International Journal of Business and Management; Vol. 13, No. 12; 2018
ISSN 1833-3850 E-ISSN 1833-8119
Published by Canadian Center of Science and Education

A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance

Michele Rubino[1]

[1] Department of Economics and Management, University LUM Jean Monnet, Italy

Correspondence: Michele Rubino, Department of Economics and Management, University LUM Jean Monnet, Casamassima (BA) - Italy. E-mail: rubino@lum.it

Received: September 28, 2018 Accepted: October 16, 2018 Online Published: November 20, 2018

doi:10.5539/ijbm.v13n12p203 URL: https://doi.org/10.5539/ijbm.v13n12p203

Abstract

The significance of the Enterprise Risk Management (ERM) is widely recognized by the academic and professional literature. Knowledge and management of business risks are an integral part of every successful business strategy and are increasingly becoming a primary factor of competitiveness. Although several risk management frameworks have been published and updated over time, these standards still have limitations. The advent of IT helped companies to better manage business risks. The rise of the IT governance has improved the management and the monitoring of business processes as well as the implementation of policies and procedures. The aim of this paper is twofold. First, a comparative analysis of the main risk management frameworks was carried out, highlighting their limits and weaknesses. Second, it was highlighted how the IT governance and the related frameworks as COBIT could contribute to a better implementation of the risk management process that allows to overcome the limitations of the examined standards.

Keywords: COSO ERM update, ISO 31000, AS/NZS 4360 standard, Framework for the Management of Risk – Canada, IT Governance and COBIT 5 for risk

1. Introduction

The relevance of the role played by the ERM is widely recognized by the academic (Jensen, 1993; Spira & Page, 2003; Power, 2004; Rubino & Vitolla, 2012a; Mikes & Kaplan, 2015) and professional literature (COSO, 1992, 2004 and 2017; ISACA, 2012 and 2013). The past 30 years have been characterized by a growing interest in risk management issues (Olson & Whu, 2015). Indeed, the great corporate scandals have highlighted the limits and weaknesses of companies in identifying and managing risks. At the same time, companies have increased the awareness that risk management facilitates the achievement of corporate objectives by ensuring the preservation and growth of company value. Effective risk management allows the understanding of the potential positive and negative aspects that can influence the company's activity and, at the same time, increases the chances of business success, reducing uncertainty about the achievement of the set goals.

In order to guide public and private companies to implement a correct and effective risk management process, over time different standards have been published. There is no standard universal approach to implement ERM. However, some frameworks such as the COSO ERM, the ISO 31000 risk management guidelines, the AS/NZS 4360 standard and the framework for the Management of Risk – Canada have been suggested (Raz & Hillson, 2005; Frigo & Anderson, 2014; Ahmad et al., 2014; Agarwal & Ansell, 2016). Although these frameworks have been recently updated they still have some limitations. Existing risk management frameworks often have different structures, requirements and terminology that prevent their effective understanding and implementation (IRM 2018a). One of the reasons that pushed the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2017, to update the ERM framework was to promote a greater understanding and applicability of the standard to make it simpler, clearer and more integrated into business management. Indeed, frameworks such as COSO are often considered as highly abstract conceptual frameworks that do not identify control objectives at a level of specificity sufficient to design detailed audit tests (Tuttle & Vandervelde, 2007; Huang et al., 2011; Rubino & Vitolla, 2014c). Concurrently, it should be noted that many standards focus on the general phases of the risk process, leaving out more specific aspects related to the management of processes and the definition of policies and procedures. Furthermore, in some frameworks the terms like risk culture and risk appetite are often defined in a vague way (Bromiley et al., 2015). In contrast, these aspects are increasingly seen in IT governance frameworks. For example, the COBIT framework is becoming increasingly established within companies by supporting control frameworks and expanding their reach (Ridley et al., 2004; Tuttle & Vandervelde, 2007; Rubino & Vitolla, 2012b and 2014a).

The aim of this paper is twofold. First, a comparative analysis of the main risk management frameworks was carried out to: (a) bring models back to a common analysis scheme; and (b) highlight their peculiarities and limitations. Second, how the IT governance and the related frameworks could contribute to a better implementation of the risk management process was highlighted, allowing to overcome the limitations of the examined standards.

The paper is structured as follows. Section 2 compares the main risk management clarifying their aim, scope and structure. Section 3 bringing frameworks back to a common analysis scheme by illustrating the existing similarities and divergences. Section 4 highlights the main limits of the risk frameworks and illustrates how the IT governance and the COBIT 5 for risk framework could help firms to a better implementation of the risk management process. Finally, the main conclusions are outlined.

2. The Frameworks' Aim, Scope and Structure

The purpose of this section is to perform a comparative analysis of the main risk management frameworks recognized and applied worldwide to highlight their peculiarities by identifying a common risk management process. The analysis focuses on the COSO ERM (Enterprise Risk Management), the ISO 31000 standard, the AS/NZS 4360 framework and on the Risk Management Framework applied in Canada. The decision to analyze these frameworks concerns the consideration and observation that they are more structured and provide a good level of analysis of the theme, compared to other smaller frameworks applied worldwide.

