An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance)

Nicolas Mayer[1], Béatrix Barafort[1], Michel Picard[1], and Stéphane Cortina[1]

[1] Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg
{nicolas.mayer, beatrix.barafort, michel.picard, stephane.cortina}@list.lu

Abstract. GRC (Governance, Risk and Compliance) is an umbrella acronym covering the three disciplines of governance, risk management and compliance. The main challenge behind this concept is the integration of these three areas, generally dealt with in silos. At the IT level (IT GRC), some research works have been proposed towards integration. However, the sources used for the construction of the resulting models are generally mixing formal standards, *de facto* standards arising from industrial consortia, and research results. In this paper, we specifically focus on defining an ISO compliant IT GRC integrated model, ISO standards representing by nature an international consensus. To do so, we analyse the ISO standards related to the GRC field and propose a way of integration. The result of this paper is an ISO compliant integrated model for IT GRC, aiming at improving the efficiency when dealing with the three disciplines together.

Keywords: Governance, Risk management, Compliance, GRC, Standards

1 Introduction

Today, it is clearly acknowledged that Information Technology (IT) is no more only a technical issue. Indeed, IT organization has evolved from technology providers to service providers and, according to Peterson [1], "Whereas the domain of IT Management focuses on the efficient and effective supply of IT services and products, and the management of IT operations, IT Governance faces the dual demand of (1) contributing to present business operations and performance, and (2) transforming and positioning IT for meeting future business challenges". 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 ap-

adfa, p. 1, 2011.

proach 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" [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 [3]. However, some reference models for IT GRC have recently emerged [3, 4] and propose relevant processes towards an integrated approach of governance, risk management and compliance for IT. These integrated frameworks rely on various sources, such as formal standards, *de facto* standards, or scientific models, but it is difficult to select and adopt adequate underlying models, and even more difficult to justify their selection is sound [3].

However, at the International Organization for Standardization (ISO) level, the three individual domains of GRC have been considered as mature enough to be standardized at an international level (see Section 3). International standards have been developed for IT governance [5], risk management [6], and very recently for compliance [7]. Nevertheless, to the best of our knowledge, there is no published standard (or standard in progress) dealing with an integrated approach for IT GRC.

Our aim is to define an integrated IT GRC model with the widest range of adoption. Our main assumption is that such a model should be based on ISO standards, representing by nature an international consensus. The objective of the paper is thus to specifically focus on defining an ISO compliant IT GRC integrated model. To do so, we analyse in this paper the ISO standards related to the GRC field and propose a structured way of integration.

Section 2 describes the related work by surveying existing IT GRC models and approaches. Section 3 is an overview of the standards for IT governance, (IT) risk management and (IT) compliance at the ISO level. Section 4 is about the construction of an ISO compliant IT GRC model, comprising the analysis of the existing ISO standards and their integration in an integrated model. Finally, Section 5 draws conclusions about the results and proposes some future work.

2 Related work

As stated in the introduction, our scope is focused on IT GRC that can be considered as a subset of corporate GRC [3]. Considering the lack of scientific references about IT GRC, we will also consider in this section some integrated approaches for corporate GRC, where IT GRC is contained.

Racz *et al.* have proposed a frame of reference for integrated GRC composed of three subjects (Governance, Risk Management and Compliance), four components (strategy, processes, technology and people), and rules associated to the subjects (respectively internal policies, risk appetite and external regulations) [2]. From this frame of reference, they have then defined a process model for integrated IT GRC management [3]. This process model is based on a mix between an ISO standard

(ISO/IEC 38500 [5]), an industrial standard (Enterprise Risk Management (ERM) — Integrated Framework [8] developed by COSO), and research results.

Based on the IT GRC process model of Racz *et al.*, Vicente and da Silva have proposed a business process viewpoint of IT GRC. Their research result is based on a merger between a conceptual model for GRC they defined [9] and the IT GRC process model of Racz *et al.* [3]. They have designed their business viewpoint for integrated IT GRC by modelling with ArchiMate [10], an enterprise architecture modelling language, the merger model and completing it with the business objects used between the business processes.

