ICT Governance, Risks and Compliance
A Systematic Quasi-review

Claudio Junior Nascimento da Silva, Denise Xavier Fortes
and Rogério Patrício Chagas do Nascimento
Federal University of Sergipe, Aracaju, Brazil

Keywords: ICT Governance, ICT Risks, ICT Compliance, Model.

Abstract: The present study aims to conduct a quasi-systematic review in a structured way to identify, evaluate and summarize the main evidence on Governance, Risk Management and Compliance in the area of Information Technology and Communication (ICT) of companies. The objective is to analyze the existing methods and / or techniques, characterizing their application in an ICT environment so as to enable the reader to be assisted through a secondary study. Thus, a research question was adopted to guide the quasi-systematic review that conducted an initial study of 47 articles, among which 18 were selected for the construction of this work through a selection that included ICT Governance, Risk Management and Compliance.

1 INTRODUCTION

In recent years the pressure on companies about Information and Communication Technology (ICT) managers has increased considerably. It is observed among the audit professionals a tendency in the examination of the computerized systems as a way to guarantee that the processes are producing the expected results.

In parallel with and under the pressure of high impact regulations in the business itself, such as the Sarbanes-Oxley Act 2002 (SOx), Basel II, European Directive 2006/43 / EC and from markets prone to crisis and frauds governance scandals, New requirements for corporate governance, risk management and compliance emerged (Racz, Weippl and Bonazzi, 2011)

The acronym GRC means Governance, Risk and Compliance as an integrated concept and describes different organizational activities, from the organization of an annual audit to the establishment of internal procedures for continuous monitoring, definition of roles and responsibilities in the business processes and users of the system. When restricting GRC activities for ICT operations, the term ITGRC is used, including Governance, Risk Management and ICT Compliance (Racz; Weippl; Bonazzi, 2011). According to ISO / IEC 38500: 2009, ICT Governance (ITG) is the system by which current and future use of ICT is directed and controlled. It involves evaluating and directing plans for the use of ICT to support the organization and monitoring of this use to achieve business objectives (Racz; Weippl; Bonazzi, 2011).

ICT Risk Management (ITRM) is seen as a part of enterprise risk management (ERM). It aims to identify potential events that may affect the entity, manage the risk to be within its limit or tolerance (risk appetite) and provide reasonable assurance about the achievement of the entity's objectives (Racz; Weippl; Bonazzi, 2011). ICT Compliance (ITC) describes processes to ensure an organization's ICT adherence to laws, regulations, contracts and other obligations (Racz; Weippl; Bonazzi, 2011).

In this context, this article presents a method proposed by (Kitchenham, 2004) and uses the protocol available by (Mafra, 2005), making use of primary studies to support the construction of this secondary study. Throughout this article we describe how this secondary study was conducted and presented the results of its analysis according to its characterization.

In the present study, 18 ITGRC methods or techniques are presented, with possible applications in ICT management of organizations. This article is divided into 5 sections. Section 2 describes the quasi-systematic review and protocol. Section 3 describes the conduct of this quasi-review and the results obtained. Section 4 presents the results of the quasi-systematic review using the categorization

Silva, C., Fortes, D. and Nascimento, R.
ICT Governance, Risks and Compliance - A Systematic Quasi-review.
DOI: 10.5220/0006317804170424
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 3*, pages 417-424
ISBN: 978-989-758-249-3

proposed for the methods and techniques encountered. Section 5 discusses the results of the analysis and points out future work. .

2 QUASI-SYSTEMATIC REVISION PLANNING

A summary of the three guidelines that are most frequently cited in the medical community is presented in (Kitchenham, 2004). A systematic review of the literature is characterized as a means to identify, evaluate and interpret all available and relevant research in a topic, area or element of interest for a specific study. Individual studies, such as research, case studies; experiments (ITG Institute, 2003) that contribute to a systematic review are characterized as primary studies. Systematic review is characterized as a secondary study (Mafra, 2005).

To conceive a well-formulated research question, it is necessary to describe its population, the factor under study (intervention), and the expected outcome for the review.