The analysis shows that most used standards, although introduced in the past, have recently been updated to make them more adherent and applicable to the various private and public companies. The COSO ERM, issued in 2004, has been updated in 2017 to help managers understand and prioritize the risks their organizations face and measure how these risks impact business performance. The complexity of the implementation (Bromiley et al., 2015), the lack of integration of the ERM at the strategic level (Bromiley & Rau, 2016) and the changes in the external environment are just some of the reasons that required the updating (COSO, 2017). The underlying philosophy of the new framework emphasizes the way in which risk management is carried out, which must normally be carried out as part of the business, observing not only negative risks, but also potential positive risks. Therefore, the risks must be analyzed in conjunction with the decisions related to the strategy and the impact assessments on performance.

The ISO 31000 guidelines introduced in 2009 were also updated in 2018 to support companies in: (a) applying risk management principles to improve their risk planning and assessment; and (b) to make more effective and easier decision-making measures. The new ISO 31000 keeps risk management simple by emphasizing the concept of leadership by the top management in risk management as well as the need for continuous interaction with the external environment and finally the importance of interactive risk management (IRM, 2018b).

The AS/NZS 4360 framework, on the other hand, is another important tool for guiding companies to manage risk. This standard was published in 1999 by the Joint Standards Australia / Standards New Zealand Committee - Risk Management and, subsequently, was updated with the publication of the 2004 and 2009 releases. The latest version has introduced the 11 principles adopted by ISO improving the framework applicability.

Finally, the last standard to be compared is the Framework for the Management of Risk - Canada which in 2010 replaced the Integrated Risk Management Framework (2001) and the Integrated Implementation Management Guide (2004). This framework represents a tool which is specifically applicable to public administrations. In this sector, characterized by a strong dynamism and complexity, risk management plays a significant role in strengthening the ability of the government to recognize, understand, welcome and capitalize on new challenges and opportunities. Effective risk management enables federal governmental organizations to actively respond to change and uncertainty by using risk-based information to enable more effective decision-making. The risk-based approach to risk management, articulated in this framework, offers the flexibility for departments and agencies to adapt management solutions to their mandate and objectives.

All frameworks describe risk in terms of threats and opportunities. However, some standards like the AS/NZS 4360, contemplated only later a risk definition also considering positive events. As shown in Table 1, as regards the aim and scope, the different frameworks show a strong similarity. All standards analyzed provide guidelines and general principles that encourage and facilitate the effective and efficient implementation and development of risk management activities. These activities are applicable to a wide range of organizations and not only to individual projects but to all the activities of the bodies, whether public or private. In cases where the frameworks have been updated, a goal linked to increase management and stakeholder confidence and the importance of considering risk in both the strategy-setting process and in driving performance are highlighted (COSO, 2017). As regards the ISO 31000 framework, it is possible to state that the aim of the new standard is very similar to the original version. However, both the ISO 3100 guideline and the AS/NZS 4360 standard clearly state that they not intend to promote uniformity of risk management across organizations. In this regard the ISO 31000 highlights that the design and implementation of risk management plans and frameworks will need to consider the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed. Finally, the Framework for the Management of Risk – Canada provide guidance to apply ERM into the public administration.

Table 1. Risk management frameworks' aim and scope

Framework	Aim and scope
COSO ERM 2004	This framework provides key principles and concepts, a common language, and clear direction and guidance, for an enterprise risk management. It is expected that the framework will become widely accepted by companies and other organizations and indeed all stakeholders and interested parties. The framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.
COSO ERM 2017	This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment. It is a concise framework for applying enterprise risk management within any organization to increase management and stakeholder confidence. The updated document highlights the importance of considering risk in both the strategy-setting process and in driving performance.
ISO 31000 (2009 and 2018)	This international standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture. Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities. This standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context. The standard it is not intended to promote uniformity of risk management across organizations.
AS/NZS 4360 2009	This international standard provides principles and generic guidelines on risk management and can be used by any public, private or community enterprise, association, group or individual. The standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. The standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations.
Framework for the Management of Risk – Canada (2010)	The purpose of this framework is to provide guidance to Deputy Heads on the implementation of effective risk management practices at all levels of their organization. This will support strategic priority setting and resource allocation, informed decisions with respect to risk tolerance, and improved results. The framework provides principles and guidance for Deputy Heads to consider in their role as leaders of sound risk management practices and risk management integration within their organizations.

Examining the depth level of the standards, it is possible to say that COSO ERM with its 254 pages provides a greater level of detail regarding the principles and focus points. However, also the other standards appear quite exhaustive. In particular, it should be noted that the Framework for the Management of Risk - Canada, being specifically addressed to the public sector, specifically provides for a series of principles and check lists concerning the bodies and specific management characteristics of the public administration.