The Open Compliance and Ethics Group (OCEG), an industry-led non-profit organization, has published in 2012 the last release of the "GRC capability model (Red Book)" [11]. It is based on the so-called "Principled Performance" concept – a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty (both risk and reward) and acting with integrity (honouring both mandatory commitments and voluntary promises) – enabled by the GRC function in an organization. The scope of the GRC capability model is corporate GRC, and OCEG claims no compliance of their document to ISO standards or other references. COBIT 5 [12] is another governance framework owned by the Information Systems Audit and Control Association (ISACA), a non-profit organization. This framework for the governance and management of Enterprise IT helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. This framework is consistent with the ISO/IEC 38500:2015 [5] standard and can be considered as a pragmatic way to implement its concepts and principles within the organizations.

Gericke *et al.* have developed and evaluated a situational method that supports the implementation of an integrated GRC solution [13]. However, they are more concerned by rollout aspects than by organizational and recurring processes of GRC. Asnar & Massacci have developed another method, entitled "SI*-GRC" [14], comprising a modelling framework, an analysis process, analytical techniques, and a supporting software tool. This method is dedicated to information security and the outcome is the analysis and design of suited security controls.

Finally, some high-level frameworks have been established for GRC. We can mention the RSA GRC Reference Architecture [15] providing a visual representation of GRC within an organization, its guiding principles and its final objectives. Frigo & Anderson have proposed a "Strategic Governance, Risk, and Compliance Framework" composed of three layers [16]. Paulus has proposed a "GRC Reference Architecture" [17] consisting in four steps to follow (requirements modelling, status investigation, situation improvement, and crisis and incident management). Last but not least, Krey *et al.* developed an "IT GRC Health Care Framework" [18], taking care of health specific characteristics.

As a conclusion, a set of references and/or models have been established for GRC (and sometimes for IT GRC), but none of them propose an integrated and ISO compliant approach. The sources used for the construction of these models are generally mixing formal standards (i.e. standards established by formal standards organizations such as ISO, IEC or ITU), *de facto* standards arising from industrial consortia, and research results.

3 Overview of the ISO standards for IT governance, (IT) risk management and (IT) compliance

In this section, an overview of the ISO standards for IT governance, IT risk management and IT compliance (respectively ISO/IEC 38500:2015 [5], ISO 31000:2009 [6], and ISO 19600:2014 [7]) is performed. It is worth to note that ISO/IEC 38500:2015 is published by both ISO and IEC. IT being considered as an overlapping standardization domain between the respective scopes of ISO and IEC, they created in 1987 a Joint Technical Committee (JTC), known as ISO/IEC JTC1, to develop standards in the IT domain. In the next sections, each standard is presented first from an overall perspective, then from a structure perspective, and finally from a process perspective.

3.1 IT Governance

The reference document for IT governance at the ISO level is the ISO/IEC 38500:2015 standard [5] entitled "Information Technology — Governance of IT — for the organization". This International Standard is the flagship standard of the ISO/IEC 38500 series. The objective of ISO/IEC 38500:2015 is to provide guiding principles for governing bodies on the effective, efficient, and acceptable use of IT within their organizations. It also provides guidance to those advising, informing, or assisting governing bodies. The governance of IT is considered here as a subset of organizational governance (or corporate governance). ISO/IEC 38500:2015 is applicable to all types of organizations (i.e. public and private companies, government entities, not-for-profit organizations), whatever their size and regardless of the extent of their use of IT.

ISO/IEC TR 38502:2014 [19] provides guidance on the nature and mechanisms of governance and management together with the relationships between them, in the context of IT within an organization. The purpose of this Technical Report is to provide information on a framework and model that can be used to establish the boundaries and relationships between governance and management of an organization's current and future use of IT.

Structure: The IT governance framework developed by ISO/IEC lies on six principles (responsibility, strategy, acquisition, performance, conformance and human behaviour) and three main tasks (evaluate, direct and monitor). The main part of the standard is a guidance about the activities to perform for each of the six principles when passing through the "Evaluate – Direct – Monitor" process. Throughout the standard, ISO/IEC claims a clear distinction between the governing body, in charge of the IT governance, and managers, in charge of management systems for the use of IT, such as risk managers or compliance managers.

