The impact of an IT governance framework on the internal control environment

Michele Rubino, Filippo Vitolla and Antonello Garzoni
Department of Economics and Management, University LUM Jean Monnet, Casamassima, Italy

Received 12 March 2016
Revised 3 June 2016
Accepted 20 July 2016

Abstract

Purpose – The purpose of this paper is to analyze how an IT governance framework [Control Objectives for Information and related Technology (COBIT)] influences the control environment and the internal control system. In particular, it aims to illustrate how the COBIT's structure and processes impact on the seven categories of factors that compose the control environment.

Design/methodology/approach – This paper aims to highlight how an IT governance framework with its processes enables to improve the control environment assessment and implementation.

Findings – The analysis indicates that the implementation of the COBIT framework provides some indications for managers and auditors, which must implement or assess internal control system.

Practical implications – The adoption of the framework allows managers to focus effectively on integrating, aligning and linking processes. This improves the understanding of the key aspects connected to the control environment. In addition, the adoption of the framework allows overcoming some limitations regarding the Committee of Sponsoring Organizations framework.

Originality/value – This paper addresses an area of relevance to both practitioners and academics. This analysis focuses on Accounting Information Systems themes and, through the examination of an IT governance framework, suggests solutions and tools than can help managers and auditors to address the control environment assessment.

Keywords Internal control system, COBIT 5, Control environment, COSO report, IT governance

Paper type Viewpoint

1. Introduction

The internal control continues to represent an important topic in the business world (Arwinge, 2013). Firms have a constant need to have an internal control system, as they are exposed to various risks that prevent the achievement of specific objectives (Simons, 1995; COSO, 2013). Past corporate experiences and the global financial crisis have shown the importance of the internal control and risk management system. Such events have led to the full recognition of the strategic role of the controls especially when considering the internal control system as crucial element for any organization (Collier *et al.*, 2007; Fraser and Simkins, 2010).

An effective internal control system is ensured by a clear identification and evaluation of the control environment, which represents the overall control consciousness of an entity (Zack, 2013). The control environment provides the basis on which management determines the design of the internal control system and has an influence on each of the three internal control objectives and on all activities (COSO, 1992, 2013; Moeller, 2011). It includes a set of elements such as integrity and ethical values, the attitude of top management in the field of control, the management philosophy, competence and professionalism of those working in the firm and other variables such as the allocation of powers and responsibilities as well as

Records Management Journal
Vol. 27 No. 1, 2017
pp. 19-41
© Emerald Publishing Limited
0956-5698
DOI 10.1108/RMJ-03-2016-0007

the existence of policies and procedures. These elements together define the level of the importance that the organization allocate to the controller (Beretta and Pecchiari, 2007; Graham, 2015).

Most firms use the Committee of Sponsoring Organizations (COSO) Internal Control Framework as a benchmark for assessing the effectiveness of their internal controls including their control environment. This framework helped companies to detect, as well as to prevent errors in the internal controls system but, despite the update, the new 2013 version has still some limitations (Rubino and Vitolla, 2014a). Although one of the most relevant components of the COSO framework is information and communication, it should be noted that this framework did not consider explicitly internal control concepts related to information technology (Janvrin *et al.*, 2012; Chen *et al.*, 2014; Rubino and Vitolla, 2014a). Presently, more than ever before, information technology (IT) has been recognized as a core competitive and strategic competency for most organizations (Bendoly *et al.*, 2009; Ojiako, 2012). IT became an increasingly important part of the operations within firms, which use computers to process information. Moreover, IT impacts every aspect of accounting, including financial reporting, managerial accounting, auditing and tax (Bagranoff *et al.*, 2010). Considering that most accounting systems are computerized, accountants should understand how hardware, software and human procedures turn data into decision-useful financial information and how to develop and evaluate internal controls (Simkin *et al.*, 2015). Therefore, it is necessary to understand the activity of control that information systems manage to obtain an effective evaluation of the key aspects connected to the control environment.

From this perspective, it should be recognized that every firm needs an effective IT governance which ensures that IT is efficient and effective that also meets the needs of the organization considering those relating to the internal control system (Weill and Ross, 2004; Haislip *et al.*, 2015). One of the widely accepted IT governance frameworks is represented by the Control Objectives for Information and related Technology (COBIT). This framework, now in its fifth iteration, became a tool of corporate governance focused on the governance of information systems, and it gained some significance not only in IT but also in relation to issues of accounting information systems (AIS). Larger firms, especially in the USA, adopted it to ensure an effective internal control system and to satisfy an ever growing number of statutory, regulatory and contractual requirements such as the Sarbanes Oxley Act (SOX). In this context, while the COSO framework should be considered as an overall evaluation framework for internal control, COBIT provides a useful guidance and background material in the consideration of specific controls over technology (Protiviti, 2014).

Although the growing importance that the framework is taking in IT governance studies, there has been limited research describing the benefits and the opportunities that firms could receive using the COBIT framework in the process of assessing and implementing the internal control and its control environment. Based on these motivations, the purpose of this article is to analyze how an IT governance framework such as COBIT can improve the assessment of the control environment, which is considered the foundation of all of the other components of internal control (Whittington, 2014). Understanding the COBIT-related processes may help managers and auditors to implement internal control system when applying the COSO framework, as well. This approach improves internal controls and helps organizations to better identify the key elements that constitute the control environment.

The remainder of the paper is organized as follows. Section 2 focuses on IT governance and internal control. Section 3 presents the main factors that constitute the control environment (COSO, 1992). Section 4 briefly illustrates the structure of COBIT and examines the extent of COBIT processes' impact on the control environment. Section 5 lays out the conclusions that also include the managerial implications.

2. Information technology governance and internal control

Over the past decades, IT represented a valuable asset in the management and automation of data. At the core of all firm's processes, data should be available to management to turn information into effective and timely decisions in compliance with the overall efficiency of the firm. At the same time, 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, inescapable carrier of accounting information especially in the global knowledge society (Granlund, 2011; Peslak, 2012). Therefore, taking into account that in the current environment, firms must integrate their IT with internal control activities; it can be argued that there is a strong link between internal control and IT which, being the foundation of the IT governance and compliance discipline, aims to define secure processes and organizational architectures.

IT governance is defined as the structures, processes and relational mechanisms for the IT decision-making by which organizations seek to ensure that their investment in IT facilitates strategic and tactical goals (Van Grembergen *et al.*, 2004). IT governance includes establishment of decision rights, setting of objectives and goals, building of organizational capability to meet those objectives and goals and in feedback loops that use a variety of measurement and metrics (Van Grembergen and De Haes, 2008; Wilkin and Chenhall, 2010). IT governance is a subset of broader corporate governance, focusing on the role played by information technology within the organization (Debreceny, 2013). In particular, the focus of IT governance is on IT risk management and the alignment of corporate systems to purposes of business (Ko and Fink, 2010). In essence, IT governance ensures that the processes for IT management operate in a controlled way to make it easier to achieve the expected benefits, to support the current business activities and to support the long-term success of the organization (Lomas, 2010).

The term IT governance was used for the first time by Loh and Venkatraman (1992) and Henderson and Venkatraman (1993) to describe the set of mechanisms needed to ensure the attainment of the IT capabilities needed. This term was not very significant in academic literature until the late 1990s, when Brown (1997) and Sambamurthy and Zmud (1999) began to refer to a notion of "IS governance frameworks" and then later to "IT governance frameworks" in their papers (Brown and Grant, 2005). IT governance at present concerns how the IT organization is managed and structured, and it provides mechanisms that enable the development of integrated business and IT plans; it allocates the responsibilities within the IT organization, and it prioritizes IT initiatives. It is important to ensure that the IT governance is not only designed to achieve internal efficiency in the IT organization, such as deploying good IT processes and making sure that the means and goals are documented. The final goal of good IT governance is rather to provide business enabling support (Simonsson *et al.*, 2010).