The protocol for a systematic review should include (Becker et al., 2011): Formulation of one or more research questions; Identification of the need for a systematic review; Comprehensive research, including primary studies; Quality assessment of included studies; Data extraction; Summary of study results; Interpretation of results to determine applicability and reporting. Systematic reviews have a well-defined research method that aims to obtain as much relevant bibliographic material as possible. Before conducting research on primary studies, it is necessary to define the systematic review protocol that will be used to perform the review. The protocol defines the inclusion and exclusion criteria for each primary study and documents the search strategy, allowing readers (researchers) to identify their degree of accuracy, the veracity of the topic, as well as its objective, as it uses a rigorous review reliable methodology and susceptible to auditing

The study in question has the objective of characterization, that is, there is no need for previous knowledge to make comparisons about the object searched. Thus, we call a quasi-systematic review, according to (Kitchenham, 2004). The purpose of this review is to examine existing methods and / or techniques in ITGRC to characterize their application in an ICT environment, through a secondary study. In the following subsections, we have the detailed protocol developed. Thus, it becomes possible to evaluate and repeat the review by other researchers

2.1 Objectives

The objective of this quasi-systematic review was formalized using the GQM model proposed by (Basili and Weiss, 1983) and presented by (Solingen et al., 2002): **To analyze** methods and / or techniques of ICT Governance, Risk Management and Compliance In ICT **for the purpose** of characterization **with respect** to the criteria for the use of methods and techniques **from the point** of view of the ICT managers of the organizations and **in the context** of the method (s) and / or the technique (s) that have a better application in a Environment.

2.2 Research Question

To reach the objective the following question was defined for the systematic review:

- **Question:** What are the existing methods and / or techniques for ITGRC?
- **Population:** Project Managers, ICT and CIO's Manager.
- **Intervention:** Methods and / or Techniques.
- **Results:** Methods and / or Techniques.
- **Evaluation and Experimentation:** Any type.

2.3 Strategy for Researching the Studies

The search strategy makes explicit the scope of the search, as well as the terms to be used in it, which are used to compose the search sequences. The definitions of these terms are through population, intervention, and expected results, which were defined in the research question.

- **Scope of research:** research in electronic databases, including journals and conferences;
- **Sources:** Scopus, Brazilian Digital Library (BDBComp), IEEExplore and Portal Periodicals CAPES.

Due to the fact that there are a large number of articles that contain the term ITGRC, it was necessary to consider it together with other terms in order to select the papers most related to the topic. The terms used in the search: Method, Technical, Model, Practices, Framework, IT Governance, Information Technology Governance, ITG, Risk, ITRM, Compliance, ITC and ITGRC. In Portuguese: “Método”, “Técnica”, “Modelo”, “Práticas”, Framework, “Governança de TI”, “Governança de

Tecnologia da Informação", "Riscos", ITRM, "Conformidade", "Conformidade", "ITC" and "ITGRC". The search sequence was generated by the combination of the key terms: ((OR method OR standards) AND (IT governance OR ITG) AND (risk OR ITRM) AND (compliance OR ITC) OR ITGRC).

2.4 Criteria for Selection, Inclusion and Exclusion of Studies

Criteria for Selection, Inclusion and Exclusion of Studies:

- Studies published after 2006;
- Keyword search tools;
- Consultation of articles available through the web.

The inclusion criteria for the studies were:

- Articles available on the;
- Must present studies on ICT Governance, Risks and Compliance;
- They must present full texts of the studies in electronic format;
- Must be written in English or Portuguese.

The exclusion criteria were:

- Studies on Governance, Risks and Compliance other than ICT;
- Do not answer research questions;
- Repeated: if the job is played in different search sources;
- Duplicates: works with similar studies. It will then be considered the most recent study or with more complete information;
- Irrelevant to the purpose of the research;
- Do not present conclusive results.

2.5 Data Extraction Strategy

For each selected item to the complete selection process, one researcher extracted the following data:

- Information for standard reference;
- For the question: a) The importance of the study to quasi-review; b) Description of the studies presented.