Process: The main tasks to be followed by IT governing bodies, represented in Fig. 1, are:

- **Evaluate** the current and future use of IT.
- **Direct** preparation and implementation of strategies and policies to ensure that use of IT meets business objectives.

- **Monitor** conformance to policies, and performance against the strategies.

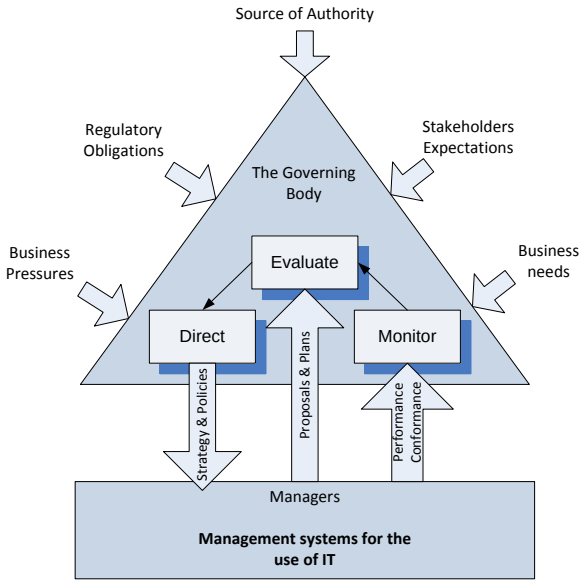

Fig. 1. Model for Governance of IT (as represented in [5])

3.2 IT Risk management

There is no dedicated IT risk management standard at the ISO level. Thus, the reference document for IT risk management is the ISO 31000:2009 standard [6] entitled "Risk management — Principles and guidelines" that can be applied to any type of risk, whatever its nature. ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual and is thus not specific to any industry or sector. The scope of ISO 31000:2009 is not focused on IT risk management, but on risk management in general, whatever the application domain. ISO/IEC 27005:2013 [20] is another relevant risk management standard that has been considered, but that is focused on information security. Although IT risk management and information security risk management are broadly overlapping, it is important to be aware that their concerns are different. From one side, IT risk management will consider risks related to IT strategy or to IT investments in general (i.e. not directly related to information security) that are not considered in information security risk management. From the other side, information security risk management may consider non-IT (e.g., paper-based) processes and their associated risks, that would not be considered in IT risk management.

Structure: ISO 31000:2009 is structured in three main parts. The first one provides a set of eleven principles an organization should comply with for risk management to be effective. The second part is a high-level framework which main objective is to assist the organization to integrate risk management into its overall management sys-

tem. This framework lies on a continual improvement cycle and suggest having such an approach for risk management. Finally, the last core part of the standard is the process to follow, embedded in the different phases of the general framework, and that is of main interest in this paper.

Process: The risk management process proposed in ISO 31000:2009 is represented in the next section within Fig. 2. It is composed of the following activities:

- **Establishing the context** of the organization, including the definition of the scope, objectives and context of the risk management process, and making clear what criteria will be used to evaluate the significance of risk.
- **Assessing the risks**, that means **identifying** sources of risk and areas of impacts, **analyzing** the risks through the estimation of the consequences of risks and the likelihood that those consequences can occur, and finally **evaluating** which risks need treatment and their priority level.
- **Treating the risks** via the selection of risk treatment options (e.g., modifying the risk with the help of design decisions leading to likelihood or consequences change, sharing the risk with another party, retaining the risk by informed decision, etc.) and definition of risk treatment plans. The risks are then assessed again to determine the residual risks: risk remaining after risk treatment.

In parallel of the preceding activities, it is also necessary to regularly monitor and review the risks and the underlying risk management process. Moreover, communication and consultation with the different stakeholders should take place during all stages of the risk management process.