The IT governance provides structure and good practice that organizations can adopt and adapt to enhance their performance (Weill, 1992; Tippins and Sohi, 2003; Nfuka and Rusu, 2011) or to improve the reliability of financial reporting (Hirshleifer and Teoh 2003; Li *et al.*, 2012), and also to ensure compliance with applicable laws and regulations (Damianides, 2005; Sinnett, 2006; De Haes *et al.*, 2013). These elements allow to achieve the objectives of the internal control system and mitigate firms' risks (Devos *et al.*, 2012; Rubino and Vitolla, 2014b).

Over the years, IT governance became increasingly more important because it was recognized that information systems and their relevant technology influence every aspect of a firm's activities (Jaska and Hogan, 2006; Bhattacharjya and Chang, 2007; Sánchez-Rodríguez and Spraakman, 2012), and that they also create organizational value (Masli *et al.*, 2011; Tambe and Hitt, 2012). The key role of the information system and IT was also emphasized as a result of the evolution of the internal control systems, inside which IT governance is crucial. IT governance is becoming ubiquitous in nature, i.e. modern IT crossed organizational activities and became strongly aligned with business activities. Thus, IT governance can be viewed as an integral part of corporate governance and requires the senior management's attention (Ko and Fink, 2010).

IT governance becomes even more important also under SOX provisions. The Public Company Accounting Oversight Board (PCAOB) specifically states that IT control should be considered as company level control or application level, given the extensive and pervasive usage of IT in the companies' daily business processes and transactions. The key role that IT and information security play in an overall system of internal controls is highlighted by numerous studies (Gordon *et al.*, 2003; Canada *et al.*, 2009; Kuhn *et al.*, 2013). IT helps managers to perform effectively and efficiently, risk management activities (Guan and Levitan, 2012) and to evaluate IT-based control environments (Hunton *et al.*, 2004). The adoption of effective IT controls provides important benefits to the entire firm or organization (Kimiloglu *et al.*, 2012); this allows to monitor the control environment and consequently to improve the internal control system. Numerous studies and research demonstrated that the absence or the inadequacy of controls determine major deficiencies in the internal control system (Messier *et al.*, 2004; Li *et al.*, 2007; Grant *et al.*, 2008; Morris, 2011; Li *et al.*, 2012; Klamm *et al.*, 2012). The importance of IT controls came hand in hand with greater dependence of business processes on IT systems and a tendency to build into these systems' automated managerial controls (Benaroch *et al.*, 2012; El-Sayed and Youssef, 2015).

3. The control environment in the Committee of Sponsoring Organizations framework

The COSO framework, issued in 1992 and updated in 2013, is one of the models most commonly adopted by firms for assessing internal control effectiveness (Arena *et al.*, 2006; Altamuro and Beatty, 2010). This report identifies five components (control environment, risk assessment, control activities, information and communication and monitoring) designed to give reasonable assurance that the management's control objectives will be achieved. Each component includes several checks that are designed to prevent or detect errors and activities that may compromise the achievement of three categories of objectives:

(1) effectiveness and efficiency of operations;

(2) reliability of financial reporting; and

(3) compliance with applicable laws and regulations.

The first COSO's component is the control environment that can be defined as the attitude toward internal control and control consciousness both established and maintained by the management and employees of an organization. It is a product of management's governance, that is, its philosophy, style and supportive attitude, as well as the competence, ethical values, integrity and morale of the people of the organization. The control environment serves as the umbrella for the other four components (COSO, 1992). Without an effective control environment, other components hardly contribute to the creation of a suitable internal control, regardless of their quality (Schartmann, 2007; Moeller, 2011). The essence of a firm that is effectively controlled is represented by the attitude of its management. If top management believes that control is important, the other members of the organization will feel so and will respond with a conscientious respect of the controls established. Therefore, if firm's members consider that the control is not a major concern for the management, it is almost certain that objectives of management control will not be effectively pursued. The control environment consists of actions, policies and procedures that reflect the general attitude of senior management, members of the board of directors regarding internal control and its importance for the firm. To understand and assess the control environment, managers and auditors should focus on certain aspects included in the following seven categories of factors (COSO, 1992).

3.1 Ethical values and integrity

Ethical values and integrity are key elements contributing to a good control environment. They are the product of ethical and behavioral standards of the firm, as well as the way they are communicated and reinforced in practice; for example, through management's actions aiming at reducing incentives or outrageous behavior that the employees might have in engaging in illegal or unethical business. This component also includes dissemination of firms' values and standards by drafting policies, codes of conduct and exemplary actions to staff. The corporate culture plays an important role in the internal control system and gained increasing acceptance and also focused attention on the concept of corporate ethical values (Elias, 2004). In fact, there is a relationship between organizational cultures and the ways in which business and records processes are perceived and translated into practice (Foscarini, 2012).

3.2 Commitment to competence

The competence is a characteristic of people who have the skill, knowledge and capability to perform tasks. The commitment to competence involves the management's consideration of the levels of competence taking into account the specific jobs and the analysis of the way by which these levels translate into skills and knowledge.

3.3 Board of directors and audit committee

An effective board of directors must be independent from senior management. Although the board delegates the responsibility for internal control to management, the first has the burden of providing periodic independent evaluations of internal controls established by the second. An active and objective board can greatly reduce the likelihood that management bypasses existing controls. In support of its monitoring activities, the board will create an independent audit committee that assumes, among other things, the responsibility to maintain continuous communication with the external and internal auditors. An audit committee that operates effectively is a key feature in a strong corporate governance culture, which can bring significant benefits to the control environment.

3.4 Management's philosophy and operating style

The management, through its activities, provide clear signals to employees in accordance of the importance of the internal control. Some top-level managers frequently take significant risks in their new business or product ventures, while others are very cautious or conservative. These elements have a considerable influence over a firm's control environment. Internal auditors and others responsible for assessing internal controls should understand these factors and take them into consideration when evaluating the effectiveness of internal controls (Moeller, 2008).

3.5 Organizational structure

The organization structure component provides a framework for planning, executing, controlling and monitoring activities to achieve the overall objectives. This control environment factor relates to how functions are managed and organized, following a classic organization chart (Moeller, 2008). The organizational structure defines the lines of responsibility and how the existing authority is managed. By understanding the organizational structure, the auditor may capture managerial and functional items of the firm and perceive how controls are made.

3.6 Assignment of authority and responsibility

In addition to the informal aspects of the communications made by the management and the board of directors as part of daily operations, formal methods of communication, authority, responsibility and other similar issues related to control, are also important. Among these methods, it is possible to account top manager's controls and related issues, organizational and operational plans, employees' job profiles and policies.

3.7 Human resources policies and practices

The most important aspect of internal control is personnel. If employees are competent and reliable, even in the absence of other types of control, the firm could achieve good results. Incompetent or dishonest people can create a great chaos, even if several controls are set. Honest and efficient employees are able to offer a high level of performance even when there are few controls. However, even competent and trustworthy people can show personal flaws. Given the importance of the presence of competent and reliable personnel in providing effective control, it follows that the methods of recruitment, assessment, training, promotion and incentive must be considered as an important part of internal control. Therefore, the auditors use this information as a basis for assessing the attitudes and awareness of management and the board of directors of the importance of control.

Although the COSO framework considers all relevant the factors described above, it should be noted that, for applicative scopes, it has some limitations. Some studies found that the framework focuses on high-level guidance for internal controls and does not provide detailed control objectives that auditors require in the design of audit tests (Tuttle and Vandervelde, 2007; Huang *et al.*, 2011; Chang *et al.*, 2014). This limitation can be considered partially overcome with the introduction of recent updates. The updated framework, in fact, introduces the clarification of 17 principles associated with the five components, which, however, cannot be considered a novelty, as they were still implicit in the original framework. For the control environment, the updated framework takes into account the following five principles (COSO, 2013):

1. the organization demonstrates a commitment to integrity and ethical values;
2. the board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control;
3. the management establishes, with the board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives;
4. the organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with the objectives; and
5. the organization holds individuals accountable for their internal control's responsibilities in the pursuit of objectives.