For the preliminary selection process, it was decided that a researcher applies the search strategy to identify primary studies. The results will be analyzed by another researcher involved and any disagreements will be discussed and resolved. If a consensus on a particular study is not achieved, it will be included

The final selection process: copies of all articles included as the initial search results will be reviewed entirely by at least one of the researchers. With this review of articles to be included, the process is terminated. If there is any disagreement about the reviewed articles, there will be a discussion to find a solution. If agreement is not reached, the item will be included. For the evaluation of the quality of the material, no procedure was prepared. The review aimed to find methods and / or techniques for ITGRC. The only question to be considered is that the article include a description of the method and / or technique, as this description will be part of the data to be extracted

3 QUASI-SYSTEMATIC REVIEW DEVELOPMENT

Advanced filtering tools were used to perform the search in the Scopus database and in the IEEExplore database, considering the summary (summary) of the articles, languages (Portuguese and English) and research area (Computer Science), with the purpose of minimizing articles that did not include ITGRC methods and / or techniques. However, for BDBComp, a basic search was performed, since the database does not have advanced search mechanisms. The following is a summary of the execution of the search in each database:

- **Scopus:** ((ABS ("method") OR ABS ("technical") OR ABS ("framework") OR ABS ("model") OR ABS ("PRACTIES")) AND (ABS ("IT GOVERNANCE") OR ABS ("ITG") OR ABS ("INFORMATION TECHNOLOGY GOVERNANCE")) AND (ABS ("RISK") OR ABS ("ITRM")) AND (ABS ("COMPLIANCE") OR ABS ("ITC"))) OR ABS ("ITGRC") AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cr") OR LIMIT-TO (DOCTYPE , "re")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "BUSI")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SRCTYPE , "p") OR LIMIT-TO (SRCTYPE , "j"));
- **IEEExplore:** (((method OR technical OR framework OR model OR practies) AND (it governance OR information technology governance OR ITG) AND (risk OR ITRM) AND (compliance OR ITC)) OR ITGRC);
- **BDBComp:** This database does not have an advanced search, so the key words in English and Portuguese were searched for by keywords: (("IT

governance") AND ("risk") AND ("compliance") AND ("methodology") AND ("model").

The planning of the quasi-systematic review occurred from October to November 2016. The search with the search sequences was carried out in November 2016.

In the search in the IEEExplore database, only keywords were used in English and 22 articles were obtained. Using the search parameters in the Scopus database, 25 articles were found. In the database BDBComp, no article with Portuguese or English keywords was found. In total, searches in the databases returned 47 articles. The largest number of articles is in the Scopus database, since it includes items from multiple databases (ACM, ScienceDirect, and others) is noted. These databases that make up Scopus are often used by Computer Science researchers (Tang, Meng, Wu, 2012)

Once the research was completed, the selection of articles was started based on selection criteria and procedures. With the adoption of inclusion and exclusion criteria for the articles, evaluations were carried out to answer the question asked. Of the 47 articles found, 18 were selected to compose the response to this quasi-Revision. Figure 1 illustrates the steps of the search process and article selection in this quasi-review and the study totals found. During the execution of the process of searching and selection of articles were carried out detailed analyzes with the purpose of identifying the items that best fit the proposed objective.

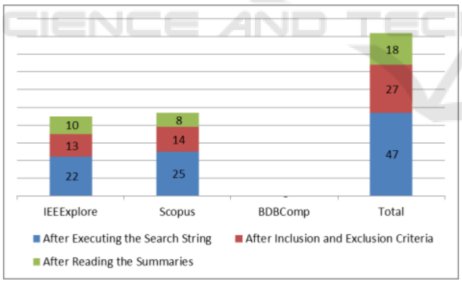

Figure 1: Process of Research and Adoption of Selection, Inclusion and Exclusion Criteria.

When applying search string and keywords in databases, 47 articles were found. After the adoption of the inclusion and exclusion criteria, 27 articles were found. These articles were summarized and had their methods or techniques described. It was observed that there was a great reduction in the number of articles. This reduction was obtained through exclusion criteria focused in the context of the article in which only 8 articles were selected in the Scopus database and 10 articles in the IEEExplore database.

The complete identification of the primary studies can be found in the References section of this article. After the completion of the selection, the primary studies were directed to the reading of the methods and / or techniques and analysis. The results of this step can be found below.

3.1 Results obtained

Table 1 summarizes the articles selected after searching the databases and executing the inclusion and exclusion criteria. The methods, methodologies, techniques or models that use ITGRC processes are briefly described.

The innvestigations of methods and / or techniques on ITGRC have varied over the years. However, in 2011 there was a greater dedication in relation to the other years, having been found eight studies. In 2009 no study was found on the subject. Figure 2 details the statistical evolution of the studies over the last decade (2006-2016).