3.3 IT Compliance

There is no dedicated IT compliance standard at the ISO level. Thus, the reference document for IT compliance is the ISO 19600:2014 standard [7] entitled "Compliance management systems — Guidelines". This standard provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization. Compliance is to be considered here as an outcome of an organization meeting its obligations, and is made sustainable by embedding it in the culture of the organization and in the behaviour and attitude of people working for it. The standard is based on the principles of good governance, proportionality, transparency and sustainability. The guidelines provided are applicable to all types of organizations.

Structure: The standard has adopted the so-called "high-level structure" developed by ISO to align the different management system standards. It consists of a fixed clause sequence, including common text and common terminology, which is completed with specific guidance on compliance management. The core of the standard is thus structured in seven main clauses (from Clause 4 to 10) that can be represented under the form of a flowchart described in more details in the next paragraph.

Process: The compliance management process proposed in ISO 19600:2014 is represented in Fig. 2 under the form of a flowchart. The main activities are the following:

- Establishment of the context of the organization, by **identifying external and internal issues**, and **interested parties and their requirements**. **Good governance principles** defined by the standard are also part of this context.
- **Determination of the scope of the compliance management system**, taking into account the context of the organization.
- **Establishment of a compliance policy** that is appropriate to the purpose of the organization, providing a framework for setting compliance objectives, and including a commitment to satisfy applicable requirements and to continual improvement.
- **Identification of compliance obligations** (including requirements the organization has to comply with and requirements it chooses to comply with) and **evaluation of related compliance risks**.
- **Planning on how to address compliance risks and how to achieve objectives.**
- Implementation of actions planned through **operational planning and control.**
- **Performance evaluation** through indicators development and application, audit, and management review.
- Improvement of the compliance management system by **managing non-compliances and continual improvement**.

4 An ISO Compliant IT GRC Model

In order to define an integrated IT GRC model, a bottom-up approach, based on the integration of the existing standards, has been followed. Our approach is composed of the following steps:

1. Identify common activities between risk management and compliance management
2. Extract in compliance management and risk management the tasks involving the governing body (at the opposite of what is under strict responsibility of managers) to encapsulate risk management and compliance management in a governance umbrella that integrates thus the three domains.

It is worth to note that the objective is not to exhaustively describe all of the activities to be performed in IT governance, IT compliance and IT risk management, but rather to focus on potential integration between activities that are redundant or interdependent in every single model. For example, the scope of IT governance is much broader than IT compliance and risk issues, and also encompasses topics such as generating business value from IT investments or optimizing the cost of IT services.

4.1 Common activities between compliance management and risk management

According to ISO 19600:2014, risk management is a key activity in a compliance management system. A compliance-related risk management process can clearly be

drawn all along the different steps of the compliance management system establishment, as highlighted in Fig. 2.