These principles call attention to some critical elements included in the seven categories of factors already mentioned, which affect the control environment. For each principle, COSO provides a listing of approaches that illustrate how organizations apply the principles in designing, implementing or conducting certain aspects of internal control (COSO, 2013). Furthermore, for each approach, one or more examples are provided to illustrate how an important aspect of the approach that firms have put in place. The framework also provides 77 points of focus to enhance the rigor of understanding of each principle. Those points of focus represent important characteristics associated with the principles and, as such, provide support to the principles to which they pertain. Despite the improvements, however, the framework has still limits. First, practical approaches and examples reflect the limitations inherent in the bottom-up approaches, which are not applicable in all circumstances. Second, although the new framework reflects the increased relevance of technology, it would not be suitable to be used purely as a tool to facilitate the evaluation of the IT controls (Rubino and Vitolla, 2014a).

4. Mapping the relationship between Control Objectives for Information and related Technology processes and control environment

The COBIT framework can be considered as the most known professional standard regarding IT governance processes. Since its first publication, issued in 1996, the framework evolved significantly and changed its focus. As a simple audit tool, the framework became a tool of corporate governance focused on the governance of information systems with the latest version (COBIT 5) published in 2012. Considering the growing importance on IT in recent years, it can be argued that COBIT and IT governance frameworks became a major issue for both academics and practitioners. A growing number of companies using COBIT or decides to support this framework with other control models such as COSO especially to meet the compliance with SOX (Klamm and Watson, 2009; Kuhn *et al.*, 2013). However, COBIT can help organizations meet not only the requirements of SOX but also contributes toward compliance with other regulatory mandates, such as data privacy and security laws, and the internal control objectives (Cereola and Cereola, 2011, Mancini *et al.*, 2013). The combined use of the two frameworks, COBIT and COSO, allows the former to be able to fill the limitations provided by the latter. At the same time, COBIT relies on COSO to implement IT controls within the five components of the internal control system (Rubino and Vitolla, 2014a).

To understand how the COBIT's processes influence the control environment, it is necessary to describe preliminarily the structure and the operating logic of the framework highlighting its contribution to the control environment. The framework's structure is characterized by three levels. The first level considers business requirements for information that must be satisfied to achieve the company objectives: effectiveness, efficiency, reliability, compliance, confidentiality, integrity and availability. The second level includes resources needed for the control and administration of IT (IT resources). Such resources are defined as information, applications, infrastructure and people. Finally, there is a third level that concerns IT processes (Simonsson and Johnson, 2006; Bernroider and Ivanov, 2011). The integration of components, which makes up the three levels of the COBIT structure, enables the implementation of a set of IT controls which produce positive effects also on the control environment. The model is based on the assumption that the IT resources are managed by IT processes to achieve the IT objectives that meet the firm's information business requirements (Lainhart, 2000; ITGI, 2004). A firm should elaborate, through IT resources, all that information which corresponds to its own needs to satisfy the specific business needs (ISACA, 2012a).

Having said that, it is easily observed that the business requirements for information is a basic precondition for the operation of an internal control system and, in particular, for the component connected to the control environment. Information problems limit the effectiveness of the understanding of the control environment and represent one of the causes of failure of the internal control systems (Jensen, 1993, Romney *et al.*, 2006, Doyle *et al.*, 2007). The information plays a key role within companies, but equally important are the communication processes in relation to the control environment which allow the exchange of information, the definition of roles and responsibilities and decision-making (Huber, 1990; Sandhu *et al.*, 1996; Weidenmier and Ramamoorti, 2006). Elements such as human resources policies, personnel commitment, organizational structure, assignment of authority and responsibility and the role of the board of directors or audit committee require the presence of an effective information system that should benefit from information and communication policies that meet the seven categories as business requirements for information. If the information is not available, reliable, effective and efficient, thus, this means that the internal control system is vulnerable, and, consequently, the control environment would be difficult to understand and evaluate. Many studies and research (Allegrini and D'Onza, 2003; Ettredge *et al.*, 2006; Whitley, 2006, Hightower, 2008; Arwinge, 2013) have shown that an unclear understanding of the control environment causes an incorrect implementation of the internal control system and even an inadequate risk assessment. At the same time, it should be noted that a lack of understanding about the elements that constitute the control environment is often caused by the poor quality and availability of information, as well as of the processes through which they are managed (Kinney, 1999; Bovee *et al.*, 2003). However, the quality of the information is not sufficient for understanding the control environment in absence of suitable information flows and the resources which are necessary to manage them. In fact, COBIT provides, on the second level, the resources as information, applications, infrastructure and people, which are necessary for the IT governance. The aforementioned resources are essential for a correct assessment and understanding of the control environment, with particular reference to the components connected to human resources management, the definition of role and responsibility, organizational structure in general as well as the understanding of the role played by the board of directors (Bhatt and Grover, 2005; Nolan and McFarlan, 2005; Rubino and Vitolla, 2012). COBIT 5 is based on 37 high-level IT control objectives and on a structure that identifies three levels of IT activity: domains, processes and activities. These high-level IT control objectives identify which information criteria are important for each process and which IT resources should be managed by the processes (Hussain and Siddiqui, 2005; ITGI, 2007).

The IT control objectives are grouped into five domains that match organizational area of responsibility. The domains are grouping of IT processes and are defined as follows (ISACA, 2013): evaluate, direct and monitor (EDM); align, plan and organize (APO); build, acquire and implement (BAI); deliver, service and support (DSS); and monitor, evaluate and assess (MEA). The IT processes are placed in the domains, in line with what is generally the most relevant area of activity, at company level, when looking at IT (ISACA, 2012a; De Haes *et al.*, 2013). Each IT process is a reference or check guide that makes possible to review the processes by providing managers with a benchmark of reference to improve the reliability of financial reporting. Indeed, COBIT provides many indications for each process such as a process purpose statement, process description, IT-related goals and related metrics, outcomes, best practices to be followed, detailed activities and work products that contain the detailed inputs and outputs process descriptions (Goeken and Alter, 2009; Bernard, 2012; ISACA, 2012b). In relation to processes, another important aspect is represented by the presence, within the framework, of a process capability model. This model is used to measure the current or "as-is" maturity of an enterprise's IT-related processes, to define a required "to-be" state of maturity and to determine the gap between them and how to improve the process to achieve the desired maturity level (ISACA, 2012a; De Haes *et al.*, 2013). This approach to capability models for control over IT processes consists of developing a method of scoring so that a firm can grade itself from incomplete process (zero) to optimizing process (five). The capability level of a process is determined on the basis of the achievement of specific process attributes (Paulk *et al.*, 1995; Becker *et al.*, 2009; Simonsson *et al.*, 2010; ISACA, 2013).

With the purpose of understanding the relationship between COBIT's processes and control environment, the following paragraph provides an analysis of the individual processes of the framework showing how the same impact on the seven categories of factors that compose the control environment (Table I). The control measures provided by COBIT's processes do not necessarily have the same impact level on different factors of the control environment. The processes for which the control objective directly affects the individual category of factors are identified by the letter P (primary); the letter S (secondary) was used for the processes whose control objective only partially or indirectly affects the category of reference. To facilitate the analysis of the impact of individual processes, the control environment's components are numbered as shown in Table I.

In relation to the first domain, it is possible to identify the following processes that affect the control environment. The EDM.01 process primarily affects the sixth component and, secondarily, the fifth and seventh. This process puts in place and maintains effective enabling structures, principles, processes and practices that contribute to improve the clarity of responsibilities and authority to achieve the firm's goals and objectives. Furthermore, the process requires the development of some activities, metrics and detailed IT control objectives that improve the definition of human resources policies and procedures and assure a better functioning of the organizational structure. Another relevant process, included in this domain, is the EDM.04 that covers resources optimization. The process ensures that adequate and sufficient IT-related capabilities (people, process and technology) are available to effectively support firms' objectives at optimal cost. These elements require the development of some activities concerning the guiding principles for allocation of resources; the assignment of responsibilities for resource management; the communication of ethical values. However, also the others domain's processes provide positive contributions on control environment, as they develop activities that help spreading the ethical values and the management's philosophy and operating style (EDM.03 and EDM.05).

