The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0268-6902.htm

Internal control over financial reporting: opportunities using the COBIT framework

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

Abstract

Purpose – The purpose of this paper is to analyze how the COBIT framework, integrated within the internal control framework, enables improvement in the quality of financial reporting while helping to reduce or eliminate the material weaknesses (MWs) of internal control over financial reporting (ICFR). The Control Objectives for Information and Related Technology (COBIT) model is a framework for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. Preliminarily, the analysis in this paper illustrates how the Committee of Sponsoring Organizations (COSO) framework impacts on the MWs, highlighting strengths and weaknesses. This paper shows how these limits can be overcome with the use of the COBIT framework.

Design/methodology/approach – This is a conceptual paper that aims to highlight the relationship between COBIT and COSO, by illustrating how the IT processes reduce or eliminate the main MW categories.

Findings – The analysis indicates that the implementation of the COBIT framework, or more generally the adoption of effective IT controls, provides important benefits to the entire company or organization. IT control objectives have a direct impact on the IT control weaknesses and indirectly on the other categories of material weaknesses.

Practical implications – The adoption of the framework allows managers to implement effective ICFR. In particular, the COBIT approach provides managers with a more evolved tool in terms of compliance with the Sarbanes–Oxley Act requirements. This framework also improves the reliability of financial reporting in relation to the requirements of Public Company Accounting Oversight Board's Auditing Standards No. 2 and 5.

Originality/value – The analysis provides an interdisciplinary approach, connecting accounting and information systems themes, and suggest solutions and tools than can help managers to address the internal control weaknesses. This paper addresses an area of relevance to both practitioners and academics and expands existing accounting literature.

Keywords Financial reporting, COBIT 5 framework, SOX, COSO framework, IT controls, Material weaknesses

Paper type Conceptual paper

Introduction

The internal control system represents an increasingly important corporate governance mechanism that supports operations, lays the foundations for successful business strategies and corporate performance (Simons, 1995; Sarens and De Beelde, 2006; Naciri, 2010; Arwinge, 2013). The internal control system aims, amongst other things, to provide reasonable assurance in terms of the achievement of an adequate level of

Managerial Auditing Journal
Vol. 29 No. 8, 2014
pp. 736-771

0268-6902
DOI 10.1108/MAJ-03-2014-1016

financial reporting's reliability and capacity for drafting financial statements (COSO, 1992, 2013). From this standpoint, against the numerous corporate scandals occurring over the past 30 years, the issue of corporate control has become increasingly relevant, and since 2002, many countries have adopted a set of laws and regulations aimed at improving the reliability of financial reporting (Rose *et al.*, 2013).

One of the internationally recognized example of these regulations is the American Sarbanes–Oxley Act (SOX). This was followed in other countries, such as the Directive of the European Parliament 2006/43/CE, the Company Acts in Australia and the UK and the Italian law No. 262/2005 on savings. The financial reporting issue was particularly examined within SOX, especially as far as the provisions of Sections 302, 404 and 906 are concerned. Under Section 404, companies should identify, report and find solutions to any weaknesses in the control system, allowing remediation prior to year-end (Grant *et al.*, 2008). The identified control weaknesses which remain as unremediated at year-end and which meet criteria for material weakness, must then be disclosed to the financial markets in the 10-K statement as required by Section 404 (SEC, 2002; Arnold *et al.*, 2011). Thus, it is important to assess the analysis of these material weaknesses (MWs) and to improve the financial reporting process.

The provisions of SOX mainly require management to assert its responsibility to establish and maintain adequate internal control systems for financial reporting and to provide an effective assessment of such internal controls by indicating the framework used to carry out such evaluations (SEC, 2002; Li *et al.*, 2007). These provisions also require external auditors to attest and report on the assessment made by the management. That being said, it should be noted that the most frequently used framework is the Committee of Sponsoring Organizations (COSO) framework, which is a highly abstract conceptual framework that does not identify control objectives at a level of specificity sufficient to design detailed audit tests (Tuttle and Vandervelde, 2007; Huang *et al.*, 2011; Chang *et al.*, 2014). Therefore, its use does not achieve optimal levels of effectiveness in terms the reliability of financial reporting in respect of identified MWs. However, the inadequacy of the COSO framework can be countered through the use of other types of control frameworks. As companies largely depend on information technology (IT)-based information systems, it is possible for them to have access and be able to manage information to conduct appropriate internal control over the financial reporting system that includes controls either on the accounting and management processes, as well as on the IT infrastructures (Stoel and Muhanna, 2011).

The SOX internal control requirements directly integrate and reflect the importance of information quality on decision-making (Li *et al.*, 2012). The quality of the information, produced by the financial reporting function which uses the management information system, is particularly germane, as it represents core data used by managerial decision-makers (Krishnan, 2005). Given the increasing use of complex IT, such as enterprise resource management systems, the assessment of internal control effectiveness requires an opportune and adequate level of knowledge about IT audit techniques (Abdolmohammadi and Boss, 2010). Gelinas *et al.* (2008) assert that SOX has increased the importance of accounting information system-related knowledge for external auditors. The importance of the IT controls grows with business processes' reliance on information systems and with the tendency to integrate them with automated management control systems (Benaroch *et al.*, 2012). Indeed, those studies that have analyzed MWs, carried out in compliance with SOX, support the fact that

many of the financial reporting errors were due to the ineffectiveness resulting from IT controls (Messier *et al.*, 2004). In this context, it is clear that IT controls have a great influence on the reliability of financial reporting. The growing importance of information systems has stimulated the proposition and development of a vast number of resources to support management guidance on the operational level. Amongst these, the Control Objectives for Information and Related Technology (COBIT) model is particularly important as a generally accepted framework that allows companies to achieve their governance and management objectives. COBIT is a worldwide accepted set of guidelines and supporting IT tools used to support corporate governance. Auditors and managers use it as a mechanism to integrate technology in implementing controls and meet specific business objectives. This framework is well suited to companies focused on risk management and mitigation (Bernard, 2012).

