for audit management."
	Evaluate	"re: 1) translation of external regulations into operational compliance measures re: 2) again the term ""audits"" which could also be part of the audit management process"
	Report	"distinguish between documentation (part of compliance itself) and reporting of GRC outcomes Is there any connection between G, R and C in reporting?"

Audit management	Report	2 is inside of 1
		"define target groups of GRC reporting (internal and external) IT stakeholders?"
	Evaluate	"connection of risks and compliance requirements translation of laws and regulations into operational compliance measures"
Issue management	Direct	what is the difference between risks and issues (issues as materialized risks?)
	Evaluate	Not sure about the connection between issue management and value delivery

Table a15. Completeness assessment feedback grades 1 – definitely include, 2 – maybe include, 3 – maybe exclude, 4 – definitely exclude.

Functionality	**Process flow**	**Process**	**Grades**			
Audit management	Monitor	Performance measurement	1	2	2	1
	Evaluate	Re-assess risks	1	2	2	1
		Evaluate heatmaps	2	3	2	1
		Measure KPIs	1	1	2	2
		Inspect internal controls	1	1	2	1
	Report	Report findings	1	1	2	1
		Escalation where appropriate	2	2	4	
Issue management	Direct	Manage issues	1	1	2	2
		Update risks	2	1	1	2
		Update internal controls	1	2	2	1
		Value delivery	2	1	2	2
	Evaluate	Value delivery	2	2	3	1
	Report	Produce prioritized matrix/heatmaps	1	2	3	

Policy management	Direct	Strategic alignment	2	1	1	1
		Deficiency management	1	2	3	1
		Manage policies	1	1	1	1
		Manage procedures	1	1	2	1
		Define risk appetite	1	1	1	1
		Establish compliance management system	1	1	1	
		Commitment to developing of a compliance culture	1	1	3	
		Definition of roles and responsibilities	1	1	1	
	Evaluate	Requirements analysis	1	2	2	1
		Deviation analysis	1	1	2	
	Report	Reporting/documentation	1	2	2	1
		IT compliance reporting	1	2	1	1
	Monitor	IT control self-assessment and measurement	2	1	1	2
Risk management	Direct	Resource management	2	1	3	1
		Risk response - Risk treatment	1	1	1	1
		Control activities	1	1	1	1
		Manage risks	1	1	1	1
		Develop KRI - establish the context	1	1	1	1
		Remediation & control management	2	1	1	1
		Objective setting	1	2	3	1
	Evaluate	Internal environment - internal context	1	2	1	1
		Risk identification	1	1	1	1
		Determine risk appetite – risk attitude	1	1	1	1
	Report	Information & communication – communication and co...	2	1	1	1

	Monitor	Monitoring	1	1	1	1
	Evaluate	Evaluation of key risk management practices	1	1	1	

IX. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Mihkel Vunk**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

A Framework for Assessing Organisational IT Governance Risk and Compliance,

(title of thesis)

supervised by

Raimundas Matulevičius and Nicolas Mayer

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **03.03.2017**