Integration of IT Governance and Security Risk Management: a Systematic Literature Review

Dieter De Smet, Nicolas Mayer
Luxembourg Institute of Science and Technology
5, avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
{dieter.desmet, nicolas.mayer}@list.lu

Abstract— **GRC is an umbrella acronym covering the three disciplines of governance, risk management and compliance. In this context, IT GRC is the subset of GRC dealing with IT aspects of GRC. The main challenge of GRC is to have an approach as integrated as possible of the three domains. The objective of our paper is to study one facet of IT GRC: the links and integration between IT governance and risk management that we consider today as the least integrated. To do so, the method followed in this paper is a systematic literature review, in order to identify the existing research works in this field. The resulting contribution of the paper is a set of recommendations established for practitioners and for researchers on how better deal with the integration between IT governance and risk management.**

Keywords- IT governance; risk management; information security; systematic literature review; GRC

I. INTRODUCTION

Today, it is clearly acknowledged that Information Technology (IT) is no more only a technical issue. Thus, the complexity and importance of IT in companies involve a necessary governance layer. Such a governance layer generally encompasses risk management and compliance as steering tools. This evolution has implied the adoption of a new paradigm in IT, coming from the business world, usually referred to as "GRC". GRC is an umbrella acronym covering the three disciplines of governance, risk management and compliance.

The main challenge of GRC is to have an approach as integrated as possible to governance, risk management and compliance. The aim is to improve effectiveness and efficiency of the three disciplines, mainly compared to the traditional silo approach generally performed within organizations. Basically, according to Racz et al., GRC can be defined as "an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness" [1].

Our research field is focused on IT GRC, that can be considered as a subset of corporate GRC [2]. It is usually acknowledged that GRC in general (i.e. corporate GRC), and more specifically IT GRC, has currently received very few attention from the scientific community [2]. However, risk management and compliance are already well integrated in some contexts. For example, recent standards and regulations related to security include a part dedicated to risk management among the requirements the organization shall comply with [3, 4]. Moreover, compliance and governance are strongly connected and guidelines are available for practitioners. In particular, in ISO 19600:2014 [5] the activities involving the governing body of the organisation are formally mentioned in the standard when applicable and separated from the ones under the responsibility of the managers, making clear the link between governance and compliance in terms of roles and activities. Finally, in the preceding standards very few information is given on the relations between IT governance and risk management. More generally, we consider that the link between both domains is often neglected.

Our aim is to improve the integration of IT governance with risk aspects. More specifically, the focus of this paper is to propose recommendations to achieve a better consideration of security and risk in IT governance. These recommendations will be organised from the different perspective of GRC, i.e. strategy, process, people and tools [2]. To establish such guidelines, our approach is to analyse the links existing between IT governance and risk management through a systematic literature review.

Section 2 describes the protocol established and followed to perform our systematic literature review. Section 3 presents the raw results of our search protocol. Section 4 summarises the key findings we can draw up from the literature. Finally, Section 5 presents our conclusions from the work performed and introduces the future work.

II. SYSTEMATIC LITERATURE REVIEW

A. Targeted research

For this systematic literature review [6, 7], the main topic of interest is the state of the art on IT governance and its links with risk management and information security. The main motivations for this topic are (1) the identification of the necessary conditions for disposing of IT governance that includes explicitly risk management (2) the identification of the

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

978-1-908320/61/2/$31.00 © 2016 IEEE

different types of information that are needed for this (3) how to achieve this IT governance.

B. Methodology

This systematic literature review protocol, inspired by relevant literature in the field [6, 7], is composed of four successive steps.

First of all, the possible keywords were listed and these would be used for scanning through the different sources of information. A first list of keywords was formulated and submitted for review to another expert. This resulted in a modified list of keywords that would be used iteratively during the systematic literature review. Ten keywords were retained for applying the search protocol: Information governance, Information security, IT governance, IT risk, IT risk governance, IT security, IT security governance, IT value governance, Security governance and Value governance.

The next step involved the identification of the targeted research journals. The ranking used for this review is based on the ABS Academic Journal Guide 2010 (subject field Information Management). The grade four to two journals that were accessible from the Luxembourg database were retained. The Journal of the Association for Information Systems (JAIS) was however added to the list because of its relevance despite being not available from Luxembourg. The final list of journals to search with the keywords and the search protocol were: Decision Support Systems, European Journal of Information Systems, Information and Management, Information and Organization, Information Systems Journal, Information Systems Management, Information Systems Research, Journal of Information Technology, Journal of Management Information Systems, Journal of Strategic Information Systems, Journal of the Association for Information Systems (JAIS) and MIS Quarterly.