In the second domain (APO), it is possible to identify four processes that mainly affect the control environment. The first APO.01 process has the objective to implement and maintain mechanisms and authorities to manage information. Moreover, this process also provides a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organizational structures, roles and responsibilities, reliable and repeatable activities and skills and competencies. Therefore, considering that the process includes the development of activities aimed to establish an internal and extended organizational structure that reflects business needs and IT priorities; establish, agree on and communicate roles and responsibilities of IT personnel; communicate awareness and understanding of management objectives and direction; and maintain compliance with policies and procedures, it is possible to observe a direct influence on the fourth, fifth, sixth and seventh control environment's component. Secondarily, the process influences also the ethical value component. The APO.02 process aims to align strategic IT plans with business objectives. The process requires that it is necessary to clearly communicate the objectives and associated accountabilities so they are understood by

Table I.
COBIT 5 processes and control environment components

COBIT 5 processes		Control environment components						
		(1) Ethical values and integrity	(2) Commitment to competence	(3) Board of Directors and Audit Committee	(4) Management's philosophy and operating style	(5) Organizational structure	(6) Assignment of authority and responsibility	(7) Human resources policies and practices
Evaluate, Direct and Monitor								
EDM.01	Ensure governance framework setting and maintenance					S	P	S
EDM.02	Ensure benefits delivery							
EDM.03	Ensure risk optimization	S			S			
EDM.04	Ensure resource optimization	S			S	S	P	P
EDM.05	Ensure stakeholder transparency	S			P			
Align, Plan and Organize								
APO.01	Manage the IT management framework	S			P	P	P	P
APO.02	Manage strategy	S			P			P
APO.03	Manage enterprise architecture							
APO.04	Manage innovation							
APO.05	Manage portfolio							
APO.06	Manage budget and costs							
APO.07	Manage human resources	S	P		P	S	S	S
APO.08	Manage relationships							
APO.09	Manage service agreements							
APO.10	Manage suppliers							
APO.11	Manage quality							

(*continued*)

Table I.

COBIT 5 processes		Control environment components						
		(1) Ethical values and integrity	(2) Commitment to competence	(3) Board of Directors and Audit Committee	(4) Management's philosophy and operating style	(5) Organizational structure	(6) Assignment of authority and responsibility	(7) Human resources policies and practices
APO.12	Manage risk	P	S	P	P	S	P	P
APO.13	Manage security							
Build, Acquire and Implement								
BAI.01	Manage programs and projects							
BAI.02	Manage requirements definition							
BAI.03	Manage solutions identification and build							
BAI.04	Manage availability and capacity							
BAI.05	Manage organizational change enablement	P			P		S	S
BAI.06	Manage changes	P			P		S	S
BAI.07	Manage change acceptance and transitioning	P			P		S	S
BAI.08	Manage knowledge		P				S	S
BAI.09	Manage assets							
BAI.10	Manage configuration							

(*continued*)

Table I.

COBIT 5 processes		Control environment components						
		(1) Ethical values and integrity	(2) Commitment to competence	(3) Board of Directors and Audit Committee	(4) Management's philosophy and operating style	(5) Organizational structure	(6) Assignment of authority and responsibility	(7) Human resources policies and practices
Deliver, Service and Support								
DSS.01	Manage operations			P	S	S	P	P
DSS.02	Manage service requests and incidents							
DSS.03	Manage problems					P	S	P
DSS.04	Manage continuity		P					S
DSS.05	Manage security services							
DSS.06	Manage business process controls							
Monitor and Evaluate								
MEA.01	Monitor, evaluate and assess performance and conformance					S	S	S
MEA.02	Monitor, evaluate and assess the system of internal control	P	S	P	P	S	P	P
MEA.03	Monitor, evaluate and assess compliance with external requirements			P		S	P	P

management at any level. This process directly influences the fourth and seventh control environment's components, and secondarily the first and the sixth. Its activities are focused on communication and understanding of management philosophy, strategic firm objectives and on the procedures that the personnel should follow. Secondly, the process increases the awareness of the corporate values. Another relevant process for the control environment is the APO.07 that concerns human resources and in particular develops activities with has the following objectives: maintain adequate and appropriate staffing; identify key IT personnel; maintain the skills and competencies of personnel; identify human resources responsibilities for IT; and ensure that consultants and contract personnel comply with the firm's policies. These objectives highlight the existence of a direct influence on almost all components of the control environment with particular reference especially to commitment to competence. The aim of this process is to evaluate staffing requirements on a regular basis or on major changes to the enterprise or operational or IT environments to ensure that the firm has sufficient human resources to support its goals and objectives; and to define and manage the skills and competencies required of personnel. This process is important to regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience; and to verify that these competencies are being maintained, using qualification and certification programs where appropriate. It is necessary provide to employees, with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve the firm goals. Finally, another important process which influences the control environment is the APO.12. This process has the purpose to identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management. Risk management requires full involvement of the organizational structure. First, it is necessary to inform staff of the culture of risk in terms of ethical values and management philosophy. Then, it should establish policies and practices assigning personnel the related responsibilities. Therefore, this process impacts on all control environment's components, also affecting the board of directors and the audit committee which are responsible for defining risk tolerance.

The processes included in the third domain (BAI), which influence the control environment, are the ones that concern the change (BAI.05, BAI.06 and BAI.07) and knowledge management and staff skills (BAI.08 and BAI.04). The first involving aspects are the dissemination of corporate values and management philosophy as well as the ways in which change is managed in terms of accountability and establishment of policies and procedures. The latter, however, affect personnel with particular reference to staff training to upgrade their skills.

In the DSS domain, there are three key processes. The DSS.01, among other things, aims to maintain and perform operational procedures and operational tasks reliably and consistently; and manage the communications within the organizational structure. Therefore, the process involves the management of human resources and organizational structure. The DSS.03, identifies and classifies problems and provides timely resolution to prevent recurring incidents. This process helps to improve the organizational structure and the human resources policies and practices. Finally, there is the DSS.04 process that manages continuity ensuring a continuity plan training for all employees.

Within the last domain, the processes that most significantly influence the control environment are two. The first MEA.02 aims to monitor, evaluate and assess the system of internal control and has a direct impact on all components of the control environment. The assessment of the internal control system requires a careful evaluation of the control environment. For this reason, this process aims to monitor and propose changes to human resources policies and practices, assignment of responsibility, organizational structure, management philosophy and ethical values diffusion, communication policies of the Board and audit committee. The second process (MEA.03) ensures that the enterprise is compliant with all applicable external requirements. Therefore, it influences the control environment through the update of policies, principles, procedures and standards and through the continued demand for interaction between board of directors and top management.

The performed analysis shows that the structure of the COBIT processes guarantees a correct evaluation and a good functioning of the control environment, taking into account that the various domains ensure proper planning, execution and control of the objectives and activities related to the control environment (Hardy, 2006; Tuttle and Vandervelde, 2007). Indeed, a control environment's assessment and implementation require an in-depth understanding of a company's activities, the risks it faces and the controls it has put in place to treat risk exposure. This implies a clear comprehension of business processes, organizational structure, roles and responsibilities, ethical values and management's philosophy (Rau, 2004; Hanim Fadzil *et al.*, 2005; Hermanson *et al.*, 2012; Heise *et al.*, 2014). Furthermore, the analysis of the processes appears clear if we consider that COBIT is an IT governance framework based primarily on IT controls which positively impact on the control environment. In fact, IT controls have a direct impact, in the first place, on the hard elements of the control environment such as organizational structure, assignment of authority and responsibility and human resource policies and procedures (Bresnahan *et al.*, 2002; Raymond *et al.*, 1995; Lee *et al.*, 2010). Second, the definition of IT controls also affects soft elements such as integrity, ethical values, attitude of top management and its philosophy (Romney *et al.*, 2006; Rezaei and Griffiths, 2011).