3. The Frameworks' Risk Management Process

As regards the risk management process, it is possible to state that the frameworks have a comparable approach by sharing similar activities. However, in order to allow an effective comparison, it appropriate to trace back the activities of the standards into a common scheme by identifying four main phases that should generally characterize a risk management process as indicated in Table 2. The apparent divergences essentially depend on variations in the use of the terminology or by the explicit or implicit prediction of some phases or activities. This highlights the existence of a broad consensus on how to implement the risk management process, which should include the following phases:

1. Understanding the organization and its internal and external context, which concern:

(a) the organizational environment, which reflects the philosophy of the top management in risk and its levels of acceptability, the culture of risk and behaviour of people operating at all levels of the company, the managerial style, the integrity and ethical values, skills, definition of areas of authority and responsibility, the existence of appropriate policies and procedures.

(b) the external context which should include (but is not limited to) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; key drivers and trends having impact on the objectives of the organization; and relationships with, perceptions and values of external stakeholders.

(c) The objectives setting. To achieve the successful integration of the risk management function into the organization, it is important to set vision, objectives and operating principles of the organization. A clear articulation of the vision, objectives and operating principles could also help foster the creation and promotion of a supportive risk management culture. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

2. Risk management activity. This phase is central to the risk management process. First, it is necessary to identify events inside and outside the organization, which affect the achievement of its objectives, must be appropriately identified and distinguished in opportunities (events with a positive impact) and risks (events with negative impact). The former must be evaluated by reconsidering the previously defined strategic planning process, while the latter must be the subject to adequate analysis aimed at defining the appropriate strategies to manage them. Secondly, the risks associated with the identified events must be assessed. The management pays attention to risks following a scale of priorities, depending on their likelihood of a future event, also considering their impact. Risks are assessed in terms of inherence (risk in the absence of any intervention) and residual (residual risk, or risk that persists after the implementation of interventions for its downsizing). Finally, after having selected the significant risks, the management assesses the responses to each risk (avoid, accept, reduce or share it), starting actions to align the risks identified with the levels of risk tolerance and risk appetite. Risk response or treatment involves selecting one or more options for modifying risks and implementing those options.

3. Control activities and monitoring. An effective risk management requires that policies and procedures must be defined and implemented to ensure that risk responses are provided effectively through the establishment of control mechanisms, i.e. organizational procedures and solutions aimed at limiting operational risks and identifying actual risks. The control activities make it possible to: identify possible events or risk factors; implement changes in policies and procedures and/or adopt new control procedures; monitor the effectiveness of the controls already implemented. At the same time the risk management process must be subjected to continuous monitoring that verifies the correct and effective functioning, as well as the adequacy with respect to the internal and external context of the company.

4. Information and communication. Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance. Therefore, it is relevant to identify, collected and disseminated information in the right form and time in such a way as to allow all the corporate subjects to fulfil their responsibilities. The information systems produce reports containing operational and accounting data relating to compliance with legal and regulatory obligations, which allow the management and control of company activities. These systems treat not only the data produced internally by the company, but also those related to events, activities and external situations, necessary to make detailed decisions and prepare the financial information. Equally important are the processes of communication, i.e. the ways in which information is shared and monitored within the company system. The quality of information and communication processes increasingly depends on the quality of the information system that can be formalized or not.

Table 2. The frameworks' risk management process

Phases	Framework for the Management of Risk - Canada	ISO 31000 (2009 and 2018)	AS/NZS 4360 2009	COSO ERM 2004	COSO ERM 2017
1	Planning and Designing the Approach and Process	Establishing the Context	Establishing the context	Internal Environment Objective Setting	Governance and Culture Strategy and Objective-Setting
2	Implementing Integrated Risk Management	Risk assessment Risk treatment	Risk assessment Risk treatment	Event Identification Risk Assessment Risk Response	Performance
3	Practicing Integrated Risk Management	Monitoring and review	Monitoring and review	Control Activities Monitoring	Review and Revision
4	Continuously Improving Integrated Risk Management	Communicate and consult Recording and reporting*	Communicate and consult	Information and Communication	Information, Communication and Reporting

* This component was comprised only in the ISO 31000:2018.

Although in each framework the individual components of the model are displayed in sequence, it should be noted that risk management is not a strictly sequential process, but an interactive and multi-directional process in which each component can influence another independently of the sequence of the same. Examining Table 2, it emerges that each framework provides a series of activities able to contemplate the four identified phases. However, there are differences. First, unlike other frameworks, COSO ERM has been reported twice in table 2 to allow the examination of the new and the old structure. The COSO ERM updated introduces a new structure composed by five related components for which the relevant principles are outlined. In the developmental process, COSO built the framework passing from the COSO cube, which remains valid, to the rainbow double helix. Considering that the most important and distinctive aspects of COSO's definition of ERM in the framework applied in strategy-setting and across the enterprise were either misunderstood or ignored in practice (Protiviti, 2016), a review of the framework has been carried out. The components that have undergone the major changes concern: strategy and objective setting, performance and information, communication and reporting.