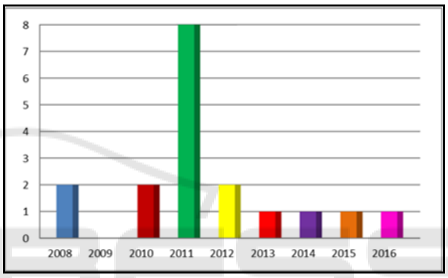

Figure 2: Statistics of Studies throughout the Last Decade.

The analysis of the data reveals that there is no predominance in the country of origin of the authors of the publications. Figure 3 shows that the United Kingdom and Switzerland, each with 3 publications, individually lead the ranking. However, it is generally perceived that Asian countries have a relatively large volume of publications. India, Malaysia and Indonesia contributed 5 publications.

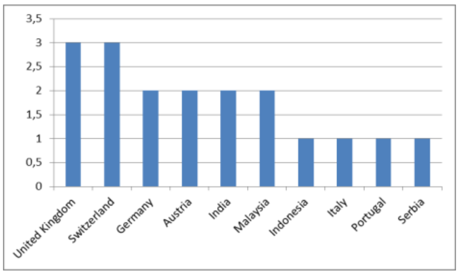

Figure 3: Ranking of the studies by country (author).

Table 1: Selected results.

Reference	Methods, Techniques and ICT Governance Models, Risks and Compliance (TTGRC)
(Maidin; Arshad, 2010)	The aim of this research is to develop the model of ICT governance practices for the public sector in Malaysia. Interview sessions were held with ICT professionals at the management level in Putrajaya. Based on the interviews, a theoretical model of ICT governance was built, which involves the involvement of top management in ICT, corporate performance measurement systems, corporate communication systems, risk management, strategic alignment, value delivery, ethics / culture Compliance and resource management.
(Becker *Et Al.*, 2011)	In this article, the main Digital Preservation capabilities were defined as ICT Governance processes and linked to the central processes of COBIT. Based on an established method for defining and controlling operations, a process model is suggested to abstract key activities, formalizing objectives, and enabling clear assignment of responsibilities.
(Gregory, 2011)	It highlights the need for care with customer data management. Defines and details data governance. Explains the strong link between corporate governance, risk and compliance and how the data sustain all three, and how it also needs to be governed.
(Krey *Et Al.*, 2010a)	In the first part of this article, different areas of focus for the GRC approach were derived. Successful application of ICT governance principles can provide a mechanism to increase the effectiveness of ICT and, on the other hand, meet the growing demands of ICT business. A survey was conducted to give an overview of the ICT governance models used in the health sector and tries to answer the question of whether they actually meet industry requirements.
(Kul, 2011)	This paper proposes a new conformity assessment and a new monitoring method to ensure the safe use of ICT resources made available by financial institutions.
(Tan; Eze; Teo, 2008)	Research indicates that governance of information and communication technology (ITG) is attracting tremendous attention from professionals and academics. This is fueled by the growing importance of ICT governance in delivering ICT Compliance and in its ability to create value for enterprises. Organizations realize the benefits of IT governance but are unfamiliar with ICT structures.
(Tang; Meng.; Wu, 2012)	Based on the quantitative content analysis of the existing literature from the year 1996 to the year 2010, this paper refines twelve essential components of the concept of ICT governance, including corporate governance, corporate goals, governance structure, governance process.
(Rubino; Vitolla, 2014)	The objective of this work is to analyze how the COBIT framework, integrated in the internal control framework, allows the improvement in the quality of the financial reports, helping to reduce or eliminate material weaknesses (MWS) of internal control over financial reporting (ICFR).
(Vukovic; Fertalj, 2008)	This article discusses reference model governance and frameworks, and proposes a holistic approach in which the prerequisites for quality assurance are built on information system architecture.
(Krey, 2015a)	Due to the complexity in both the hospital environment and the ITGRC field, the objectives of this paper are to systematize the importance of the integrated ICT GRC for health care to analyze the extent to which the principles of ITGRC are recognized, established and accepted by CIOs and ICT executives from Swiss hospitals.
(Krey, 2016b)	This research is associated with a survey that was conducted in 2009 and thus allows to draw conclusions about the progress of ITGRC management in Swiss hospitals in the last 5 years. The findings revealed that ITGRC in health care is still too often seen as the domain and sole responsibility of the CIO and the ICT department. The results demonstrated that IT GRC has not been sufficiently utilized by the executive management of many hospitals, especially the public ones.
(Wiesche; Schermann; Krcmar, 2013)	This article investigates the complications of effective governance conception for ICT risk management (ITRM). In the analysis of two organizations, however, it implies that both coercive and enabling governance for RTIs can lead to bureaucratic derision. The study contributes to the knowledge of the IT governance body, linking types of bureaucracy to IT governance tasks and providing associated anti-standards.
(Krey *Et Al.*, 2012b)	This article presents a practically validation method for this approach. After discussing the challenges for the development of a validation method, the concept of triangulation as a basis for the development of the method will be applied to the given context of health care.
(Saha *Et Al.*, 2011)	With the growing trend of globalization and e-governance initiatives passing by different industrial sectors, multinational corporations are forced to conform to the multiple government regulations required by various stakeholders including regulatory authorities, legal entities, consumer forums and partners. In this article, we propose a framework for the construction of a multiagent information model that captures the notion of compliance semantics and presents it using ontology.