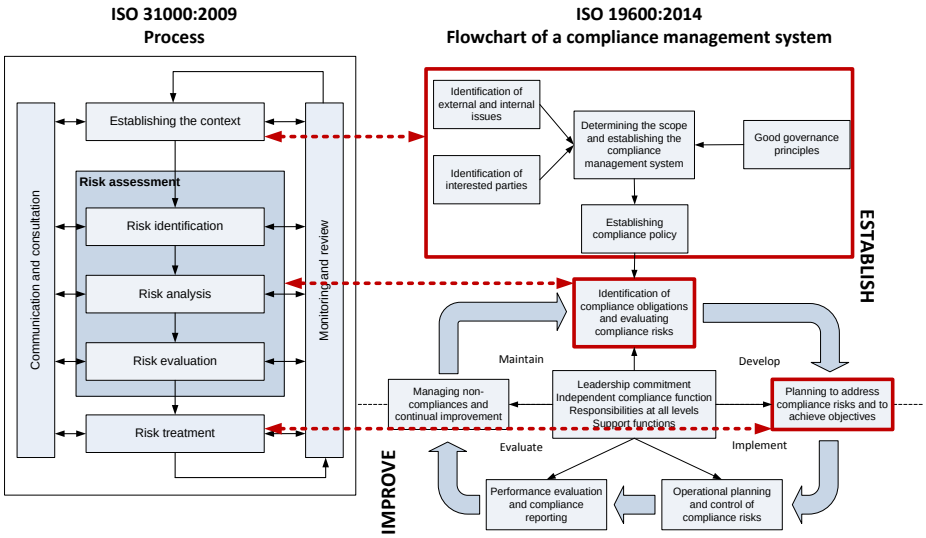

Fig. 2. Common activities between compliance management and risk management

Regarding ISO 31000:2009, the risk management process is part of the implementation step of the risk management framework, which is "intended […] to assist the organization to integrate risk management into its overall management system" [6]. In line with the preceding quote, we claim that to perform a compliance-related risk management process conforming with the ISO 31000:2009 process is fully aligned with ISO 19600:2014 requirements:

- By identifying external and internal issues, interested parties coming with their requirements, and following good governance principles, we are able to determine the scope and establish the compliance management system, then to establish the compliance policy (see Fig. 2). By doing this set of activities, we have especially established the context of the organization from a risk management perspective, including the definition of the risk-related scope, objectives and context.
- The next step about identification of compliance obligations (including requirements the organization has to comply with and requirements it chooses to comply with) and evaluation of related compliance risks consists in a risk assessment according to ISO 31000:2009.
- Finally, planning to address compliance risks and to achieve objectives includes a risk treatment process as described in ISO 31000:2009.

The other sets of requirements of ISO 19600:2014 that are related respectively to implementation of actions planned, performance evaluation, improvement of the compliance management system, and lastly compliance management system support activities (e.g., leadership commitment, roles and responsibilities, document management, etc.) are not directly related to the risk management process, but will provide

the relevant and necessary inputs for the risk monitoring and review activity, as required by ISO 31000:2009. As a conclusion, when establishing a compliance management system, it is relevant to deal with risk-related activities through an ISO 31000:2009 process.

4.2 Governance aspects of compliance and risk management

Basically, our objective is to identify in compliance and risk management standards the tasks involving the governing body. Referring to Fig. 1, the compliance and risk management related activities the governing body performs are extracted from the studied standards and highlighted in the frame of the Direct – Evaluate – Monitor process. They are summarized in Table 1.

Table 1. Compliance and risk management activities related to the governing body

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

It is a straightforward process to identify in ISO 19600:2014 the activities that involve the governing body of the organisation from the other activities led and/or per-

formed only by the managers of the organisation. The involvement of the governing body is indeed formally mentioned in the standard when applicable (references to the standard's clause are in square brackets):

- *[5.1] The governing body and top management should demonstrate leadership and commitment with respect to the compliance management system […]*
- *[5.2.1] 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*
- *[5.3.1] 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
- *[5.3.2] The active involvement of, and supervision by, governing body and top management is an integral part of an effective compliance management system*
- *[5.3.3] The governing body and top management should: […]*
  c) include compliance responsibilities in position statements of top managers
  d) appoint or nominate a compliance function […]
- *[7.3.2.3] The development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body […]*
- *[9.1.7] 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 […]*
- *[10.1.2] Where appropriate, escalation should be to top management and the governing body, including relevant committees*

In ISO 31000:2009, there is no separation of responsibilities between the management and the governing body. The different activities to be performed are formulated in a general manner, stating that "the organisation should […]". However, ISO/IEC TR 38502:2014, aiming at defining a framework and model about IT governance, provides further information about the role and responsibilities of the governing body, with regards, mainly, to risk management related to IT, but also some related to compliance:

- *[3.3] 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
- *[4.1.2] 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*
- *[4.2.2] 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*
- *[4.3.2] 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.*

- *[4.2.2] 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.*
- *[4.5.2] 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.*

Moreover, ISO/IEC TR 38502:2014 recommends to have a compliance committee and a risk management committee respectively for compliance and risk management in order to deal with the activities listed in Table 1.