The objective of this paper is to analyze how the COBIT framework, integrated within the internal control framework, improves the quality of financial reporting, while helping to reduce or eliminate the weaknesses of internal control over financial reporting (ICFR). Preliminarily, the analysis illustrates how the COSO framework impacts on the MWs, highlighting strengths and weaknesses. The paper then shows how these limits can be overcome with the use of COBIT, which represents a complementary framework for the reliability of financial reporting focused on IT governance. This work contributes to expand existing accounting literature in this area. Despite the significance of the issue of ICFR weaknesses, most of the studies and researches, which integrate different approaches connected to the accounting and information system themes, have lacked in suggesting any proper solutions or tools able to face the problem of the MWs observed (Power, 2009; Janvrin *et al.*, 2012).

The remainder of the paper is organized as follows. The second section provides a background of the literature taken from the studies that have dealt with the weaknesses related to internal financial reporting control. Prior studies identify the main significant deficiency or material weakness disclosed by companies. The third section examines how the COSO framework impacts on the objective of the reliability of financial reporting, highlighting the strengths and weaknesses of this framework. The fourth illustrates the COBIT structure and its attributes and the relationship with financial reporting. The fifth section emphasizes the relationship between COBIT and COSO by illustrating how the IT processes enable reduction or elimination of the main MW categories. The paper ends with final conclusions and also provides managerial implications and insights for future research.

Material weaknesses: a literature review

Since 2002, SOX provisions have contributed to the development of numerous studies that have examined various issues related to MWs. The MWs literature comes from the analysis of companies based in the USA, whereas it is only in this context that managers are obliged to publicly disclose the weaknesses that affect their companies (Brown *et al.*, 2014). The following paragraph illustrates some empirical studies that have identified the main types of MWs disclosed by companies, performing also a classification of the same, as reported in Table I.

Ge and McVay (2005) show that poor internal control is usually related to an insufficient commitment of resources for accounting controls. Raghunandan and Rama (2006) examine the association between the audit fees and the internal control

Table I.
Material weaknesses identified by prior research

Authors	Identified material weaknesses
Ge and McVay (2005)	They identify 493 weaknesses that were classified into nine categories represented in a decreasing order of importance: Account specific Training Period-End/accounting policies Revenue recognition Segregation of duties Account reconciliation Subsidiary specific Senior management Technology issues
Raghunandan and Rama (2006)	They identify the following MWs disclosed by companies: Quality and training of accounting personnel Reconciliation of accounts, financial statement preparation Segregation of duties Information systems related problems Quality of internal audit and/or audit committee
Doyle *et al.* (2007a)	They suggest two types of classification for material weaknesses. The first makes a distinction between: Account-specific or transaction-level MWs, mainly due to inadequate internal accounting controls in terms of lost contingencies, including bad debts, deficiencies in the documentation of a receivables securitization program, no adequate internal controls over the application of new accounting principles or over the application of existing accounting principles to new transactions Company-level MWs, also due to an override by senior management and an ineffective control environment The second classification identifies three categories of weaknesses: Staff, or inadequate qualified staff and resources, leading to the untimely identification and resolution of certain accounting and disclosure matters as well as failure to perform timely and effective reviews, the need to increase the training of the financial staff and weak internal controls and procedures relating to the separation of duties

(*continued*)

Table I.

Authors	Identified material weaknesses
	Complexity, characterized by inconsistencies in the application of company policies among business units and segments or material weaknesses in the interpretation and application of complex accounting standards, such as those standards related to hedge transactions General, which includes three types of weaknesses such as weak internal controls related to contracting practices; deficiencies related to the design of policies and execution of processes related to accounting for transactions and deficiencies in the period-end reporting process
Grant *et al.* (2008)	They identify, in descending order of importance, the main deficiencies reported by companies: Accounting documentation policy and/or procedures Material and/or numerous auditor year-end adjustments Accounting personnel resources (competency, training) Restatement or non-reliance of company filings Untimely or inadequate account reconciliations Information technology (software, security, access issues) Non-routine transactions control issues Segregation of duties, design of controls; (l) *Journal Entry Control Issues*; (m) Senior management (competency, tone, and reliability issues); (n) Ethical or compliance issues with personnel
Huang (2009)	The main MWs which have been identified are: Problems in specific types of transactions or accounts only Quality of accounting personnel Segregation of duties Year-end adjustment problems Information system related problems Quality of internal auditor and/or audit committee

(*continued*)

Authors	Identified material weaknesses
Calderon *et al.* (2012)	They shows a ranking of the top ten types of MWs, over the 2004-2010 period: Accounting documentation, policy, or procedures Material or numerous auditor/year-end adjustments Accounting personnel resources and competency/training Restatement of or nonreliance on company filings Untimely or inadequate account reconciliations Inadequate disclosure controls Information technology, software and security and access Nonroutine transaction control issues Restatement of previous SOX section 404 disclosures Segregation of duties and design of controls and journal entry control issues
Gordon and Wilford (2012)	They illustrate that the main MWs, that companies report in multiple consecutive years, are: Accounting documentation, policy and/or procedure Accounting personnel resources, competency and training Information technology, software, security and access issues Segregations of duties/design of controls Material and/or numerous auditor/year-end adjustments Untimely or inadequate account reconciliations; (g) Restatement or non-reliance of company filings
Boritz *et al.* (2013)	They identify the following 14 categories of IT weaknesses in order of decreasing frequency of occurrence: access monitoring design issues change and development end-user computing segregation of incompatible functions policies documentation master files

(*continued*)

Table I.

Table I.

Authors	Identified material weaknesses
	backup staffing sufficiency and competency security (other than over access) outsourcing operations
Mitra *et al.* (2013)	They classify internal control weaknesses, reported under SOX 404, into company-level and account specific weaknesses. Examples of company-level weaknesses are as follows: Quality and training of accounting personnel Segregation of duties Reconciliation of accounts and financial statement preparation Information systems-related problems Quality of internal audit or audit committee Inconsistencies in the application of company policies among business units and segments Material weaknesses in the interpretation and application of complex accounting standards, such as standards related to hedge transactions Weak internal controls related to contracting parties Deficiencies related to the design of policies and execution of processes relating to accounting for transactions Deficiencies in the period-end reporting process Account-specific ICW relate to specific accounts or transactions, namely: Inadequate controls for income tax accounting including deferred income taxes with proper reconciliations between book and tax income Inadequate controls for accounting for loss contingencies Inadequate controls for accounting for receivables including bad debts Revenue recognition problems Deficiencies in the documentation of a receivables securitization program Inadequate internal controls over the application of new accounting principles or existing accounting principles to new transactions