4.1 Practical considerations for managers and auditors

The analysis performed shows that COBIT requires that managers and auditors should pay particular attention to the following key aspects when implementing the control environment or when performing its audit. First, the structure of the framework draws attention to the human resource management and related processes to:

- establish HR policies and procedures that demonstrate the commitment to integrity, ethical behavior and competence;
- assign to management and employees appropriate levels of authority and responsibility to facilitate effective control environment, including adequate limitations;
- employee recruitment and retention for key positions which should be guided by the principles of integrity and by the necessary competencies associated with the positions;
- support employees by providing access to the tools and training needed to perform their roles; and
- set the tone.

Second, the framework requires managers to:

- maintain an organizational structure that facilitates effective reporting and other communications about control environment among various functions and positions of management;
- maintain processes for objective verification of information generated from the organization's information system;

- develop a clearly articulated statement of values or ethical behaviors that should be understood by key executives and the board;
- communicate the importance of ethical values to all employees in a manner suitable for the organization; and
- evaluate the employee performance and the organization's compensation practices, including those affecting senior management.

All these elements help to improve the control environment. The implementation of the COBIT also provides to managers a few important tips such as:

- consider the local culture and values when determining the criteria for assessing business conduct and other elements of the control environment;
- pay attention to change management and the review of procedures and assignment of responsibility, and take into account the new training requirements;
- deliver to employees a copy of the organization's code of ethics and code of business conduct;
- the board should develop governance principles and included among these principles is the board's responsibility for evaluating and monitoring risks;
- ensure that communication and feedback systems within the organization are adequate;
- design the segregation of duties to reduce the opportunities for someone to perpetrate and/or conceal errors or irregularities in the normal course of their duties;
- increase the frequency of meetings between managers and employees; and
- verify the existence of an appropriate process of communication and control between governance and management.

These tips provide to managers and auditors important indications. COBIT, as noted, supports the assessment and the implementation of the control environment, as it focuses its processes on human resources management, segregation of duties and assignment of responsibilities. These aspects, often, are the main weaknesses of the internal control system (Ge and McVay, 2005; Huang, 2009; Gordon and Wilford, 2012; Boritz *et al.*, 2013; Mitra *et al.*, 2013). COBIT, as an IT governance framework, suggests metrics and best practices that improve the quality of communication and understanding of variables such as ethical values, the management's philosophy and operating style. It also stimulates the development of greater interaction between board and management. Also, these aspects are considered weaknesses of the internal control system (Brody *et al.*, 1998; Doyle *et al.*, 2007; Skaife *et al.*, 2013).

5. Conclusions

The control environment has a pervasive influence on the organization's decisions and activities and provides the foundation for the overall internal control system. If the foundation is not strong enough and the control environment is not positive either, the overall system of internal control would not be as effective as it should be. The analysis conducted in this article shows how the structure of COBIT, characterized by detailed control processes, is a valid model for implementing specific processes that can help managers and auditors to better assess and manage the components of the control environment. One of the specificities that enabled the rapid dissemination of COBIT framework in business is the fact that it is business goal-oriented, itself. Such a framework was not only designed to be used by

IT service providers and auditors but, more particularly, was designed to become a complete guide for managers. Indeed, the other existing management and IT control frameworks do not provide a complete reference on IT control to support the firm processes. This aspect allows COBIT to stand out from the other frameworks thanks to this model that is strictly connected to business objectives, even though it is mainly focused on IT. A characteristic that contributed to the dissemination and appreciation of COBIT is that this framework accepted some observations provided by the professional practice and academic studies. The use of these observations allowed to develop valid best practices that lead toward an effective control of the processes, which, in turn, ensure greater reliability in terms of data and information. Similar to what happened for COSO report, COBIT represents a model of reference that is commonly and internationally accepted with regards to IT governance and, more generally, to the overall improvement of the governance model of the informative system (Kess *et al.*, 2010).

The peculiar aspect that allows the model to drive significant improvements to control environment's components is represented by the structure of the processes. The process approaches allow to focus on integrating, aligning and linking processes effectively to achieve planned goals and objectives, and, furthermore, it facilitates the involvement and empowerment of people and the clarification of their responsibilities. The basic concept of the model is that, for IT control, it is necessary to consider the information needed to support the implementation of the firm objectives (Rau, 2004; Goeken and Alter, 2009; Debreceny, 2013).

The results of the paper provide important information for managers. First, from a general viewpoint, it should be observed that COBIT provides firms with an opportunity to implement an internal control framework that allows to overcome the COSO's limitations. In addition to the problem of establishing rules and policies, it is necessary to establish a system of verification on the adequate dissemination and application of IT governance. This system will have to define what controls and what processes are needed to ensure that the governance of the information system does not remain unrealized. In this way, it is possible to support effectively the management and implementation of the model and detect the critical areas. Therefore, a good system of internal control that starts from the fundamental component of the control environment also requires the adoption of an IT framework such as COBIT. This framework allows to address, in an adequate manner, the needs of firms in terms of IT governance, which can be understood in terms of both strategic and operational alignment. The firms' need is to adopt an approach to the internal control system that takes into account, more deeply, the government information system. The implementation or evaluation of the control environment's components takes also place within a management model of the IT processes which, at turn, provide concrete practices (De Haes *et al.*, 2013). To this aim, it is therefore necessary that each firm creates its own approach to the governance of the information system through the use of the different process framework available which depend on the strengths and specificities of the framework themselves. From this standpoint, COBIT can be also considered a valid tool due to its latest version which incorporates a ITIL framework that helps to define, in detail, how to articulate IT operations (ISACA, 2012a).

As noted in the previous section, the structure of COBIT primarily affects the human resource management and the organizational structure in general. The segregation of duties, the assignment of responsibilities and authorities, the focus on continuous improvement of staff skills and an adequate dissemination and communication of ethical values and management philosophy are the key elements to improve the control environment. However, the framework suggested has some limitations, which do not make the overall model as effective. First, it should be noted that the framework is not very much suited to interpret the managerial dynamics of small-medium companies, which often have difficulties in implementing and managing the IT governance as well as the internal control frameworks. Second, the added value can be achieved when the management is fully aware of introducing the change within its firm system by implementing new control tools that cannot be considered as merely costs because they are investments.

This paper addresses an important topic within the AIS field. AIS are often considered the instrument by default for accounting automation (Mancini *et al.*, 2013), but, in this case, the performed analysis has shown that the implementation of an IT governance framework like COBIT can produce better result in the control environment assessment and implementation. COBIT is the most widespread standard for IT governance; however its implementation is one of the most problematic aspects to control AIS and cannot be based on a simple textbook implementation. At the same time, the COSO framework has some limitations regarding the analysis of the control environment. This paper improves awareness about the use of COBIT highlighting how each process can be able to provide important contributions to the analysis of the components that constitute the control environment.

References

Allegrini, M. and D'Onza, G. (2003), "Internal auditing and risk assessment in large Italian companies: an empirical survey", *International Journal of Auditing*, Vol. 7 No. 3, pp. 191-208.

Altamuro, J. and Beatty, A. (2010), "How does internal control regulation affect financial reporting?", *Journal of Accounting and Economics*, Vol. 49 No. 1, pp. 58-74.

Arena, M., Arnaboldi, M. and Azzone, G. (2006), "Internal audit in Italian organizations: a multiple case study", *Managerial Auditing Journal*, Vol. 21 No. 3, pp. 275-292.

Arwinge, O. (2013), *Internal Control: A Study of Concept and Themes*, Springer-Verlag, New York, NY.