COSO provides a multidimensional focus in strategy-setting highlighting that risk to the strategy is not the only dimension of risk to consider strategically (Bowling & Rieger, 2005; Rubino et al., 2017a and b; Frigo & Anderson; 2011). There is the possibility of a strategy not aligning with the company's mission, vision and core values that define what it is trying to achieve and how it intends to carry out business. Moreover, management must consider the implications of the strategy chosen considering that each alternative strategy has its own risk profile (Protiviti, 2016). Furthermore, the update framework provides a road map to improve cyber risk management and introduces a focus on reporting that must supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations (COSO, 2017).

Considering the four common phases described above, examining in depth the individual frameworks, the following can be stated:

1. In the first phase, the only framework that includes two components is COSO ERM even if, between the version of 2004 and 2017, there are profound differences in terms of emphasis on aspects such as governance, the examination of the strategy, its implementation and the related risks. Instead, the other frameworks identify a single component that does not include all the elements that should be present in phase 1. For example, reference is not made to ethical values to governance aspects, management style, codes of conduct, human resource's skills and the definition of areas of authority and responsibility. However, some aspects are generally identified at the level of mandate and commitment and the new ISO 31000 updated fills part of these gaps. However, compared to COSO, ISO and AS/NZS standards dedicates more space to the analysis of the external context.
2. In the second phase, there are no substantial differences between the frameworks. COSO ERM 2017 introduces a component called performance that embraces the former components of the old ERM. The new ERM document focuses on the concept according to which manage risk organisation-wide helps to sustain and improve performance. Concurrently, a correct risk management activity creates, preserves,

realizes and reduces the erosion of a company's value. As regards the risk assessment and response the AS/NZS standard carries out an in-depth analysis compared to the others.

3. There are no differences about the third and fourth phases. The control monitoring activities and those related to the framework revision of the as well as those related to the information and communication components are examined in each framework. The only positive developments that exist are those related to the fourth phase, introduced by the COSO update, which has delivered two specific principles. The first one is devoted to the use and management of information, to the risks involved, and to the management of information systems. The second concerns the reporting activities that supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy and objective-setting, governance, and day-to-day operations (COSO, 2017).

The standard that is more complete and comprehensive, from every point of view is, without a doubt, the COSO ERM framework whose analysis must be carried out jointly, also observing the original model of 2004 that remains valid. The recent introduction of the principles, for each component of the model, guides the management facilitating the implementation of the model. COSO ERM is the most complete standard but this is also evident from the body of the document that exceeds 250 pages against the 50 pages of which the other standards are made up on average. This aspect has been one of the limitations of the model. Indeed, the other frameworks, although less exhaustive, are lean and easier to understand and apply. Among these, we can certainly point out the ISO 31000 guideline that, as noted, was updated in 2018. Instead, the Canadian framework represents a valid best practice to implement the risk management in the public administration. From this standpoint, the framework differs from the others by providing a model that is sufficiently clear to the applicability and to the organs involved in its execution.

4. The Risk Frameworks' Limitations and Weaknesses: The Role of the IT Governance

Despite the updates, in relation to some aspects, the risk frameworks are not sufficient for the implementation of an effective and correct risk management process. First, it should be noted that implementing a risk management process means setting up an internal control system, which it is a whole of: coordinated and integrated structures; formal support and operating mechanisms; safeguards; actions; and corrective and improvement mechanisms aimed at the prevention of risks relating to business management. This indicates the high complexity that characterize risk management implementation, which must be integrated with the company's control systems (Mikes & Kaplan, 2015; Agarwal & Ansell, 2016).

Considering that the risk management frameworks are little integrated with the corporate control systems, including strategic planning and management control, the first limitation becomes clear (Williamson, 2007). As already noted, the update of the COSO starts from the observation that applications of ERM were rarely integrated with strategy-setting (Protiviti, 2016; COSO, 2017). Although COSO has partially covered the theme of defining strategic objectives, there is still no clear integration with the themes of management control (Desender, 2011). Even worse, the other frameworks completely neglect the management of the issues. Moreover, some empirical evidence highlight that some companies tried to implement ERM as an assurance initiative, rather than to run and manage the business better (Protiviti, 2016; COSO, 2017). From this, it follows that risk management frameworks appear to be strongly disconnected from management control tools. The guidelines often reflect a methodology that can not be considered as alternative to the classical tools of corporate control. The different standards should recall, at various levels, the tools of corporate control. From their reading often emerges a list of things that appears disconnected from the vision of corporate control.

Another aspect that limits the applicability of risk frameworks is linked to their high level of abstraction. Tuttle and Vandervelde (2007) argue that risk management frameworks does not identify control objectives at a level of specificity sufficient to design detailed audit tests. This is confirmed also in other research (Huang et al., 2011; Rubino & Vitolla, 2017a). Power (2009) states that COSO ERM do not ensure the understanding of the risk concept and its implications is weak. It is obvious that frameworks must represent general guidelines and consequently they can not foresee specific situations considering that risk management varies from company to company. However, despite the frameworks provide a set of principles that describe practices that can be applied in different ways for different companies' size, type, or sector, there are no indications on how to structure the main processes within companies. The definition of the processes, the subjects involved, and the people in charge could help the managers to better implement the risk process.