disclosures made pursuant to section 404. They find that audit fees are much higher for companies showing material weakness disclosure than for those without such a disclosure. Their research also shows that the relationship between audit fees and the presence of a material weakness disclosure does not vary, depending on the type of material weakness. Doyle *et al.* (2007a) examine the determinants of weaknesses in internal control for 779 firms disclosing material weaknesses. They illustrate that firms with more serious entity-wide control problems are smaller, younger and weaker financially, while firms with less severe, account-specific problems are financially healthy but have complex, diversified and rapidly changing operations. Grant *et al.* (2008) examine 278 companies reporting IT control deficiencies in the first three years of the SOX 404 requirements. Using quantitative analysis, they reveal that companies with IT deficiencies report more significant accounting errors than companies which do not. Huang (2009) investigates recent changes in US-traded foreign companies' internal control reporting and contributes to the intense debate about the costs and benefits of SOX 404. The empirical evidence shows that both US firms and US-traded foreign companies from developed countries experienced a similar statistically significant descending trend in MWs reported from 2004 to 2006. In other research, Calderon *et al.* (2012) analyze the MWs reported by companies from 2004 to 2010, showing how the same have decreased over the years. Gordon and Wilford (2012) empirically re-examine the relation between MWs and cost of equity. The findings provide evidence that reporting material weakness in multiple consecutive years, lacking any remediation, has a significantly negative impact on the cost of equity. Boritz *et al.* (2013), by using an automated content analysis approach, provided a snapshot of the terminology that auditors actually use to describe IT weaknesses (ITWs). Using the dictionary with a content analysis software led to the identification of 14 categories of ITWs. Finally, Mitra *et al.* (2013) examine the relationship between accounting conservatism and internal control weaknesses (ICW) in the post-SOX period. The analysis shows that the firms having ICW, especially the firms with company-level ICW, have significantly changed their conservative reporting practice from the *ex ante* to the post-SOX period.

The internal control framework and financial reporting

Internal control systems have long been recognized as important in ensuring high-quality financial reporting (Kinney, 2000; Felo *et al.*, 2003; Altamuro and Beatty, 2010; Johnstone *et al.*, 2011; Brown *et al.*, 2014). In this context, the most widely used framework is referred to as COSO (Gupta, 2007) which has also become the main framework for the ICFR compliance as a result of regulations introduced by SOX (Klamm and Watson, 2009; Martin *et al.*, 2014). The COSO framework was introduced in 1992 and has been recently revised in 2013. The updated framework does not change the definition for internal control and its three categories of objectives:

(1) effectiveness and efficiency of operations;

(2) reliability of financial reporting; and

(3) compliance with applicable laws and regulations.

These three objectives directly relate to five integrated components:

(1) control environment;

(2) risk assessment;

(3) control activities;
(4) information and communication; and
(5) monitoring activities.

Each of the five components of internal control set forth in the framework is important for achieving the objective of reliability of financial reporting. The five COSO components work together to prevent or detect and to correct material misstatements of financial reports. When the five components are present and are all functioning, to the extent that management is reasonably assured due to the fact that financial statements are being prepared reliably, internal control can be considered effective (COSO, 2013).

The revised framework has included enhancements and clarifications designed to guide users in applying it and has codified principles that support the five components of internal control. While the 1992 version implicitly reflected the core principles of internal control, the updated version explicitly stated 17 principles representing fundamental concepts associated with the five components of internal control (Protoviti, 2014). The framework has also provided 77 points of focus to enhance the rigor of understanding of each principle. Points of focus represent important characteristics associated with the principles and, as such, provide support to the principles to which they pertain. Furthermore, the COSO board has developed an Internal Control over External Financial Reporting Compendium (ICEFR compendium) to assist users of the framework who are responsible for designing, implementing and conducting a system of internal control over external financial reporting. The ICEFR compendium provides practical approaches and examples that illustrate how companies may apply the principles set forth in the framework when preparing financial statements and other external financial reporting for an entity and subunits. The structure of the framework, taking into account the improvements made by the recent upgrade, provides guidelines for assessing effective control system attributes. The framework provides managers and auditors with the necessary tools they need to identify and assess the internal control deficiencies. These deficiencies may have the potential to adversely affect the ability of the entity to achieve the reliability of financial reporting. For each component, the framework, through the finding of appropriate principles, points of focus, example and approaches, helps management with establishing and maintaining effective ICFR.

The control environment is the set of standards, processes and structures that provide the basis for carrying out internal control across the organization. The theoretical basis of COSO is a strong control environment that represents the foundation for the effectiveness of the other components, as shown also by Klamm and Watson (2009). For this component, which is associated with five principles (Principles 1 to 5), the framework aims to raise awareness of the entire organization for the following critical aspects. According to COSO, it appears relevant to evaluate both the top management's integrity and ethical values, as well as the management's philosophy and its operating style. In addition, it is necessary to take into account the organizational structure, the financial reporting competencies and related oversight roles, the adequacy of the levels of authority and responsibility assigned to the staff. Senior management should prepare organizational charts to document, communicate and enforce accountability for the achievement of the entity's financial reporting objectives. This requires assignment of authority and responsibility. Furthermore, senior management should seek to align roles and responsibilities with the financial reporting objective,

establishing policies and practices. The organization should demonstrate a commitment to attract, develop and retain competent individuals to align with the objectives. In this context, the board of directors and management must evaluate competence across the organization and in the outsourced service providers in relation to established policies and practices and must act as necessary to address shortcomings. At the same time, the implementation of training courses for staff should not be overlooked.

In the component which relates to risk assessment, the framework provides management with the information necessary for identifying and assessing risks concerning the reliability of financial reporting. Risks to the achievement of this objective from across the entity are considered relative to established risk tolerances. The risk assessment activities involves identification and analysis of the risks of material misstatement. Establishment of financial reporting objectives articulated by a set of financial statement assertions for significant accounts is a precondition to the risk assessment process. The COSO recognizes that a company must first have in place an appropriate set of financial reporting objectives. At a high level, the objective of financial reporting is to prepare reliable financial statements, which involves attaining reasonable assurance that the financial statements are free from material misstatement. Consequently, the management must specify the financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting (COSO; 2013). These risks must be subsequently analyzed and managed. In fact, when an organization determines that an internal control deficiency exists and is severe, management must implement appropriate measures to reduce or eliminate these risks. For this component the framework associates four principles (Principles 6-9) and considers relevant, not only the activities related to the objectives' specification and risks' identification but also the consideration of the potential for and the identification and assessment of changes that could significantly impact on the internal control system. The identification and risk assessment must relate to the company as a whole, also taking into account risks related to IT.