Bagranoff, N.A., Simkin, M.G. and Norman, C.S. (2010), *Core Concepts of Accounting Information Systems*, 11th Edition, John Wiley & Sons, Hoboken, NJ.

Becker, J., Knackstedt, R. and Pöppelbuß, D.W.I.J. (2009), "Developing maturity models for IT management", *Business & Information Systems Engineering*, Vol. 1 No. 3, pp. 213-222.

Benaroch, M., Chernobai, A. and Goldstein, J. (2012), "An internal control perspective on the market value consequences of IT operational risk events", *International Journal of Accounting Information Systems*, Vol. 13 No. 4, pp. 357-381.

Bendoly, E., Rosenzweig, E. and Stratman, J. (2009), "The efficient use of enterprise information for strategic advantage: a data envelopment analysis", *Journal of Operations Management*, Vol. 27 No. 4, pp. 310-323.

Beretta, S. and Pecchiari, N. (2007), "Analisi e valutazione del sistema di controllo interno: Metodi e tecniche", *Il Sole 24 Ore*, Milano.

Bernard, P. (2012), *COBIT® 5 – A Management Guide*, Van Haren Publishing, Zaltbommel.

Bernroider, E.W. and Ivanov, M. (2011), "IT project management control and the control objectives for IT and related Technology (CobiT) framework", *International Journal of Project Management*, Vol. 29 No. 3, pp. 325-336.

Bhatt, G.D. and Grover, V. (2005), "Types of information technology capabilities and their role in competitive advantage: an empirical study", *Journal of Management Information Systems*, Vol. 22 No. 2, pp. 253-277.

Bhattacharjya, J. and Chang, V. (2007), "Evolving IT governance practices for aligning IT with business – a case study in an Australian institution of higher education", *Journal of Information Science and Technology*, Vol. 4 No. 1, pp. 24-46.

Boritz, J.E., Hayes, L. and Lim, J.H. (2013), "A content analysis of auditors' reports on IT internal control weaknesses: the comparative advantages of an automated approach to control weakness identification", *International Journal of Accounting Information Systems*, Vol. 14 No. 2, pp. 138-163.

Bovee, M., Srivastava, R.P. and Mak, B. (2003), "A conceptual framework and belief-function approach to assessing overall information quality", *International Journal of Intelligent Systems*, Vol. 18 No. 1, pp. 51-74.

Bresnahan, T.F., Brynjolfsson, E. and Hitt, L.M. (2002), "Information technology, workplace organization and the demand for skilled labor: firm-level evidence", *The Quarterly Journal of Economics*, Vol. 117 No. 1, pp. 339-376.

Brody, R.G., Golen, S.P. and Reckers, P.M. (1998), "An empirical investigation of the interface between internal and external auditors", *Accounting and Business Research*, Vol. 28 No. 3, pp. 160-171.

Brown, A.E. and Grant, G.G. (2005), "Framing the frameworks: a review of IT governance research", *Communications of the Association for Information Systems*, Vol. 15, pp. 696-712.

Brown, C.V. (1997), "Examining the Emergence of Hybrid IS governance solutions: evidence from a single case site", *Information Systems Research*, Vol. 8 No. 1, pp. 69-94.

Canada, J., Kuhn, J.R. Jr and Sutton, S.G. (2009), "The pervasive nature of IT controls: an examination of material weaknesses in IT controls and audit fees", *International Journal of Accounting and Information Management*, Vol. 17 No. 1, pp. 106-119.

Cereola, S.J. and Cereola, R.J. (2011), "Breach of data at TJX: an instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation", *Issues In Accounting Education*, Vol. 26 No. 3, pp. 521-545.

Chang, S.I., Yen, D.C., Chang, I.C. and Jan, D. (2014), "Internal control framework for a compliant ERP system", *Information & Management*, Vol. 51 No. 2, pp. 187-205.

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*, Vol. 30 No. 7, pp. 685-689.

Chen, Y., Smith, A.L., Cao, J. and Xia, W. (2014), "Information technology capability, internal control effectiveness, and audit fees and delays", *Journal of Information Systems*, Vol. 28 No. 2, pp. 149-180.

Collier, P.M., Berry, A.J. and Burke, G.T. (2007), *Risk and Management Accounting: Best Practice Guidelines for Enterprise-Wide Internal Control Procedures*, Elsevier, Burlington, MA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), *Internal Control–Integrated Framework*, COSO, CA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), *Internal Control–Integrated Framework*, COSO, CA.

Damianides, M. (2005), "Sarbanes-Oxley and IT governance: new guidance on IT control and compliance", *Information Systems Management*, Vol. 22 No. 1, pp. 77-85.

De Haes, S., Van Grembergen, W. and Debreceny, R.S. (2013), "COBIT 5 and enterprise governance of information technology: building blocks and research opportunities", *Journal of Information Systems*, Vol. 27 No. 1, pp. 307-324.

Debreceny, R.S. (2013), "Research on IT governance, risk, and value: challenges and opportunities", *Journal of Information Systems*, Vol. 27 No. 1, pp. 129-135.

Devos, J., Van Landeghem, H. and Deschoolmeester, D. (2012), "Rethinking IT governance for SMEs", *Industrial Management & Data Systems*, Vol. 112 No. 2, pp. 206-223.

Doyle, J., Ge, W. and McVay, S. (2007), "Determinants of weaknesses in internal control over financial reporting", *Journal of Accounting and Economics*, Vol. 44 No. 1, pp. 193-223.

Elias, R.Z. (2004), "The impact of corporate ethical values on perceptions of earnings management", *Managerial Auditing Journal*, Vol. 19 No. 1, pp. 84-98.

El-Sayed, H. and Youssef, M.A.E.A. (2015), “Modes of mediation for conceptualizing how different roles for accountants are made present”, *Qualitative Research in Accounting & Management*, Vol. 12 No. 3, pp. 202-229.

Ettredge, M.L., Li, C. and Sun, L. (2006), “The impact of SOX Section 404 internal control quality assessment on audit delay in the SOX era”, *Auditing: A Journal of Practice & Theory*, Vol. 25 No. 2, pp. 1-23.

Foscarini, F. (2012), “Understanding functions: an organizational culture perspective”, *Records Management Journal*, Vol. 22 No. 1, pp. 20-36.

Fraser, J. and Simkins, B.J. (2010), *Enterprise Risk Management: Today’s Leading Research and Best Practices for Tomorrow’s Executive*, John Wiley & Sons, Hoboken, NJ.

Ge, W. and McVay, S. (2005), “The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act”, *Accounting Horizons*, Vol. 19 No. 3, pp. 137-158.

Goeken, M. and Alter, S. (2009), “Towards conceptual metamodeling of IT governance frameworks approach-use-benefits”, *Proceedings of the 42nd Hawaii International Conference on System Sciences, IEEE Computer Society, WA*, pp. 1-10.

Gordon, L.A. and Wilford, A.L. (2012), “An analysis of multiple consecutive years of material weaknesses in internal control”, *The Accounting Review*, Vol. 87 No. 6, pp. 2027-2060.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003), “Sharing information on computer systems: an economic analysis”, *Journal of Accounting & Public Policy*, Vol. 22 No. 6, pp. 461-485.

Graham, L. (2015), *Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework*, John Wiley & Sons, Hoboken, NJ.

Granlund, M. (2011), “Extending AIS research to management accounting and control issues: a research note”, *International Journal of Accounting Information Systems*, Vol. 12 No. 1, pp. 3-19.

Grant, G.H., Miller, K.C. and Alali, F. (2008), “The effect of IT controls on financial reporting”, *Managerial Audit Journal*, Vol. 23 No. 8, pp. 803-823.

Guan, J. and Levitan, A.S. (2012), “A model for investigating internal control weaknesses”, *Communications of the Association for Information Systems*, Vol. 31 No. 3, pp. 61-84.

Haislip, J.Z., Masli, A., Richardson, V.J. and Watson, M.W. (2015), “External reputational penalties for CEOs and CFOs following information technology material weaknesses”, *International Journal of Accounting Information Systems*, Vol. 17, pp. 1-15.