The third step consisted in the creation of the search protocol itself. The following field in the SCOPUS database was used to systematically go through the keywords per journal: "Article, title, abstract, keywords" AND "Source title" with a limitation on the publication year (ranging from 2000-2015), considering that GRC is a recent concept that has appeared in the early 21th century [2]. The entire search was conducted from 29/07/2015 until 11/08/2015 included.

The fourth and final step was the creation of the various inclusion and exclusion criteria that would be used to filter the obtained articles. A first set of criteria was proposed and submitted for review to another expert. This resulted in the following inclusion criteria for the preliminary scanning of the abstracts of the articles that were obtained by applying the search protocol/keywords: strategy, process, practices, enterprise architecture, tools, standards, risk management, governance structures, case study, policies. The exclusion criteria were defined as: software development, outsourcing, real options, supply chain, internet, SOX, internal control, websites, cloud, disclosures, employee behavioural research, shareholders, knowledge, mergers, acquisitions, conference proceedings, book chapters. After a few iterations in the screening process, it became clear that some type of studies emerged, which were not in scope of this research. Therefore the exclusion criteria used in the beginning were less strict than the final list that is presented in this article. Decisions on the creation of the new exclusion criteria by the analysing researcher were discussed with the internal team of experts.

The actual analysis of the outputs with this search protocol, keywords, inclusion and exclusion criteria was the following:

Apply the search protocol in SCOPUS → List all the obtained abstracts → Read and select the abstracts by using the inclusion and exclusion criteria → Decide to keep (or not) the full article by using the inclusion and exclusion criteria (+ check availability to download full text) → Read the remaining full articles. This process was applied to each source of articles (journals selected for this review).

III. RESULTS OF THE SYSTEMATIC LITERTATURE REVIEW

Table I contains the amount of articles that were obtained for every keyword and journal.

TABLE I. RESULTS OF SEARCH PROTOCOL

Journal	**Results of search protocol**	
	Articles found	***Articles left***
MIS Quarterly	106	12 articles selected on abstract 4 articles remained for reading after screening
Information Systems Research	105	7 articles selected on abstract 3 articles remained for reading after screening
Information Systems Journal	38	3 articles selected on abstract 3 articles remained for reading after screening
Journal of Management Information Systems	105	7 articles selected on abstract 5 articles remained for reading after screening
Journal of the Association for Information Systems (JAIS)	3	2 articles selected on abstract 0 articles remained for reading after screening
European Journal of Information Systems	90	5 articles selected on abstract 0 articles remained for reading after screening
Information and Management	123	9 articles selected on abstract 3 articles remained for reading after screening
Journal of Information Technology	101	15 articles selected on abstract 1 articles remained for reading after screening
Decision Support Systems	206	4 articles selected on abstract 2 articles remained for reading after screening

978-1-908320/61/2/$31.00 © 2016 IEEE

Journal	Results of search protocol	
	Articles found	*Articles left*
Journal of Strategic Information Systems	40	1 articles selected on abstract 1 articles remained for reading after screening
Information and Organisation	8	0 articles selected on abstract 0 articles remained for reading after screening
Information Systems Management	83	0 articles selected on abstract 0 articles remained for reading after screening
TOTAL	**1008**	**22 articles remained for reading after screening**

As presented in Table I, 1008 articles were parsed, and after the use of inclusion and exclusion criteria, 22 articles have been selected across the different journals. Within our selection of 22 articles, not all of them provided relevant conclusions on our specific topic. Usually, the main reason was that, although risk management was effectively addressed in the paper, it was not its key topic and no relevant conclusions or guidelines could be extracted or drawn up to help us to reach IT governance integrated with risk aspects.

IV. Structured Overview of Findings

This section presents the main observations and conclusions that can be argued from the systematic literature review. They are organised following the four facets of IT GRC: strategy, process, people and tool [2].