In addition, all risk frameworks include the information and communications component but do not provide for integration procedures with information systems. This aspect represents the major weakness of risk frameworks given the role that information, information systems and IT governance frameworks play within companies. Many boards are not receiving the information they need. The PwC annual corporate directors survey of the 2016, argued that 58% of boards do not receive updates at every meeting on the amount of risk the company is taking. This aspect highlights a big limit for companies that requires a more in-depth analysis of the problem.

How can risk management frameworks' limitations and weaknesses be overcome? This question has been answered by companies that are increasingly using with the classics risk frameworks, such as COSO, IT governance standards such as COBIT (Rubino & Vitolla, 2017b). In 2013, this framework introduced a special guide called "COBIT 5 for Risk" and is now preparing the COBIT 2019 version to consolidate its role as the main reference point for the governance of IT and, in general, of the entire corporate system. Therefore, a possible support to solve the problems related to the risk management frameworks can be offered by the information system and the support frameworks.

Over the past few decades, the ability to pursue the goals set by companies, is becoming linked to the quality and availability of information and the systems that manage it (Javaid & Iqbal, 2017). At the core of all companies' processes, information should be available to management to turn it into effective and timely decisions (Rubino et al., 2017a). IT is increasingly being recognized and used as a tool to assist with managerial activities that involve decision-making for complex organizational problems (Chapman, 2005, Liew, 2015). IT plays an important role in creating new knowledge and became an essential especially in the global knowledge society (Granlund, 2011; Peslak, 2012; Rubino et al., 2017b). The digitalization of business processes, which goes far beyond document dematerialisation, is an example of how IT can contribute to managing a business in an integrated, effective and collaborative way, governing business risks and approaching the concept of Industry 4.0. Therefore, the role of IT becomes fundamental for the provision of services, the management of resources and for the organization and coordination of the entire corporate structure. Today IT structures, by their pervasiveness, have become primary partners of the business functions for the innovation of products and business processes. For these reasons the IT governance and IT alignment started to be commonly used in company language.

IT Governance is that part of the broader corporate governance that deals with the governance of information systems in the company, which has the function of designing the IT of the future and of tracing the initiatives able to bring the current IT towards the realization of this goal. IT Governance manages the link between the strategic vision of corporate business and the operational, management of tools, processes, and people that make IT work (Van Grembergen & De Haes, 2008; Debreceny, 2013). Generally, IT governance has a dual role. On the one hand, it incorporates and spreads strategic business objectives through a more operational and procedural language, as well as those linked to costs, risks and compliance. On the other, measures and communicates to the corporate bodies the performance achieved by identifying any anomalies found in the company processes (Rubino et al. 2017a). Instead, IT alignment means linking business and the IT plan i.e. ensuring that there is consistency between the business strategy and the IT strategy (Chan & Reich, 2007). Many studies have shown that those companies that successfully align their business strategy with their IT strategy will outperform those that do not (Kearns & Lederer, 2003; Kathuria et al., 2007). Therefore, managing, aligning and governing IT means identifying processes for the control and management of IT to ensure the achievement of the objectives set by the company, which, in most cases, are attributable to the effectiveness and efficiency of their institutional duties and the related management of business risks. Professional and academic literature suggests that IT serves as the foundation of an effective system of internal controls (COSO, 2013; Masli et al., 2011; Li et al., 2012) ensuring the achievement of the main objectives as enhance company's performance (Nfuka & Rusu, 2011) the improvement of the reliability of financial reporting (Hirshleifer & Teoh 2003;Rubino & Vitolla, 2014c), the compliance with applicable laws and regulations (De Haes et al., 2013) and the risk mitigation (Devos et al., 2012; Rubino & Vitolla, 2014b).

Therefore, in relation to risk frameworks it is possible to see how IT governance and the related support frameworks can help overcome the limits and the weaknesses highlighted. IT alignment makes it possible to overcome the first limit by requiring the construction and implementation of an information system that considers the company objectives and is strictly connected to the logic and the corporate control tools. Secondly, the IT governance logic requires a concrete vision of reality by constructing and managing a system that is in line with what is required (Racz et al., 2010). Therefore, there can be no abstractness and low level of detail in IT management. On the contrary, these aspects constitute the bases of the management of information systems. Furthermore, IT management and the development of information system requires the mapping of IT processes with a view to supporting the business. The strategic model for the IT Governance consists mainly of two macro realities in which to map the processes: (a) Operative processes, which have the task of promoting the good functioning of the IT and (b) Analytical Processes, which monitor and analyze the functioning of the IT in the planning and governance phases.