Hanim Fadzil, F., Haron, H. and Jantan, M. (2005), “Internal auditing practices and internal control system”, *Managerial Auditing Journal*, Vol. 20 No. 8, pp. 844-866.

Hardy, G. (2006), “Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges”, *Information Security Technical Report*, Vol. 11 No. 1, pp. 55-61.

Heise, D., Strecker, S. and Frank, U. (2014), “ControlML: a domain-specific modeling language in support of assessing internal controls and the internal control system”, *International Journal of Accounting Information Systems*, Vol. 15 No. 3, pp. 224-245.

Henderson, J.C. and Venkatraman, N. (1993), “Strategic alignment: leveraging information technology for transforming organizations”, *IBM Systems Journal*, Vol. 32 No. 1, pp. 4-16.

Hermanson, D.R., Smith, J.L. and Stephens, N.M. (2012), “How effective are organizations’ internal controls? Insights into specific internal control elements”, *Current Issues in Auditing*, Vol. 6 No. 1, pp. A31-A50.

Hightower, R. (2008), *Internal Controls Policies and Procedures*, John Wiley & Sons, Hoboken, NJ.

Hirshleifer, D. and Teoh, S.H. (2003), “Limited attention, information disclosure, and financial reporting”, *Journal of Accounting and Economics*, Vol. 36 No. 1, pp. 337-386.

Huang, H.W. (2009), “Sarbanes-Oxley Section 404 compliance. Recent changes in US-traded foreign firms’ internal control reporting”, *Managerial Auditing Journal*, Vol. 24 No. 6, pp. 584-598.

Huang, S.M., Hung, W.H., Yen, D.C., Chang, I.C. and Jiang, D. (2011), "Building the evaluation model of the IT general control for CPAs under enterprise risk management", *Decision Support Systems*, Vol. 50 No. 4, pp. 692-701.

Huber, G.P. (1990), "A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making", *Academy of Management Review*, Vol. 15 No. 1, pp. 47-71.

Hunton, J.E., Wright, A.M. and Wright, S. (2004), "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?", *Journal of Information Systems*, Vol. 18 No. 2, pp. 7-28.

Hussain, S.J. and Siddiqui, M.S. (2005), "Quantified model of COBIT for corporate IT governance", *Proceeding of First International Conference on Information and Communication Technologies, ICICT, Novosibirsk*, pp. 158-163.

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

Information Systems Audit and Control Association (ISACA) (2012b), *Cobit 5 – Enabling Processes*, ISACA, Rolling Meadows, IL.

Information Systems Audit and Control Association (ISACA) (2013), *Process Assessment Model (PAM): Using COBIT*, ISACA, Rolling Meadows, IL.

IT Governance Institute (ITGI) (2004), *IT Control Objectives for Sarbanes–Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting*, IT Governance Institute, Rolling Meadows, IL.

IT Governance Institute (ITGI) (2007), *Cobit 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models*, IT Governance Institute, Rolling Meadows, IL.

Janvrin, D.J., Payne, E.A., Byrnes, P., Schneider, G.P. and Curtis, M.B. (2012), "The updated COSO internal control-integrated framework: recommendations and opportunities for future research", *Journal of Information Systems*, Vol. 26 No. 2, pp. 189-213.

Jaska, P.V. and Hogan, P.T. (2006), "Effective management of the information technology function", *Management Research News*, Vol. 29 No. 8, pp. 464-470.

Jensen, M.C. (1993), "The modern industrial revolution, exit, and the failure of internal control systems", *The Journal of Finance*, Vol. 8 No. 3, pp. 831-880.

Kess, P., Law, K.M., Kanchana, R. and Phusavat, K. (2010), "Critical factors for an effective business value chain", *Industrial Management & Data Systems*, Vol. 110 No. 1, pp. 63-77.

Kimiloglu, H., Ozturan, M. and Sencer Erdem, A. (2012), "Collaborative research: opinions and information technology utilization potential", *Management Research Review*, Vol. 35 No. 12, pp. 1134-1152.

Kinney, W.R. (1999), *Information Quality Assurance and Internal Control for Management Decision Making*, McGraw-Hill Professional, New York, NY.

Klamm, B.K. and Watson, M.W. (2009), "SOX 404 reported internal control weakness: a test of COSO framework components and information technology", *Journal of Information Systems*, Vol. 23 No. 2, pp. 1-23.

Klamm, B.K., Kobelsky, K.W. and Weidenmier, M. (2012), "Determinants of the persistence of internal control weaknesses", *Accounting Horizons*, Vol. 26 No. 2, pp. 307-333.

Ko, D. and Fink, D. (2010), "Information technology governance: an evaluation of the theory-practice gap", *Corporate Governance*, Vol. 10 No. 5, pp. 662-674.

Kuhn, J.R., Ahuja, M. and Mueller (2013), "An examination of the relationship of IT control weakness to company financial performance and health", *International Journal of Accounting and Information Management*, Vol. 21 No. 3, pp. 227-240.

Lainhart, J.W. IV (2000), "COBIT™: a methodology for managing and controlling information and information technology risks and vulnerabilities", *Journal of Information Systems*, Vol. 14 No. 1, pp. 21-25.

Lee, D., Lee, S.M., Olson, D.L. and Hwan Chung, S. (2010), "The effect of organizational support on ERP implementation", *Industrial Management & Data Systems*, Vol. 110 No. 2, pp. 269-283.

Li, C., Lim, J.H. and Wang, Q. (2007), "Internal and external influences on IT control governance", *International Journal of Accounting Information Systems*, Vol. 8 No. 4, pp. 225-239.

Li, C., Peters, G.F., Richardson, V.J. and Watson, M. (2012), "The consequences of information technology control weaknesses on management information systems: the case of Sarbanes–Oxley internal control reports", *MIS Quarterly*, Vol. 36 No. 1, pp. 179-203.

Liew, A. (2015), "The use of technology-structured management controls: changes in senior management's decision-making behaviours", *International Journal of Accounting Information Systems*, Vol. 17 No. 1, pp. 37-64.

Loh, L. and Venkatraman, N. (1992), "Diffusion of information technology outsourcing: influence sources and the Kodak effect", *Information Systems Research*, Vol. 3 No. 4, pp. 334-359.

Lomas, E. (2010), "Information governance: information security and access within a UK context", *Records Management Journal*, Vol. 20 No. 2, pp. 182-198.

Mancini, D., Vaassen, E.H. and Dameri, R.P. (2013), "Trends in accounting information systems", in Mancini, D., Vaassen, E.H. and Dameri, R.P. (Eds), *Accounting Information Systems for Decision Making*, Springer, Berlin Heidelberg, pp. 1-11.

Masli, A., Richardson, V.J., Sanchez, J.M. and Smith, R.E. (2011), "The business value of IT: a synthesis and framework of archival research", *Journal of Information Systems*, Vol. 25 No. 2, pp. 81-116.

Messier, W.F., Eilifsen, A. and Austen, L.A. (2004), "Auditor detected misstatements and the effect of information technology", *International Journal of Auditing*, Vol. 8 No. 3, pp. 223-235.

Mitra, S., Jaggi, B. and Hossain, M. (2013), "Internal control weaknesses and accounting conservatism: evidence from the post–Sarbanes–Oxley period", *Journal of Accounting, Auditing & Finance*, Vol. 28 No. 2, pp. 152-191.

Moeller, R.R. (2008), *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL*, John Wiley & Sons, Hoboken, NJ.

Moeller, R.R. (2011), *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*, John Wiley & Sons, Hoboken, NJ.

Morris, J.J. (2011), "The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting", *Journal of Information Systems*, Vol. 25 No. 1, pp. 129-157.

Nfuka, E.N. and Rusu, L. (2011), "The effect of critical success factors on IT governance performance", *Industrial Management & Data Systems*, Vol. 111 No. 9, pp. 1418-1448.