The component which concerns the control of activities requires the entire organization to select and develop, through policies and procedures, control activities that contribute to reduce the risks of reliability of financial reporting to an acceptable level. Control activities are performed at all levels of the entity, at various stages within business processes and must also include the IT. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities (COSO, 2013). The framework, which associates three principles to this component (Principles 10-12), requires a clear cut management to determine the relevant business process and to considers at what level control activities are applied and how they address the issue of segregation of duties. At the same time, management must determine whether duplicates of control activities can be eliminated and must identify opportunities to implement preventive control activities earlier in the business process. In addition, the framework considers relevant the account reconciliations, which are a part of the financial reporting process. These reconciliations require a critical control activity for reducing the risk of material misstatement in the financial statements; management should decide, then, to implement a partial

automated process. According to COSO, the organization must take into account general control activities over technology. In this context, activities related to the understanding of technology dependencies are considered relevant, whereas they evaluate end-user computing processes, as well as those relative to period-end reporting. Management must also take an interest in the IT infrastructure configuration to support restricted access and segregation of duties and to define appropriate access rights for financially significant applications and processes. Last but not least, the development and documentation of policies and procedures and their reassessment, as well as the establishment of responsibility and accountability, which become important elements for the control activities.

For the component related to Information and Communication, COSO associates three principles (Principles 13-15) that highlight the importance of the quality of information and adequacy of communication processes. Information is necessary for any entity to carry out internal control responsibilities to support the achievement of the financial reporting objective. Management obtains or generates and uses relevant quality information from both internal and external sources to support the functioning of other components of internal control. Communication is that continual and iterative process of providing, sharing and obtaining the necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down and across the entity. Thus, the three identified principles require attention to the following aspects. Management should evaluate business activities to identify information requirements and should enhance information quality through a data governance program. In this component, a crucial role is played by the Chief Information Officer (CIO) who, through data and information life cycle (input, processing, output and storage), must be able to identify, protect, retain and validate financial data and information. At the same time, the framework shows that in addition to the quality of the information, there is the need to develop an appropriate process of communication. Senior management should communicate information about the company's financial reporting objectives, financial control requirements and internal control policies and procedures and how they support individual responsibilities through a variety of communication channels (COSO, 2013).

Finally, for the monitoring activities component, to which are associated the Principles 16 and 17, the framework requires management to monitor the controls that are in place to be sure that the company continues to achieve its financial reporting objectives. The management must also evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for them to take any corrective action.

To illustrate how the COSO framework impacts on the deficiencies related to financial reporting, the main MWs, identified by prior research (Doyle *et al.*, 2007a; Grant *et al.*, 2008; Boritz *et al.*, 2013), have been classified within the context of the five components of COSO (Table II). These MWs include both those related to company-level and those that are account-specific. The company- level MWs are referred to general problems within the company itself. Account-specific MWs are weaknesses related to specific accounts or transactions. However, it should be noted that the company-level MWs are most important in relation to three different reasons:

(1) they are difficult to identify by the auditors, as they relate to general aspects of the companies' operations and are not limited to specific events/transactions;

COSO components	Material weaknesses
Control environment	Inappropriate "tone from the top" established by the executive officers or senior management.
	Low quality of internal audit or audit committee
	Weaknesses in the control environment which challenge the effectiveness of senior management's communications regarding the importance of internal controls
	Insufficient personnel resources with appropriate qualifications and training in accounting, finance or information systems
	Lack of a formal program for training members of the company's finance and accounting group
	Deficiencies related to the design of policies and execution of processes related to accounting for transactions
	Lack of adequate personnel to effectively perform supervision and review
	Lack of permanent employees in key financial reporting positions
	Inconsistent application of accounting policies
	Inadequate personnel preparation, related to the review of reconciliations
Risk assessment	Deficiency in the design and implementation of internal control over financial reporting
	No consistent risk assessment process
	Lack of adequate mechanisms for anticipating and identifying financial reporting risks
	Inadequate procedures for appropriately assessing and applying certain SEC disclosures and requirements
	Inadequate internal controls relating to the authorization, recognition, capture, and review of transactions, facts, circumstances, and events that could have a material impact on the company's financial reporting process
Control activities	Ineffective control to prevent certain members of management from overriding certain controls and effecting certain transactions and accounting entries
	Lack of internal audit review of subsidiary operations
	Lack of documentation of policies and procedures
	Lack of segregation of duties in internal control procedure
	Inadequate review of audit logs
	Failure to identify abnormal transactions in a timely manner
	Ineffective controls over the period-end financial reporting process including the procedures used for calculating significant estimates and performing consolidation entries.
	Lack of appropriate process over financial reporting or certain accounts
	Lack of compliance with established procedures for monitoring and adjusting balances relating to certain accruals and provisions, including restructuring charges
	Lack of effective controls over quarterly and annual financial statement close processes
	No adequate internal controls over the application of new accounting principles or the application of existing accounting principles to new transactions
	Problems with certain accounting reconciliations and review procedures
	Failure to timely reconcile account balances
	Deficiencies in the period-end reporting process (closing process)
	Deficiency in segregation of duties associated with personnel having access to computer accounting or financial reporting record

(*continued*)

Table II.
Material weaknesses classification

COSO components	Material weaknesses
Information and communication	Lack of appropriate documentation to support journal entries
	Insufficient documentation with respect to the review of non-standard journal entries
	Inadequate documentation surrounding standard operating procedures for certain key aspects of information technology environment
	Inappropriate segregation of duties to ensure that accurate information is contained in certain types of internal and external corporate communications, including press releases
	Lack of effective information systems required to support operations and reporting requirements
	Information technology has a number of areas where formal, documented policies and procedures have not been developed
	Lack of information systems access and security controls to initiate, authorize, and record transactions (excessive access to systems and databases)
	Lack of understanding of key system configurations
	Insufficient control over information technology back-up, recovery and firewall protections
	Weaknesses related to the establishment of standards for review of journal entries and related file documentation
	Deficiencies related to the accounting and financial reporting infrastructure for collecting, analyzing and consolidating information to prepare the consolidated financial statements
	Failure to segregate duties within applications, and failure to set up new accounts and terminate old ones in a timely manner
Monitor Activities	Inadequate controls to monitor the results of operations and other control activities
	Lack of proper oversight for making application changes and improper change management
	Insufficient controls over the monitoring of appropriate methods or assumptions

Table II.