A. Strategy - Achieving good IT governance for information security

IT governance decisions in practice are expected to be associated with IT project investment decisions, which are discussed through the various coordination mechanisms. Past research proposed a conceptual model for the effectiveness of a company's security risk management programme [9]. This could be used as a starting point (or justification) for researching the decision process within IT governance by viewing the IT security risk aspects as another budget heading that is being discussed by the actors in the IT governance framework. Past research reported that IT security investments are handled in a similar fashion to general IT investments but that the context of IT security risk is very different [15]. Research to this part of the decision process in the IT governance framework merits more attention. Regarding the context, good IT governance in general is contingent upon the success of business-IT alignment, and sufficient focus on projects aimed at rationalizing the IT portfolio, to avoid the constraints produced by path dependencies due to previous technological choices or due to business transformations [10]. The interest of focusing on a given sector to research in IT governance is also supported by the literature [16] because it offers the needed contextual information (e.g., highly regulated sector, high industry concentration or vice versa).

An effective IT governance model requires attention to the following [10]:

- The positioning of the IT area in the organizational chart
- The level of centralization of the authority in IT decisions
- Kinds of decisions on IT investments taken at corporate level
- Kinds of decision on IT investments taken within a business unit/business function
- "Make or buy" decisions in the management of IT
- The coordination mechanisms used between the IT department and business units during the IT planning process
- Use of formal investments appraisal methods for evaluating the returns from ICT investments
- Prioritization mechanisms for IT investments

IT risk management perspectives are needed along these elements of attention. The following elements related to IT specifications (in line with the IT investment process) should benefit from IT risk management perspectives [14]:

- Defining the role of IT in the organisation (e.g. identify new ways to leverage IT)
- Identify IT investment opportunities
- Establish IT priorities
- Define IT service level expectations
- Setting timelines and budgets for IT initiatives

The following elements related to IT implementation should also benefit from IT risk management perspectives [14]:

- Application development
- System integration and testing
- Choosing application platforms
- Choosing programming languages and tools
- Evaluating proposed IT initiatives
- IT sourcing decision
- Vendor qualification and screening
- Defining IT standards
- Defining IT infrastructure strategy

Another article proposes the "IT Governance Cube" as a means to visualize the possible perspectives on IT governance research. It shows that the content of IT artefacts (from an IT governance perspective) is under-researched. This opens an opportunity for IT security management research as this can be viewed as a specific content of an enterprise IT artefact, where the decision rights and technical architecture could also be considered [14].

978-1-908320/61/2/$31.00 © 2016 IEEE

B. Process - IT investment decision process

Based on the decision process for IT investments [8], one could argue that IT risk management is not immediately considered. It becomes a part of this IT spending decision process, hinting at a possible reactive approach. IT governance is viewed as the *de facto* driver of decision-making processes within organizations. The nature of IT governance is contingent on the nature of the decision and the context in which the decision is made. As such, the IT risk management and security aspects should be adequately considered in the screening criteria for IT projects (business case, technical feasibility and strategic alignment) during the IT investment process by those designated for IT governance [8].

Another aspect is that the decision-making process that takes place among the leaders of companies influences IT governance in a significant manner. The trade-off between IT security and business risks is complex and the areas in need of attention at the moment of the decision-making process (i.e. their urgency and perceived priorities) further adds constraints [9].

IT governance and IT risk management are intertwined areas of practice. However research appears to be underexploring the IT risk management perspective during the overall IT investment process (framed by IT governance). This investment process can have three or four stages [17] but an IT security management perspective (contribution) seems to be missing.

C. Process - Coordination process

The different modes of governance coordination mechanisms can be characterized by being more centralized, shared or more distributed in the organization. The coordination mechanisms themselves can also be viewed as a process of consensus making [13] where IT security management elements should be added.

D. People - Involvement of stakeholders

IT governance is viewed as a component of the wider IT management model itself, with sufficient top management commitment, transversal communication, analysis/prioritisation of IT projects (business-IT alignment) within the overall strategic decision-making process of the company [10]. The human element poses the greatest information security threat to any company. This goes beyond the purely technical foundation of IT security management and (business) management involvement from various hierarchical layers [11].

In their description of the involvement of key stakeholders, Wai Fong and Yellin do not mention security managers or IT risk functions [12]. The discussion keeps its focus on the Enterprise Architecture (EA) team and the rest of the organisation. A possible future contribution could be to argue that IT security risk managers are such a "key stakeholder" because they can act as "stewards" of operational data and processes (even be "the owner") hence influencing whether the EA standards are accepted. The role of a business analyst is also mentioned as a possible boundary spanner between the EA team, the business units and other IT personnel. A possible new contribution could be to argue that IT risk analysts are another possible boundary spanner instead of the business analyst because they could also add to the specification of the requirements [12].