One of the frameworks that has been emerging in recent years is the COBIT whose new COBIT 2019 full release will be published by December 2018. This Framework, as extensively documented by the academic literature (Lainhart IV, 2000; Ridley et al., 2004; Khrisna, 2014; Rubino & Vitolla, 2014b; Rubino et al., 2017a and b; Javaid & Iqbal, 2017), is specifically oriented towards defining IT controls aimed at ensuring certain information requirements. The model structure is based on a series of processes that help to implement an effective IT governance system which produces benefits also on the internal control and risk management system. Another important aspect of the structure of the COBIT is that relating to the definition of roles and responsibilities, which are fundamental for risk management activities. A specific guideline, called COBIT 5 for Risk, was published in 2013, which illustrates the phases and processes, procedures and policies that should be implemented for effective risk management. From a quick analysis of the framework it is easy to observe that COBIT 5 for Risk allows to overcome the main limits of the observed risk frameworks.

First, COBIT 5 provides a holistic and systemic view on governance and management of enterprise IT based on the following seven categories of enablers which are broadly defined as anything that can help to achieve the objectives of the enterprise: (1) Principles, Policies and Frameworks; (2) Processes; (3) Organisational Structures; (4) Culture, Ethics and Behaviour; (5) Information; (6) Services, Infrastructure and Applications; and (7) People, Skills and Competencies (ISACA, 2012). COBIT 5 for Risk provides guidance and describes how each enabler contributes to the overall governance and management of the risk function. For each enabler this framework defines the organisational structures and the processes that are required to: (a) govern and manage risk effectively and (b) define and sustain the risk function. Furthermore, are identified what people and skills should be put in place to establish and operate an effective risk function and what information flows are required (ISACA, 2013). Second, COBIT 5 for Risk defines seven risk principles, which formalise and standardise the risk policy implementation, to provide a systematic, timely and structured approach to risk management and to Contribute to consistent, comparable and reliable results. These policies provide more detailed guidance on how to put principles into practice and how they will influence decision making within a company. In addition, the framework identifies 3 categories of processes that are required to support the risk function: (1) Key supporting processes; (2) other supporting processes; and (c) the core risk processes as the EDM03 (which ensure risk optimisation) and the APO12 (which manages risk). Third, the framework provides specific guidance related to all enablers for the effective management of risk. In particular, it defines the core risk management processes and identifies 111 risk scenario examples across 20 scenario categories, i.e., the key information item needed to identify, analyse and respond to risk, the risk appetite and tolerance. Finally, COBIT 5 for Risk ensure compliance with the main risk management frameworks. This specific IT governance framework addresses both all ISO 31000 principles and all the components defined in COSO ERM.

Therefore, it is possible to state that COBIT for 5 risk: (a) allows a perfect integration with the company information system; (b) provides guidelines with a high level of detail; and (c) is closely connected to business management by supporting the classical tools of corporate control. At the same time, the framework ensure companies many benefits such as: (1) a more accurate view of significant current and near-future risk throughout the company; (2) understanding how effective IT risk management optimises value by enabling process effectiveness and efficiency; (3) opportunities for integration of IT risk management with the overall risk and compliance structures within the company; (4) promotion of risk responsibility and its acceptance (ISACA, 2013).

5. Conclusions

Implementing risk management is a complex activity that varies from company to company based on a series of elements such as corporate culture in terms of control, the existence of a well-defined organizational structure, the provision of appropriate procedures and company policies, the existence of an effective action carried out by the corporate governance bodies, the presence of managerial skills and so on (Rubino & Vitolla, 2012a; Rubino et al., 2017a; Bogodistov & Wohlgemuth, 2017; Agarwal & Kallapur, 2018). Therefore, the analysis of all these elements and many others cannot be contained in a simple guideline, especially if this is very small or limited such as the main risk management frameworks. As observed, the best and commonly used guideline is the COSO ERM, which presents, like the others, some limitations. Very long guidelines would be necessary, yet they would not solve anything. The solution suggested and already adopted by some companies is to support the risk frameworks of IT governance frameworks such as COBIT. Implementing and managing the information system basically means setting up a control system ensuring at least:

- The adaptation of IT to the company's activities;

- The continuous and constant coordination of IT services used by the different business areas;
- The control of the costs and benefits of the IT services provided;
- The management and measurement of company performance;
- The risk management and not just IT risks;
- The definition of processes, policies and procedures;
- The definition of information processing and corporate communication systems;
- The configuration of the company organization; and
- The implementation of procedures in line with the company control system.

The definition of these aspects and of many more, together with the application of what is described in the risk management standards would allow companies to better face future challenges.

Although the topic of the risk management has been widely explored in the literature, only a few studies have focused on the analysis of the frameworks to highlight any potential application problems. Therefore, this paper contributed to broaden the knowledge of the topic by highlighting important managerial implications. The implementation of risk management activities can be carried out by considering a reliable standard such as COSO ERM or ISO 31000 guidelines. However, this is not sufficient because the aspects related to IT governance must be considered. It is no coincidence that the auditors suggest to combine the COBIT framework with the COSO ERM to ensure SOX compliance (Abu-Musa, 2008; Rubino & Vitolla, 2014c).

This paper deals with the analysis of the COBIT 5 for Risk framework in a residual way. Future research could better illustrate the benefits that companies can obtain in the implementation phase of risk management activities.