(2) they often produce a greater impact on financial reporting, as they have a wider scope; and

(3) their negative effects are difficult to determine because the cause–effect relationship is less clear (Doss and Jonas, 2004; Doyle *et al.*, 2007a).

The MWs listed in Table II can be connected to a few categories of problems. The MWs are associated with the component of the control environment regarding the inappropriateness of the tone from the top, the insufficient personnel resources with appropriate qualifications and training in accounting and the deficiencies related to policy design. In the component of risk assessment, MWs relate to the inconsistency of the risk assessment process and to the lack of adequate mechanisms for anticipating and identifying financial reporting risks. With regard to the control activities component, the main MWs concern the lack of policies and procedures, as well as segregation of duties, deficiencies in the period-end reporting, revenue recognition and account reconciliation and also lack of internal audit review. Rather, within the Information and Communication component, the MWs relate to a low quality of information that is not

supported by adequate documentation, inadequate IT hardware infrastructure and insufficient control over the same, deficiencies in the information systems and failure in segregation of duties within applications. Finally, in the component of the monitor activities, the main MWS refer to insufficient or inadequate control activities and to the inability to make timely changes to the whole internal control system.

The analysis performed shows that the framework – through the finding of appropriate principles, points of focus, example and approaches – allows identification of the main deficiencies that may hinder the achievement of the reliability of financial reporting. This leads one to assume that the COSO framework is able to reduce the main weaknesses of the internal control system related to the reliability of financial reporting. Among other things, the effectiveness of the framework is also confirmed by the fact that most companies use COSO as a benchmark for assessing their ICFR (Shaw, 2006; Martin *et al.*, 2014). The strength of the COSO framework is to have introduced the concept of internal control and to have helped companies to detect, as well as to prevent material misstatements due to quantitative and qualitative effects caused by error or fraud. At the same time, it must be recognized that the framework has defined five basic components and guidelines that allow the internal control system to achieve the three categories of objectives.

However, COSO also shows some limitations. First of all, 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 (O'Donnell and Rechtman, 2005; Tuttle and Vandervelde, 2007; Huang *et al.*, 2011; Chang *et al.*, 2014). It is easy to understand that the level of abstraction of the framework issued in 1992 is higher than the newly updated version. The new framework fills part of this gap by also developing "illustrative tools" to provide templates and scenarios that may be useful in applying the framework. As already noted, the clarification of the 17 principles associated with the five components cannot be considered a novelty, as they were still implicit in the original framework. At the same time, although 77 points of focus help to identify, for each component, the relevant financial reporting weaknesses, it should be noted that they increase the level of detail without constituting a control processes, as they do not provide a complete and comprehensive list (Protoviti, 2014). The provision of detailed control processes might increase the effectiveness of the framework. Furthermore, the ICEFR compendium does not illustrate all aspects of the components and principles that would be otherwise necessary for an effective internal control and, therefore, it is not sufficient to demonstrate that each of the five components and relevant principles are present and well-functioning (COSO, 2013). The practical approaches and examples provided in the compendium 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 (Principle No. 11), it is, nevertheless, considered not to be a specific tool that provides useful guidance and background material in the consideration of specific controls over technology. The updated framework has implemented tools that consider how the more sophisticated technology can have an impact on the functioning of all internal control's components. Therefore, taking into account the granularity necessary when addressing technology controls, the COSO framework is not suitable to be used purely as a tool to facilitate the evaluation of the IT controls.

The COBIT framework and financial reporting

One of the most influential IT frameworks is known as COBIT, now in its fifth iteration. The purpose of COBIT is to provide a set of recommended best practices for governance and control processes of information systems and technology with the essential objective of aligning IT with business. COBIT 5, built on the foundation of earlier versions (e.g. domains, business processes, maturity models, RACI charts), makes some significant changes in the design and implementation phases. The basic assumption, that over time has allowed this framework to be continuously developed, is the understanding that information management assumes a strategic importance in any company together with the significant role that technology plays.

COBIT helps professionals and company managers to use the benefits of IT while maintaining a balance between the expected benefits and risks, in addition of helping them optimizing the use of resources. The COBIT framework, in its evolutionary path, has changed its focus. As a simple audit tool, COBIT 1 has become a tool of corporate governance focused on the governance of information systems COBIT 5, passing through COBIT 2 (Control), COBIT 3 (Management) and COBIT 4 (IT governance). This step enabled the framework to implement a more detailed set of control objectives, as well as to rewrite the structure of IT processes in a broader perspective that also considers the reliability of financial reporting (ISACA, 2012a).

The operating logic of COBIT can be briefly described by analyzing the three levels that characterize it. In the first level, there are the business requirements for information that must be satisfied to achieve the company objectives: effectiveness, efficiency, reliability, compliance, confidentiality, integrity and availability. In the second level, there are the 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, which concerns the IT processes. COBIT 5 is based on 37 high-level IT control objectives and on a general classification structure that identifies three levels of IT activity: domains, processes and activities. The COBIT framework connects the informative and governance company's requirements to the IT function objectives. Practically, the model is based on the assumption that the IT resources are managed by IT processes to achieve the IT objectives that meet the company's information business requirements. A company should elaborate, through IT resources, all that information which corresponds to its own needs to satisfy the company's specific business needs (ISACA, 2012a). As regards to these aspects, it is important to implement a solid IT control objective pattern. The integration of the components, which make up the three levels of the COBIT structure, enables the implementation of a set of IT controls that are effective to also achieve the objective of financial reporting's reliability.