5 Conclusion and future work

In this paper, our objective is to propose an integrated model for IT GRC inspired by, and compliant with, related ISO standards. It lays on existing ISO standards targeting (IT) GRC and, respectively, individually focusing on governance of IT (ISO/IEC 38500 series of standards), risk management (ISO 31000:2009), and compliance management system (ISO 19600:2014). The resulting model has been split in two parts. First, a systematic bottom-up approach has been followed in order to identify common activities between risk management and compliance management. Both standards can be combined by establishing the compliance management system in alignment with risk-related activities of the risk management process. Then, the overall part of the model has been derived from the ISO/IEC 38500:2015 model for governance of IT, where the key elements under the responsibility of the governing body for integrated IT GRC have been identified, with respect to the management ones.

Our results can help to existing standards improvement. For example, a clear distinction in ISO 31000 between governing body activities and management ones can help to better understand and implement the standard. New standards such as an integrated IT GRC standard can also be proposed in order to tackle the issues coming from the business world.

The proposed ISO compliant and integrated model for IT GRC provides a twofold view with the IT governance layer and the IT risk management and compliance one, where strategy, processes, technology and people can be integrated. The alignment of processes is a particular vector of integration and interoperability between the three disciplines of GRC and will be developed further by the authors. More future works will consist in the experimentation of the implementation of our IT GRC process model in an organization and benchmark its efficiency compared to dealing with IT governance, IT risk management and IT compliance in silos, making our work evolve from a theoretical model to a practical way to apply these ISO standards in an integrated manner.

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

6 References

1. Peterson, Ryan R: Integration strategies and tactics for information technology governance. In: Strategies for information technology governance. pp. 37–80. Idea Group Publishing, Hershey, PA (2004).
2. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: Decker, B.D. and Schaumüller-Bichl, I. (eds.) Communications and Multimedia Security. pp. 106–117. Springer Berlin Heidelberg (2010).
3. Racz, N.: Governance, Risk and Compliance for Information Systems: Towards an Integrated Approach. Sudwestdeutscher Verlag Fur Hochschulschriften AG, Saarbrücken (2011).
4. Vicente, P., da Silva, M.M.: A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In: 2011 IEEE World Congress on Services (SERVICES). pp. 422–428 (2011).
5. ISO/IEC 38500:2015: Information technology - Governance of IT for the organization. International Organization for Standardization, Geneva (2015).
6. ISO 31000:2009: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2009).
7. ISO 19600:2014: Compliance management systems — Guidelines. International Organization for Standardization, Geneva (2014).
8. Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework (Executive Summary and Framework). Committee of Sponsoring Organizations of the Treadway Commission (2004).
9. Vicente, P., Silva, M.M. da: A Conceptual Model for Integrated Governance, Risk and Compliance. In: Mouratidis, H. and Rolland, C. (eds.) Advanced Information Systems Engineering. pp. 199–213. Springer Berlin Heidelberg (2011).
10. The Open Group: ArchiMate 2.0 Specification. Van Haren Publishing, The Netherlands (2012).
11. OCEG: GRC Capability Model (Red Book 2.1). http://goo.gl/7nrKku (2012).
12. ISACA: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. (2012).
13. Gericke, A., Fill, H.-G., Karagiannis, D., Winter, R.: Situational method engineering for governance, risk and compliance information systems. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. pp. 24:1–24:12. ACM, New York, NY, USA (2009).
14. Asnar, Y., Massacci, F.: A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process Approach. In: Aldini, A. and Gorrieri, R. (eds.) Foundations of Security Analysis and Design VI. pp. 152–184. Springer Berlin Heidelberg (2011).
15. RSA: The RSA GRC Reference Architecture. (2013).
16. Frigo, M.L., Anderson, R.J.: A strategic framework for governance, risk, and compliance. Strateg. Finance. 90, 20–61 (2009).
17. Sachar Paulus: Overview Report: A GRC Reference Architecture, (2009).
18. Krey, M., Furnell, S., Harriehausen, B., Knoll, M.: Approach to the Evaluation of a Method for the Adoption of Information Technology Governance, Risk Management and Compliance in the Swiss Hospital Environment. In: 2012 45th Hawaii International Conference on System Science (HICSS). pp. 2810–2819 (2012).
19. ISO/IEC TR 38502:2014: Information technology - Governance of IT - Framework and model. International Organization for Standardization, Geneva (2014).
20. ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management. International Organization for Standardization, Geneva (2011).