Table 1: Selected results (cont.).

(Puspasari *Et Al.*, 2011)	The study reports the application of a tool that combines Governance, Risk and Compliance in ICT in a bank in Indonesia. Until then these policies were adopted separately, producing bad and damaging experiences for the organization. Based on the experience of the application of ICT Risk Management, the organization realized the importance of automation. He also realized that ICT risk management will be more effective when combined with the application of IT governance and compliance.
(Spies, 2011)	An approach to securing cloud security using model-driven architecture is presented. This approach integrates a number of current software assurance modeling frameworks as well as standardization efforts for cloud security based on ICT governance, risk and compliance management modeling, and reporting languages.
(Vicente; Silva, 2011)	In this paper we propose a business architecture that describes the integration of the main ITGRC processes. Based on a process model for IT GRC and a conceptual model for GRC, ArchiMate was used to model the behavioral, structural and informational structure from a business perspective - business processes, roles and business objects, respectively.
(Racz; Weippl; Bonazzi, 2011)	It presents an analysis of GRC's integration efforts in information technology departments of three large companies. Action project research is used to organize the research to evaluate ITGRC activities based on a five-dimensional model.

4 CATEGORIZATION OF METHODS AND TECHNIQUES FOUND

After the execution of the Quasi-Systematic Review process, the results obtained were characterized as criteria of use to facilitate the analysis. The proposed criteria were:

- **IT Governance (ITG)** - (yes / no) indicates if the presented works have activities in this area
- **ICT Risk Management (ITRM) -** (yes / no) - identifies whether selected papers are dedicated to activities in this area;
- **ICT Compliance (ITC)** - (yes / no) marks the works that have a focus of action in this area
- **Application -** classifies the application of the models identified according to the environment (Theoretical / Practical).

Table 2 identifies the studies selected according to categorization and established criteria.

Table 2: Classified results.

Reference	**ICT Governance**	**ICT Risks**	**ICT Compliance**	**Reference**
(Maidin; Arshad, 2010)	Yes	Yes	Yes	Theoretical
(Becker *Et Al.*, 2011)	Yes	No	Yes	Theoretical
(Gregory, 2011)	Yes	Yes	Yes	Practice
(Krey *Et Al.*, 2010a)	Yes	Yes	Yes	Theoretical
(Kul, 2011)	Yes	Yes	Yes	Theoretical
(Tan; Eze; Teo, 2008)	Yes	Yes	Yes	Theoretical
(Tang; Meng; Wu, 2012)	Yes	Yes	Yes	Theoretical
(Rubino; Vitolla, 2014)	Yes	No	Yes	Theoretical
(Vukovic; Fertalj, 2008)	Yes	No	No	Theoretical
(Krey, 2015a)	Yes	No	Yes	Practice
(Krey, 2016b)	Yes	No	Yes	Practice
(Wiesche; Schermann; Krcmar, 2013)	Yes	Yes	No	Theoretical
(Krey *Et Al.*, 2012b)	Yes	No	Yes	Practice
(Saha *Et Al.*, 2011)	Yes	No	Yes	Theoretical
(Puspasari *Et Al.*, 2011)	Yes	No	Yes	Practice
(Spies, 2011)	Yes	No	No	Theoretical
(Vicente; Silva, 2011)	Yes	Yes	Yes	Theoretical
(Racz; Weippl; Bonazzi, 2011)	Yes	Yes	Yes	Theoretical

Based on the selected studies, it was identified that in many cases, even referring to ICT Governance, ICT Risk Management and ICT Compliance, the methods / models and techniques did not concomitantly address the three areas. This can be observed in Fig. 4, which accurately illustrates the statistical data of the use of the areas in each selected study.