References

Abu-Musa, A. A. (2008). Information technology and its implications for internal auditing: An empirical study of Saudi organizations. *Managerial Auditing Journal*, *23*(5), 438-466. https://doi.org/10.1108/02686900810875280

Agarwal, R., & Ansell, J. (2016). Strategic change in enterprise risk management. *Strategic Change*, *25*(4), 427-439. https://doi.org/10.1002/jsc.2072

Agarwal, R., & Kallapur, S. (2018). Cognitive risk culture and advanced roles of actors in risk governance: a case study. *The Journal of Risk Finance*. https://doi.org/10.1108/JRF-11-2017-0189

Ahmad, S., Ng, C., & McManus, L. A. (2014). Enterprise risk management (ERM) implementation: Some empirical evidence from large Australian companies. *Procedia-Social and Behavioral Sciences*, *164*, 541-547. https://doi.org/10.1016/j.sbspro.2014.11.144

Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: a capability-based perspective. *The Journal of Risk Finance*, *18*(3), 234-251. https://doi.org/10.1108/JRF-10-2016-0131

Bowling, D. M., & Rieger, L. (2005). Success factors for implementing enterprise risk management: building on the COSO framework for enterprise risk management to reduce overall risk. *Bank Accounting & Finance*, *18*(3), 21-27.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long range planning*, *48*(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

Bromiley, P. and Rau, D. (2016). A better way of managing major risks: Strategic risk management. *IESE Insight*, *28*, 15-22.

Chan, Y. E., & Reich, B. H. (2007). IT alignment: what have we learned? *Journal of Information technology*, *22*(4), 297-315. Available at https://link.springer.com/article/10.1057/palgrave.jit.2000109

Chapman, C. S. (2005). Not because they are new: developing the contribution of enterprise resource planning systems to management control research. *Accounting, Organizations and Society*, *7*(30), 685-689. https://doi.org/10.1016/j.aos.2005.02.002

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). *Internal Control – Integrated Framework*, American Institute of Certified Public Accountants, New York.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise Risk Management – Integrated Framework*. New York: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control – Integrated Framework*. Amercan Institute of Certified Public Accountants (AICPA), Durham.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*. New York: American Institute of Certified Public Accountants.

Debreceny, R. S. (2013). Research on IT governance, risk, and value: challenges and opportunities. *Journal of Information Systems*, *27*(1), 29-135. https://doi.org/10.2308/isys-10339

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: building blocks and research opportunities. *Journal of Information Systems*, *1*(27), 307-324. https://doi.org/10.2308/isys-50422

Desender, K. (2011). On the determinants of enterprise risk management implementation. In *Enterprise IT governance, business value and performance measurement*. IGI Global.

Devos, J., Van Landeghem, H., & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. *Industrial Management & Data Systems*, *2*(112), 206-223. https://doi.org/10.1108/02635571211204263

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*, *22*(3), 81-88. https://doi.org/10.1002/jcaf.20677

Frigo, M. L., & Anderson, R. J. (2014). Risk management frameworks: Adapt, don't adopt. *Strategic Finance*, January, 49-54.

Granlund, M. (2011). Extending AIS research to management accounting and control issues: A research note. *International Journal of Accounting Information Systems*, *1*(12), 3-19. https://doi.org/10.1016/j.accinf.2010.11.001

Hirshleifer, D., & Teoh, S. H. (2003). Limited attention, information disclosure, and financial reporting. *Journal of Accounting and Economics*, *1*(36), 337-386. https://doi.org/10.1016/j.jacceco.2003.10.002

Huang, S. M., Hung, W. H., Yen, D. C., Chang, I. C., & Jiang, D. (2011). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, *50*(4), 692-701. https://doi.org/10.1016/j.dss.2010.08.015

Information Systems Audit and Control Association (ISACA). (2012). COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT, ISACA, Rolling Meadows, IL.

Information Systems Audit and Control Association (ISACA). (2013). COBIT 5 for Risk. ISACA, Rolling Meadows, IL.

Institute of Risk Management (IRM). (2018a). *From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks*. Institute of Risk Management, London.

Institute of Risk Management (IRM). (2018b). *A Risk Practitioners Guide to ISO 31000: 2018*. Institute of Risk Management, London.

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In *International Conference on Communication Technologies* (Com Tech), 78-90. https://doi.org/10.1109/COMTECH.2017.806575

Jensen, M. C. (1993). The modern industrial revolution, exit, and the failure of internal control systems. *Journal of Finance*, *48*(3), 831-880. https://doi.org/10.1111/j.1540-6261.1993.tb04022.x

Khrisna, A. (2014). Risk management framework with COBIT 5 and risk management framework for cloud computing integration. In *International Conference of Advanced Informatics: Concept, Theory and Application* (ICAICTA), 103-108. https://doi.org/10.1109/ICAICTA.2014.7005923

Kathuria, R., Joshi, M. P., & Porth, S. J. (2007). Organizational alignment and performance: past, present and future. *Management Decision*, *45*(3), 503-517. https://doi.org/10.1108/00251740710745106

Kearns, G. S., & Lederer, A. L. (2003). A resource-based view of strategic IT alignment: how knowledge sharing creates competitive advantage. *Decision sciences*, *34*(1), 1-29. https://doi.org/10.1111/1540-5915.02289

Lainhart IV, J. W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*, *14*(s-1), 21-25.