In relation to this objective, it should be noted that COBIT is not a specific internal control framework but is a tool of governance of information systems. However, the relevance assumed by the information systems within organizations helps to increase the importance of this framework in the ICFR. As well, the popularity of IT applications has increased reliance on computers for processing business transactions. (Chang *et al.*, 2014). Modern enterprises are critically dependent on IT for the conduct of business operations (Stoel and Muhanna, 2011). This increased reliance on IT, which also has an important role in the ICFR activities. Therefore, in this context, it is possible to highlight the positive impact that COBIT has on the activities related to ICFR.

First, the framework's analysis shows that many categories of business requirements for information, affecting, in particular, the IT control objectives, are related to the reliability of financial reporting objectives. The primary objective of financial reporting is to provide high-quality information that becomes useful for decision-making (FASB, 1999; IASB, 2008; Van Beest *et al.*, 2009). The financial reporting quality can be defined in terms of decision-making's usefulness (McDaniel *et al.*, 2002; Beuselinck and Manigart, 2007) i.e. "[…] as an information about the reporting entity that is useful to present to potential stakeholder" (IASB, 2008). This can be achieved if the information has some qualitative characteristics that coincide with the business requirements for information. The information must be relevant and pertinent to the business processes and must be made available in a timely manner, without errors, coherently in such a way that can be used as effective (effectiveness). Furthermore, the information must be managed by using the resources in an optimal manner, both in terms of productivity and savings (efficiency) and must comply with the laws and external business constraints (compliance). The information must also comply with the requirements of confidentiality and integrity. The first concerns the protection of sensitive information related to potentially unauthorized accesses. The second refers to not only the accuracy and completeness of the information but also to its validity with regards to the company's values and expectations. Another element that characterizes the quality of financial reporting is reliability. Management must provide accurate and appropriate information so that the company can be managed to address the financial responsibilities and budgetary/statutory obligations (ISACA, 2012a). The reliability of the information is connected to the ability of the informative system to produce the most honest corporate information so that it allows the elaboration of accurate data.

The reliability of financial reporting is claimed to be a function of the effectiveness of a firm's internal control (PCAOB, 2004; Donaldson, 2005). The lack of reliability adversely affects the financial statements quality (Hogan and Wilkins, 2005; Bedard, 2006; Doyle *et al.*, 2007b). In fact, the reliability of financial information depends on the organization of IT (Fox and Zonneveld, 2003), whereas expertise in IT is a requisite condition for SOX compliance (Walters, 2007). The accuracy of all available data depends on the lack of voluntary or involuntary errors or changes, on the adequacy of the controls and on the correctness of the people that are entitled to process them. To consider information as being reliable, it is necessary to make sure that it respects the requirements included in the reliability categories of transaction and budgetary balance (Beretta and Pecchiari, 2007). Wixom and Todd (2005) state that completeness and reliability play particularly important roles in explaining the overall information and quality system. The requirements relating to the reliability and accuracy of information are met thanks to an effective implementation of the COBIT itself. The integration between the IT resources and IT processes are the key requirements to ensure the proper functioning of the model. The overall examination of the seven business requirements makes it possible to highlight their contribution to the improvement of the quality of information, which is an extremely important element for the reliability of financial reporting (Jonas and Blanchet, 2000; Wittenberg-Moerman, 2008; Armstrong *et al.*, 2010; Jara *et al.*, 2011). Consequently, the fulfillment of these business requirements helps to implement IT controls which can support the improvement of the quality of financial reporting, which is characterized by a more understandable, comparable, verifiable and timeliness-based information (Van Beest *et al.*, 2009).

Second, in relation to the other two elements of the COBIT structure, it could be argued that the core of the framework is represented by the IT processes, which allows for a precise definition of policies and procedures, as well as by the organization of the resources which are needed to produce certain outputs being consistent with the reporting objectives. Indeed, the activity of forecasting and implementing IT control objectives requires a detailed mapping of all the activities purported within a company. Therefore, the definition of a company's processes and activities allows one to define the resources which are needed not only for company operations but also to coordinate them to become more effective in terms of achieving the planned objectives. This also leads to defining the relationships that should exist between the components of IT resources (people, infrastructure and applications), which represent the basis of the organizational structure of the ICFR. Moreover, all this also implies that the duties to be assigned and the company responsibilities must be well defined. Consequently, there is a need to express the basic criteria used to divide the work among the different operators that would ultimately end up in the definition of the elementary components of the organizational structure, duties and activities and the intermediate components of the organizational structure, which are obtained through the aggregation of the elementary components or organizational units. The integration between the IT resources and the IT processes facilitates the implementation of the control organization processes, as well as the information/communication organization ones. The first allows to define the behaviors that can be expected as regards to the individual roles and to check congruency between the expectations and the effective implementation of what is expected. The objectives that have to be reached and the resources available for such purpose should, of course, be specified for every organizational unit. The second, however, represents the methods which are planned and through which the members of the organization communicate to perform the duties they were assigned for. These provide the basic knowledge needed to make decisions and to fulfill the responsibilities of those who work in the company. In fact, some of the relevant issues to the financial reporting process are represented by the segregation of duties and the lack of adequate procedures and processes that are covered. Ashbaugh-Skaife *et al.* (2007) and Doyle *et al.* (2007a) also document factors, including organizational complexity, major firm changes and inadequate resources, which are common to the risk of disclosing MWs in the ICFR. IT control objectives focus on guiding the overall process for monitoring and assuring compliance with the SOX Section 404 requirements. Specific functions include the central data repository, responsibility assignment, communication, scheduling and signing-off of applicable control tests and SOX tasks. These features allow management and assurance teams a greater level of confidence regarding the status of a company's ICFR. In addition, the IT processes have a compliant strategic role aiming at streamlining only the selected and specific business procedures and targets and only certain aspects of internal control, such as policy management, record of segregation of duties, documentation and document workflow (Masli *et al.*, 2010).