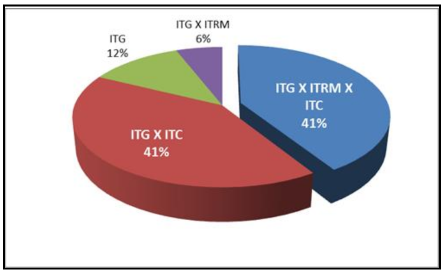

Figure 4: Use of Areas by Selected Study.

Regarding its application, it can be seen in Fig. 5 that the great majority is still in the Theoretical plan (67%), that is, proposed models that were not found in practice (33%).

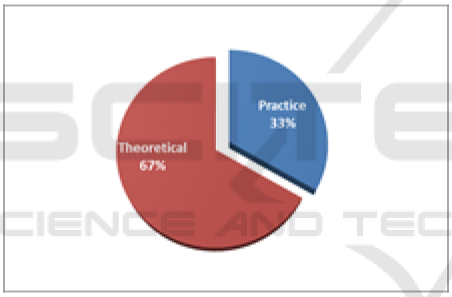

Figure 5: Application of the Proposed Models.

Considering the practical application, it is perceived that the concept of ITGRC is still far from being a reality within the organizations and even in the projects developed by the ICT área. Figure 6 illustrates the IT GRC execution process model used by several researched authors: Krey Et Al (2012b), Puspasari Et Al. (2011) and Racz, Weippl, Seufert (2010).

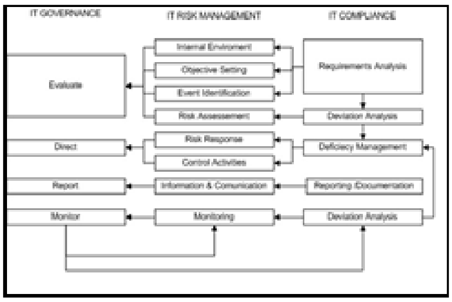

Figure 6: Process model for ITGRC.

5 CONCLUSION AND DISCUSSION OF RESULTS

In this work a quasi-systematic review was carried out to identify, analyze and characterize the ICT Governance methods, ICT Risk Management and ICT Compliance methods that can be applied in the industry. A research question was raised to guide this research and after evaluating a total of 47 studies initially returned, 18 were selected as studies relevant to the quasi-review.

The results show that until the date of the quasi-systematic review, it was not possible to identify a standard method or technique to promote and use knowledge of ITGRC. All studies found promote the practice of ICT Governance. However, the same does not occur when the criterion evaluated is ICT Risk Management and ICT Compliance. The combination of practices that define ITGRC requires that the three identified criteria or areas (ITG, ITMM and ITC) be considered concomitantly. This situation occurs in 41% of the cases studied

It is observed that many authors deal with Compliance, for example, but they never define action plans or procedures to aggregate this area to ICT Risk Management, ICT Governance or both. It must be considered that there is no perfect understanding of ICT managers or organizations' managers about the meaning, importance and necessity of a fully integrated Governance, Risk and Compliance (GRC).

It is believed that this research presents relevant results for the academy, presenting and supporting the characterization of ITGRC methods and techniques applied in ICT, becoming a source of relevant consultation for ICT management. As a future goal, one can investigate the degree of knowledge of project managers, ICT managers and CIOs about the meaning and importance of ITGRC in the ICT environment of organizations, whether private or public. In addition, it is possible to investigate the details of the operation of the ITGRC models used in organizations.

REFERENCES

Basili, V.R.; Weiss, D.M. A Methodology for Collecting Valid Software Engineering Data. 1983.

Becker, C. *Et Al*. Control Objectives for DP: Digital preservation. 48. 2011.

Gregory, A. Data governance Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability. Data and Digital Marketing Practice. 12 (3); pp. 230-248. 2011.

ITG Institute. (2003). Board Briefing on IT Governance. Rolling Meadows, IL 60008 USA: ITGI.