The centralisation of IT decision making is part of the research model used by Williams and Karahanna [13]. It is expected that it increases the ease of communication between the architecture team and other IT personnel. This provides other IT personnel the opportunity to voice their concerns. Centralization also makes it easier to ensure conformance to the EA standards and facilitate a follow-up on the different exceptions that are requested. These two elements could also imply future contributions and research by looking at the role of IT security profiles as a sub-set of the IT personnel. Possibly the IT risk perspective is one element of the IT governance frame and governance as a process between different roles and units in the company. Since one of the objectives of EA is the integration of applications and data across the company, IT risk management concerns should also be considered as this integration must be secure. Because the article says that EA standards for physical IT infrastructure reduce the heterogeneity and increase the compatibility of IT infrastructure components across business units by limiting technology choices [13], it seems arguable that IT risk managers or security managers need to be involved for defining this next IT infrastructure (supported by EA standards).

E. People - Interfirm cooperation

Tallon et al. state that a higher degree of technical knowledge is associated to a higher degree of IT risk taking. The success of IT projects is determined by the existing project management practices and the IT governance framework. IT governance is closely related to information governance and research provides a high level classification [16]. The decision making itself on information and the importance of steering committees for oversight are central. Hence a role for IT risk managers should be foreseen and this role can be involved in the following practices: data principles, data quality, data access, data life cycle and metadata. The contribution from IT risk managers in the cross-unit coordination committees could also be a new area of research. IT architectural modularity is influencing the overall IT agility that fosters alignment with the business strategy [14]. Although IT risk managers are not directly cited, yet it should be considered in the specification and implementation of IT projects. Strategic alignment between business development and IT spending is a critical area of attention.

F. People - More attention needed to the role of IT risk manager

IT governance archetypes have been proposed [17], elaborating on the attribution of responsibilities to organizational actors during the IT investment process and its implementation. It further discusses how they can interact, leaving out the possible contribution from IT risk managers. The CIO is a central actor in the IT governance framework, especially for the IT department that is involved, but this role should also be able to integrate the business and technical

978-1-908320/61/2/$31.00 © 2016 IEEE

perspectives (e.g. IT risk management). However the trade-off between business risk and IT risk in the IT investment process is difficult (e.g. due to path dependencies a.k.a. "legacies"). Top management commitment (CEO, CIO, CFO) to IT investments is needed while there must be a specific attention from this top management team to ICT in general as an enabler of a competitive advantage. One must also consider that human elements pose the greatest IT security risk. Various key architecture roles were discussed [12] in the literature but the IT risk manager is not at all in the picture, this is an opportunity for future developments since the IT risk manager role is a key stakeholder in IT governance.

G. Tools - The use of standards and reference models

The use of standards and reference models is recommended by the literature. Through the literature review, several models appeared, sometimes building on other reference models such as ISO/IEC 27001, PROTECT [18], Capability Maturity Model [19], Information Security Architecture [20]. A mapping between these different methodological tools and their information security components is especially available, combined with an "Information Security Governance Framework" that attempts to integrate the previously cited reference models [11].

V. CONCLUSION

In this paper, we have presented our approach to improve the integration of IT governance with risk aspects. The method selected was to perform a systematic literature review in this area, and then to identify from the selected results the key findings. The latter are organised according to the four facets of GRC: strategy, process, people and tools. Our contribution is thus first an overview of research results covering both IT governance and security risk management. As a conclusion, based on the systematic review of the literature we have performed, the key recommendations established for practitioners are:

- IT risks shall be better integrated in the IT strategy established, and along the lifecycle going from IT specification to IT implementation.
- IT risks shall be better integrated in the decision framework, taking care of the specificities and criticality of information security aspects. More specifically, a better consideration of IT risks is necessary in the IT investment decision process.
- The IT risk managers shall be considered as "key stakeholders" from an IT governance point of view.
- Governance coordination mechanisms shall better take care of IT risk management elements.
- The use of standards and reference models in the domain is recommended.