Another element that has an impact on the ICFR concerns the provision of a set of IT general controls and IT application controls. The first considers policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. These controls apply to mainframe, server and end-user environments, and these commonly include: controls over data center and network operations; system software

acquisition, change and maintenance; access security; application system acquisition, development and maintenance; physical security of assets, including adequate safeguards such as secured facilities over access to assets and records; and authorization for access to computer programs and data files. These controls are one of the most important areas to review, especially for companies that must comply with the SOX provisions (PCAOB, 2004; Grant *et al.*, 2008; Haislip *et al.*, 2011), taking into account that the accuracy and reliability of financial reporting depend on, to a large extent, IT controls that an organization has in place. IT application controls, however, are related to specific computer software applications and individual transactions. These controls include functions within the software application that control the processing of transaction and storage of data. In the COBIT framework, for each of the 37 processes, specific control objectives are defined. Some common application controls include (ISACA, 2009):

- logical access controls;
- data entry/field validations;
- business and workflow rules;
- field entries being enforced based on predefined values;
- work steps being enforced based on predefined status transitions;
- reconciliations: review and follow-up of application-generated exception reports;
- automated activity logs;
- automated calculations; and
- management and audit trails.

Application controls refer to controls over the processing of transactions and data within an application system and are specific to each application. The objectives of application controls, which may be manual or programmed, are to ensure the accuracy, integrity, reliability and confidentiality of the records and the validity of the entries made therein, resulting from both manual and programmed processing (ISACA, 2009).

The use of both categories of IT controls allows the framework to monitor relevant processes involving the occurrence of the main MWs related to IT. The effectiveness and validity of the framework in relation to coping MWs connected to IT is attested by numerous studies and research (Lainhart, 2000; Tuttle and Vandervelde, 2007; Rozek, 2008; Lin *et al.*, 2010; Cereola and Cereola, 2011). This structured framework allows managers to provide detailed IT audit tests. In this manner, the COBIT makes up for the limited guidance provided by COSO (Grant *et al.*, 2008) and helps managers and auditors to evaluate IT controls for SOX compliance (Blum, 2005). To assure compliance with SOX, Information Systems Audit and Control Association (ISACA) has developed a useful guidance and tools for companies trying to prepare and sustain their IT organizations relative to SOX compliance. This publication (ISACA, 2006) analyzes the principal IT general controls identified by the PCAOB Auditing Standard No. 2 and the COBIT processes.

COBIT is worldwide accepted and recognized and provides critical information of IT governance and control framework for management and reliable assurance of the IT controls (Huang *et al.*, 2011). Tuttle and Vandervelde (2007) examined the conceptual model of the COBIT framework and found that the model can be useful for auditors

while they assess IT controls. Rozek (2008) argues that COBIT can assist auditors in the assessment of the overall attitudes about IT controls and provides a standard way to record the state of the internal control. Some auditors have found that COBIT represents a valid framework for the purposes of SOX compliance (Chan, 2004; Abu-Musa, 2008). This framework has become the main resource available to firms for implementing and globally improving the IT Governance framework. In fact COBIT 5 has consolidated the previous version in a single framework by incorporating other frameworks such as Val IT and Risk IT; at the same time, the framework was updated to be in line with the current practices provided by ITIL. One of the strengths of the framework is the provision of detailed audit tests. COBIT provided for each high-level IT control objectives a series of indications such as process description, process purpose statement, outcomes, best practices to be followed, work products that contains the detailed inputs and outputs process descriptions. Every high-level control objectives is a reference or check guide that make possible to review the processes by providing managers with a benchmark of reference to improve the ICFR. The IT processes, as well as numerous specific guidance developed by the framework, provide managers and auditors specific tools.

However, the COBIT framework also has some limitations. At first, it must be argued that COBIT requires significant resources for its implementation. This could prevent the use of the framework in small- and medium-sized companies. Furthermore, as noted, COBIT is not a specific framework of internal control. In this context, while the COSO framework should be considered as an overall evaluation framework for internal control, COBIT provides useful guidance and background material in the consideration of specific controls over technology (Protoviti, 2014). COBIT essentially focuses on the governance of information systems. Consequently, it primarily allows mitigation of the problems of the financial reporting related to IT. For these reasons, it cannot constitute itself as an autonomous framework for ICFR. However, if integrated with a specific internal control framework, such as COSO, it can be a valuable tool to reduce or eliminate the MWs.

How COBIT supports the COSO framework by reducing MWs

The analysis carried out in the previous paragraph shows that the two frameworks, both COSO and COBIT, have some limitations. Nevertheless, these limitations compensate each other. Although COSO does not address the specific risks and complexities of IT, these are addressed by COBIT. This framework provides supplemental criteria in the implementation and assessment of IT controls and supplies the detailed control objectives that auditors require in the design of audit tests. Therefore, this allows for support activities relating to the ICFR. The presence of IT processes within COBIT helps to strengthen the whole system of internal control that must be based on five components that make up the COSO framework. Therefore, COBIT is not an alternative to COSO; rather, it should be seen as a complementary framework that improves the quality of financial reporting by reducing or eliminating the MWs of the ICFR. It can be said that COBIT complements the COSO framework by assessing internal control and balances risks in IT intensive environments (Ramos, 2004; ITGI, 2005; Chang *et al.*, 2014). It is important to note that the COBIT methodology is fully compliant with COSO standards. The combination of both standards provides a

good benchmark for the fulfillment of the requirements on the internal control system (Rubino and Vitolla, 2014a) and for the reliability of financial reporting.

The core structure of the framework is based on 37 high-level IT control objectives that 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 the company level, when looking at IT. (ISACA, 2012a). 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 also 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 (ISACA, 2012b, 2013).

In addition, the structure of COBIT has other important elements that help to understand the role of the framework to achieve the objective of the reliability of financial reporting. First, COBIT provides a responsible, accountable, consulted, informed (RACI) chart for each phase of its implementation that describes who is responsible, accountable, consulted and informed for the key selected activities and also for each IT process. Second, COBIT contains a process maturity model. This model, now named process capability model, is used to measure the current maturity of a company's IT-related processes. In addition, it is used to define a required state of maturity to determine the gap between the processes and to improve the process to achieve the desired maturity level (ISACA, 2012a). There are six levels of capability that a process can achieve, from "incomplete process" (zero level) to "optimizing process" (five levels). All these described elements allow COBIT to provide IT controls which are characterized by a greater level of detail. In addition, it is also important to consider the role played by the best practices or by metrics, which are used to measure the extent by which the objectives are achieved. By the same token also the presence of inputs and outputs (i.e. the process work products) receives a consideration to the extent that they are deemed to be necessary to support operation of the process.