Nolan, R. and McFarlan, F.W. (2005), "Information technology and the board of directors", *Harvard Business Review*, Vol. 83 No. 10, pp. 1-11.

Ojiako, U. (2012), "Using IS/IT to enhance service delivery", *Industrial Management & Data Systems*, Vol. 112 No. 4, pp. 584-599.

Paulk, M.C., Weber, C.V., Curtis, B. and Chrissis, M.B. (1995), *The Capability Maturity Model: Guidelines for Improving the Software Process*, Addison Wesley, Reading, MA.

Peslak, A.R. (2012), "An analysis of critical information technology issues facing organizations", *Industrial Management & Data Systems*, Vol. 112 No. 5, pp. 808-827.

Protiviti (2014), *The Updated COSO Internal Control Framework. Frequently Asked Questions*, 3rd ed., Protoviti, available at: www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Third-Edition-Protiviti.pdf (accessed 20 May 2016).

Rau, K.G. (2004), "Effective governance of IT: design objectives, roles, and relationships", *Information Systems Management*, Vol. 21 No. 4, pp. 35-42.

Raymond, L., Pare, G. and Bergeron, F. (1995), "Matching information technology and organizational structure: an empirical study with implications for performance", *European Journal of Information Systems*, Vol. 4, pp. 3-16.

Rezaei, N. and Griffiths, G. (2011), "Organizational control environment and Cobit's it control process implementation", in Krishnamurthy, S. (Eds), *Proceedings of the IADIS International Conference e-Commerce*, *IADIS Press, Rome*, *21-23 July*, pp. 121-128.

Romney, M.B., Steinbart, P.J., Zhang, R. and Xu, G. (2006), *Accounting Information Systems*, Pearson Education, New York, NY.

Rubino, M. and Vitolla, F. (2012), "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*, Access Press, Darwen, pp. 314-327.

Rubino, M. and Vitolla, F. (2014a), "Internal control over financial reporting: opportunities using the COBIT framework", *Managerial Auditing Journal*, Vol. 29 No. 8, pp. 736-771.

Rubino, M. and Vitolla, F. (2014b), "Corporate governance and the information system: how a framework for IT governance supports ERM", *Corporate Governance*, Vol. 14 No. 3, pp. 320-338.

Sambamurthy, V. and Zmud, R.W. (1999), "Arrangements for information technology governance: a theory of multiple contingencies", *MIS Quarterly*, Vol. 23 No. 2, pp. 261-290.

Sánchez-Rodríguez, C. and Spraakman, G. (2012), "ERP systems and management accounting: a multiple case study", *Qualitative Research in Accounting & Management*, Vol. 9 No. 4, pp. 398-414.

Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996), "Role-based access control models", *IEEE Computer*, Vol. 29 No. 2, pp. 38-47.

Schartmann, B. (2007), *The Role of Internal Audit in Corporate Governance in Europe: Current Status, Necessary Improvements, Future Tasks*, Erich Schmidt Verlag GmbH & Co KG, Berlin.

Simkin, M.G., Norman, C.S. and Rose, J.M. (2015), *Core Concepts of Accounting Information Systems*, 13th Edition, John Wiley & Sons, Hoboken, NJ.

Simons, R. (1995), *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*, Harvard Business School Press, Boston.

Simonsson, M. and Johnson, P. (2006), "Assessment of IT governance-a prioritization of cobit", *Proceedings of the Conference on Systems Engineering Research, Los Angeles, April*, pp. 1-10.

Simonsson, M., Johnson, P. and Ekstedt, M. (2010), "The effect of IT governance maturity on IT governance performance", *Information Systems Management*, Vol. 27 No. 1, pp. 10-24.

Sinnett, W. (2006), *Managing Governance, Risk and Compliance with Enterprise Content Management*, Financial Executives Research Foundation, MA.

Skaife, H.A., Veenman, D. and Wangerin, D. (2013), "Internal control over financial reporting and managerial rent extraction: evidence from the profitability of insider trading", *Journal of Accounting and Economics*, Vol. 55 No. 1, pp. 91-110.

Tambe, P. and Hitt, L.M. (2012), "The productivity of information technology investments: new evidence from IT labor data", *Information Systems Research*, Vol. 23 No. 3, pp. 599-617.

Tippins, M.J. and Sohi, R.S. (2003), "IT competency and firm performance: is organizational learning a missing link?", *Strategic Management Journal*, Vol. 24 No. 8, pp. 745-761.

Tuttle, B. and Vandervelde, S.D. (2007), "An empirical examination of CobiT as an internal control framework for information technology", *International Journal of Accounting Information Systems*, Vol. 8 No. 4, pp. 240-263.

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

Van Grembergen, W., De Haes, S. and Guldentops, E. (2004), "Structures, processes and relational mechanisms for IT governance", in Van Grembergen, W. (Eds), *Strategies for Information Technology Governance*, Idea Group Publishing, Hershey.

Weidenmier, M.L. and Ramamoorti, S. (2006), "Research opportunities in information technology and internal auditing", *Journal of Information Systems*, Vol. 20 No. 1, pp. 205-219.

Weill, P. (1992), "The relationship between investment in information technology and firm performance: a study of the valve manufacturing sector", *Information Systems Research*, Vol. 3 No. 4, pp. 307-333.

Weill, P. and Ross, J.W. (2004), *IT Governance. How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston, MA.

Whitley, J. (2006), "COSO to develop further internal control guidance", *Internal Auditor*, Vol. 18.

Whittington, O.R. (2014), *Wiley CPAexcel Exam Review Spring 2014 Study Guide: Business Environment and concepts*, John Wiley & Sons, Hoboken, NJ.

Wilkin, C.L. and Chenhall, R.H. (2010), "A review of IT governance: a taxonomy to inform accounting information systems", *Journal of Information Systems*, Vol. 24 No. 2, pp. 107-146.

Zack, G.M. (2013), *Financial Statement Fraud: Strategies for Detection and Investigation*, John Wiley & Sons, Hoboken, NJ.

About the authors

Michele Rubino is an Assistant Professor at LUM Jean Monnet University, Casamassima (Bari, Italy). He obtained his PhD in Business Administration and Management at University of Bari – Italy, in 2009. Since 2007, he is the Deputy Director of the Master in Entrepreneurship and Management Consulting, and a Professor of Accounting and Corporate Governance and Internal Control at the School of Management of the same University. He is also an ISACA (Information Systems Audit and Control Association) Academic Advocate. He published several papers and books. His current research interests are in the field of the internal control, accounting information systems, corporate social responsibility and SMEs. Michele Rubino is the corresponding author and can be contacted at: rubino@lum.it

Filippo Vitolla is an Associate Professor of Business Administration at LUM Jean Monnet University, Casamassima (BA) – Italy. He obtained, on April 2005, PhD in Business Administration and Management at University of Bari – Italy. Since November 2004, he has also been an Assistant Professor of Management Control, Cost Analysis and Business Strategy for the degree course in Business Administration and also in the Master's course provided at the School of Management. His research areas are corporate social responsibility, management control systems, strategic management and risk management. In 2012, he passed the National Qualification for Associate Professor in Business Administration. He published several papers and books.

Antonello Garzoni is a Full Professor of "Strategic Management" and "International Strategies" at LUM Jean Monnet University, Casamassima (Bari, Italy), where he currently is the Vice-Rector for international cooperation. From 2009 to 2011, he has been the Dean of the Faculty of Economics. He graduated in Business Administration at Bocconi University in 1993, and obtained PhD in Business Administration and Management at Bocconi University, Milan in 1999. He is a Professor of "Strategic Management" at Bocconi University, Milano, where he teaches in undergraduate, graduate and executive education courses. He currently is an Academic co-Director of Global Advanced Management Program from Georgetown University-Esade-Sda Bocconi alliance. His research interests are in the field of strategic management accounting and corporate performance measurement, competitive intelligence, resource-based view of the firm and corporate governance.

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**