Li, C., Peters, G. F., Richardson, V. J., & Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: the case of Sarbanes–Oxley internal control reports. *MIS Quarterly*, *1*(36), 179-203. https://www.jstor.org/stable/41410413

Liew, A. (2015). The use of technology-structured management controls: changes in senior management's decision-making behaviours. *International Journal of Accounting Information Systems*, *1*(17), 37-64. https://doi.org/10.1016/j.accinf.2014.05.001

Masli, A., Richardson, V. J., Sanchez, J. M., & Smith, R. E. (2011). The business value of IT: a synthesis and framework of archival research. *Journal of Information Systems*, *2*(25), 81-116. https://doi.org/10.2308/isys-10117

Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance*, *27*(1), 37-40. https://doi.org/10.1111/jacf.12102

Nfuka, E. N., & Rusu, L. (2011). The effect of critical success factors on IT governance performance. *Industrial Management & Data Systems*, *9*(111), 1418-1448. https://doi.org/10.1108/02635571111182773

Olson, D. L., & Wu, D. D. (2015). *Enterprise risk management* (2nd ed.). London: World Scientific Publishing Company.

Peslak, A. R. (2012). An analysis of critical information technology issues facing organizations. *Industrial Management & Data Systems*, *5*(112), 808-827. https://doi.org/10.1108/02635571211232389

Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos.

Power, M. (2009). The risk management of nothing. *Accounting, organizations and society*, *34*(6-7), 849-855. https://doi.org/10.1016/j.aos.2009.06.001

Protiviti, (2016). Updated COSO ERM Framework: What's New? *The Bulletin*, *6*(2).

Racz, N., Weippl, E., & Seufert, A. (2010). A process model for integrated IT governance, risk, and compliance management. In *Proceedings of the Ninth Baltic Conference on Databases and Information Systems* (DB&IS 2010) (pp. 155-170).

Raz, T., & Hillson, D. (2005). A comparative review of risk management standards. *Risk Management*, *7*(4), 53-66. https://doi.org/10.1057/palgrave.rm.8240227

Ridley, G., Young, J., & Carroll, P. (2004, January). COBIT and its Utilization: A framework from the literature. In System Sciences, 2004. *Proceedings of the 37th Annual Hawaii International Conference on IEEE*.

Rubino, M., & Vitolla, F. (2012a). Risk management, a key process of corporate governance: analysis of the related effects on organisational behavior. In Tipuric, D. and Dabic, M. (Eds.), *Management, Governance and Entrepreneurship: New Perspectives and Challenges* (pp. 314-327). Access Press, Darwen, UK.

Rubino, M., & Vitolla, F. (2012b). *Sistemi informativi e controllo interno: un approccio integrato. Analisi di un modello a supporto della compliance*. Cacucci Editore, Italy.

Rubino, M., & Vitolla, F. (2014a). IT governance, risk management and internal control system: the role of the COBIT framework. In Tipuric, D. and Mešin, M. (Eds.), *Proceedings of the 2nd International OFEL Conference on Governance, Management and Entrepreneurship: Inside and Outside of Managerial mind. Building the bridges between disciplines*, CIRU, Dubrovnik, 174-188.

Rubino, M., & Vitolla, F. (2014b). Corporate governance and the information system: How a framework for IT governance supports ERM. *Corporate Governance*, *14*(3), 320-338. https://doi.org/10.1108/CG-06-2013-0067

Rubino, M., & Vitolla, F. (2014c). Internal control over financial reporting: opportunities using the COBIT framework. *Managerial Auditing Journal*, *29*(8), 736-771. https://doi.org/10.1108/MAJ-03-2014-1016

Rubino, M., Vitolla, F., & Garzoni, A. (2017a). The impact of an IT governance framework on the internal control environment. *Records Management Journal*, *27*(1), 19-41. https://doi.org/10.1108/RMJ-03-2016-0007

Rubino, M., Vitolla, F., & Garzoni, A. (2017b). How IT controls improve the control environment. *Management Research Review*, *40*(2), 218-234. https://doi.org/10.1108/MRR-04-2016-0093

Spira, L., & Page, M. (2003). Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal*, *16*(4), 640-661.

https://doi.org/10.1108/09513570310492335

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, *8*(4), 240-263. https://doi.org/10.1016/j.accinf.2007.09.001

Van Grembergen, W., & De Haes, S. (2008). *Implementing Information Technology Governance: Models, Practices, and Cases*. IGI Publishing, Hershey.

Williamson, D. (2007). The COSO ERM framework: a critique from systems theory of management control. *International Journal of Risk Assessment and Management*, *7*(8), 1089-1119. https://doi.org/10.1504/IJRAM.2007.015296

Copyrights