Kitchenham, B. Procedures for Performing Systematic Reviews, 2004.

Kitchenham, B.; Mendes, E.; Travasso, G. Protocol for Systematic Review of Within - and Cross – Company Estimation Models 1. 2007.

Krey, M. Significance and Current Status of Integrated IT GRC in Health Care: An Explorative Study in Swiss Hospitals. System Sciences (HICSS), 2015 48th Hawaii International Conference on, Kauai, HI, 2015, pp. 3002-3012. 2015a.

Krey, M. Next word prediction for phonetic typing by grouping language models. 2016 2nd International Conference on Information Management (ICIM), London, 2016, pp. 121-126. 2016b.

Krey. M. *Et Al.* IT governance and its spread in Swiss hospitals. Part of the IADIS Multi Conference on Computer Sci. MCCSIS 2010. pp. 52-60. 2010a.

Krey M. *Et Al.* Approach to the Evaluation of a Method for the Adoption of Information Technology Governance, Risk Management and Compliance in the Swiss Hospital Environment. System Science (HICSS), 2012 45th Hawaii International Conference on, Maui, HI, 2012, pp. 2810-2819. 2012b.

Kul, A. Regulatory compliance to ensure information security: Financial supervision perspective. ECIW 2011; pp. 298-306.2011.

Mafra, S.N. Protocolo de Revisão Sistemática. Grupo de Engenharia de Software Experimental, Programa de Engenharia de Sistemas e Computação (COPPER/UFRJ), 2005a.

Mafra, S.N.; Travassos, G.H. Técnicas de Leitura de Software: Uma Revisão Sistemática. 2007b.

Maidin, S.S.; Arshad, N.H. Information Technology Governance Practices in Malaysian Public Sector. In 2010 International Conference on Financial Theory and Engineering (pp. 281-285). Dubai, UAE, 2010.

Papazafeiropoulou, A.; Spanaki, K. Understanding governance, risk and compliance information systems (GRC IS): The experts view. Information Systems Frontiers, 1–13, 2015.

Patrick, C. "Embrace This Acronym: IT GRC. It Could Save Banks a Bundle. U.S. Banker. Nov2007, Vol. 117 Issue 11, p62. 2007.

Puspasari, D. *Et Al.* Designing a tool for IT Governance Risk Compliance: A case study. Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on, Jakarta, 2011, pp. 311-316.

Racz, N.; Weippl E.R.; Seufert A. A process model for integrated IT governance, risk, and compliance management. In Proceedings of the 9ª Conference on Databases and Information Systems, 2010.

Racz, N.; Weippl, E.R.; Bonazzi, R. IT Governance Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study. SERVICES 2011, pp. 429-436, July 4-9, 2011.

Rubino, M.; Vitolla, F. Internal control over financial reporting: opportunities using the COBIT framework. Managerial Auditing Journal. Vol. 29 Iss: 8; pp.736 - 771. 2014.

Saha P. *Et Al*. Ontology Based Modeling for Information Security Management. Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on, Sydney, NSW, 2011, pp. 73-80.

Spies, M. "A Software Assurance Evidence Approach to Cloud Security," 2011 22nd International Workshop on Database and Expert Systems Applications, Toulouse, 2011, pp. 39-43.

Solingen, R.V. *Et Al*. Goal question metric (gqm) approach Encycl. Softw. Eng., 2002.

Tan, K.S.; Eze, U.C.; Teo W.L. Information technology governance in the Malaysian electronics manufacturing industry. 1-2; pp. 587-593. 2008.

Tang, Z; Meng, J.; Wu, Y. The core components and conceptual framework of IT governance based on quantitative content analysis. pp. 196-204.2012.

Vicente, P.; Silva M.M. "A Business Viewpoint for Integrated IT Governance, Risk and Compliance," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 422-428.

Vukovic, D.; Fertalj. F. Information system quality assurance in finances building the quality assurance into information system architecture. ICSOFT 2008 - Proceedings of the 3rd Intern; ISDM (ABF/-); pp. 355-360. 2008.

Wiesche, M.; Schermann, M.; Krcmar, H. When IT Risk Management Produces More Harm than Good: The Phenomenon of 'Mock Bureaucracy'. System Sciences (HICSS), 2013 46th Hawaii International Conference on, Wailea, HI, USA, 2013, pp. 4502-4511.