As argued by Racz [2], GRC has received very few attentions from the scientific community. Additional research work is also suggested by researchers, as observed during our systematic literature review. The key recommendations to the research community are:

- More research is needed to define how to well integrate security and risk management in the IT governance framework of organisations.
- A more sector-based research in IT governance is suggested to better take care of the context of the organisations.
- The contribution from IT risk managers in the cross-unit coordination committees could be a new area of research.

Regarding future work, we first plan to include the findings identified in this paper in our IT GRC model established, based on dedicated ISO standards [21]. It is also necessary to extend the conclusions and go further than what was obtained in this paper through the systematic literature review. This research work shall especially be completed with a review of the state-of-practice of IT GRC within organizations to propose more complete conclusions and draw a consolidated model of IT GRC.

REFERENCES

[1] N. Racz, E. Weippl, and A. Seufert, "A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)," in *Communications and Multimedia Security: 11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz, Austria, May 31 – June 2, 2010. Proceedings*, B. De Decker and I. Schaumüller-Bichl, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 106-117.

[2] N. Racz, *Governance, Risk and Compliance for Information Systems: Towards an Integrated Approach*. Saarbrücken: Sudwestdeutscher Verlag Fur Hochschulschriften AG, 2011.

[3] M. Dekker and C. Karsberg, *Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a,*: ENISA, 2013.

[4] ISO, "ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements," ed. Geneva: International Organization for Standardization, 2013.

[5] ISO, "ISO 19600:2014, Compliance management systems — Guidelines. ," ed. Geneva, 2014.

[6] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," *British Journal of Management,* vol. 14, pp. 207-222, 2003.

[7] S. K. Boell and D. Cecez-Kecmanovic, "On being 'systematic' in literature reviews in IS," *Journal of Information Technology (Palgrave Macmillan),* vol. 30, pp. 161-173, 2015.

[8] M.-S. Pang, "IT governance and business value in the public sector organizations — The role of elected representatives in IT governance and its impact on IT value in U.S. state governments," *Decision Support Systems,* vol. 59, pp. 274-285, 2014.

978-1-908320/61/2/$31.00 © 2016 IEEE

[9] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management,* vol. 41, pp. 597-607, 2004.

[10] P. Neirotti and E. Paolucci, "Assessing the strategic value of Information Technology: An analysis on the insurance sector," *Information & Management,* vol. 44, pp. 568-582, 2007.

[11] A. Da Veiga and J. H. P. Eloff, "An Information Security Governance Framework," *Information Systems Management,* vol. 24, pp. 361-372, Fall2007 2007.

[12] B. Wai Fong and D. Yellin, "Using Enterprise Architecture Standards in Managing Information Technology," *Journal of Management Information Systems,* vol. 23, pp. 163-207, Winter2006/2007 2006.

[13] C. K. Williams and E. Karahanna, "Causal explanation in the coordinating process: A critical realist case study of federated IT governance structures," *MIS Quarterly,* vol. 37, pp. 933-964, 2013.

[14] A. Tiwana and B. Konsynski, "Complementarities Between Organizational IT Architecture and Governance Structure," *Information Systems Research,* vol. 21, pp. 288-304, 2010.

[15] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment," *Journal of Management Information Systems,* vol. 25, pp. 281-304, Fall2008 2008.

[16] P. P. Tallon, R. V. Ramirez, and J. E. Short, "The Information Artifact in IT Governance: Toward a Theory of Information Governance," *Journal of Management Information Systems,* vol. 30, pp. 141-178, 2013/12/01 2013.

[17] X. Yajiong, L. Huigang, and W. R. Boulton, "Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context," *MIS Quarterly,* vol. 32, pp. 67-96, 2008.

[18] J. H. P. Eloff and M. M. Eloff, "Information security architecture," *Computer Fraud & Security,* vol. 2005, pp. 10-16, 2005.

[19] M. P. McCarthy and S. Campbell, *Security transformation*. New York: McGraw-Hill, 2001.

[20] J. K. Tudor, *Information security architecture - An integrated approach to security in an organization*. Boca Raton: Auerbach Publications, 2000.

[21] N. Mayer, B. Barafort, M. Picard, and S. Cortina, "An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance)," in *Systems, Software and Services Process Improvement*, Springer International Publishing, pp. 87-99, 2015.

978-1-908320/61/2/$31.00 © 2016 IEEE