The following paragraph provides a brief description of five COBIT's domains illustrating the relationship between the IT processes and the five components which make up COSO (Table III). The analysis shows how the IT processes of COBIT, in relation to the objective of reliability of financial reporting, provide some indications that improve the components of the COSO when facilitating the reduction or elimination of the MWs.

The processes included in the EDM domain deal with the risk and resource optimization which are related to the use of IT. These processes analyze and articulate the requirements for a successful governance of IT companies which put in place and maintain effective enabling structures, principles, processes and practices with clarity of responsibilities and authority to achieve the company's mission, goals and objectives. In this domain, COBIT requires the development of some activities, metrics and detailed IT control objectives that support primarily the components of the control environment, control activities and risk assessment. Periodic checks allow to verify that the roles,

COBIT 5 processes	COSO components: Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
Evaluate, direct and monitor					
EDM.01 Ensure governance framework setting and maintenance	X		X		
EDM.02 Ensure benefits delivery	X		X		
EDM.03 Ensure risk optimization		X	X		
EDM.04 Ensure resource optimization	X		X		X
EDM.05 Ensure stakeholder transparency	X				
Align, plan and organize					
APO.01 Manage the IT management framework	X		X	X	
APO.02 Manage strategy	X		X		
APO.03 Manage enterprise architecture			X		
APO.04 Manage innovation			X		X
APO.05 Manage portfolio		X	X		
APO.06 Manage budget and costs			X		
APO.07 Manage human resources	X				
APO.08 Manage relationships	X			X	
APO.09 Manage service agreements				X	X
APO.10 Manage suppliers			X	X	X
APO.11 Manage quality			X		
APO.12 Manage risk		X			
APO.13 Manage security		X	X		
Build, acquire and implement					
BAI.01 Manage programmes and projects	X		X		X
BAI.02 Manage requirements definition			X	X	

Table III.
COBIT 5 processes and COSO components

(*continued*)

COBIT 5 processes	COSO components: Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
BAI.03 Manage solutions identification and build	X		X		
BAI.04 Manage availability and capacity		X		X	
BAI.05 Manage organizational change enablement	X	X	X	X	
BAI.06 Manage changes	X		X		X
BAI.07 Manage change acceptance and transitioning	X		X		
BAI.08 Manage knowledge			X	X	
BAI.09 Manage assets		X	X		
BAI.10 Manage configuration			X		
Deliver, service and support					
DSS.01 Manage operations			X		X
DSS.02 Manage service requests and incidents			X		X
DSS.03 Manage problems			X		X
DSS.04 Manage continuity		X	X		
DSS.05 Manage security services		X	X		
DSS.06 Manage business process controls	X		X		X
Monitor and evaluate					
MEA.01 Monitor, evaluate and assess performance and conformance					X
MEA.02 Monitor, evaluate and assess the system of internal control					X
MEA.03 Monitor, evaluate and assess compliance with external requirements			X		X

Table III.

responsibilities and authorities (defined, assigned and accepted) are covered by appropriate IT processes. This allows to verify the existence of any decision-making or control processes that are not supported by IT. At the same time, it is significant to proceed with the implementation of some periodic checks such as the date of the last revision to reporting requirements, the calculation of the percentage of reports that are not delivered on time, the percentage of reports containing inaccuracies and the verification of the number of breaches of mandatory reporting requirements. These checks allow to identify some deficiencies that may affect the assessment of the control environment and of the control activities. Furthermore, the evaluation of the number of stakeholders who understand policies, the verification of the percentage of policies supported by effective standards and working practices, and also the frequency of policies reviewed and updated, are necessary to ensure a proper implementation of the processes and, hence, to reduce the risks identification.

In the second domain (APO), the 13 processes provided are intended to support goals and activities included in others domains, which are BAI and DSS, and work in the identification of the best way by which IT can contribute to the achievement of the business objectives. They define requirements for taxonomy, standards, guidelines, procedures, templates and tools and also improve the alignment, the increase of agility and the quality of information. The activities and processes included in this domain affect some aspects such as innovation, quality management and risk and safety. Some elements in this domain can be identified which include best practices, activities, metrics and sub-goals and help to understand the level of details provided by the framework. The quality of information also depends on the motivation and skills proper of human resources. For this reason, COBIT requires an assessment of the number of learning/training hours per staff member, the percentage of staff satisfied with their IT-related roles and the development of a skills and competencies' matrix. However, some best practices request the evaluation of staffing requirements on a regular basis or upon major changes to ensure that the IT function has sufficient resources to appropriately support company goals. Also very much relevant are those required policies ensuring consultants and contract personnel to comply with the organization's policies that would meet agreed-on contractual requirements. This allows one to limit certain risks inherent in the financial reporting when some activities are outsourced. It could be arguable that the set of these elements is to strengthen the components of the control environment, information and communication, control activities and risk assessment.

The BAI domain, instead, provides solutions that transform them into services. To implement the IT strategy, the IT solutions must be identified, developed/acquired, implemented and integrated with the company processes. Moreover, the changes and maintenance of the existing applications also fall into this domain to ensure the continuity of the life cycle of the systems. This domain concerns not only the new projects' ability to satisfy the company needs but also the implementation of new projects with respect to deadlines and the budget. In this domain, relevant aspects are those related to the change management and the processes development that provide solutions to the problems encountered. The best practices of COBIT recommend to make appropriate test periods, on the new procedures, to limit the risks linked to the existence of some bugs. Change management and the introduction of new regulations involve the development of procedures that are not tested. Furthermore, the best practices require management to ensure that approved

changes are implemented as planned, to define an appropriate retention period for change documentation, as well as *ex ante* and post-change system and user documentation; to maintain a tracking and reporting system to document rejected changes; to communicate the status of approved and in-process changes; and to complete changes. These are some critical issues that affect financial reporting. Again, these elements help strengthening the components of the control environment, information and communication, as well as control activities and risk assessment.

The processes that belong to the DSS domain receive solutions and make them usable for end users. This domain is concerned with the actual delivery and support of required services, which include service delivery, management of security and continuity, service support for users and management of data and operational facilities. To enable an effective delivery and usage of information, COBIT requires to monitor and track incident escalations, as well as resolutions and request handling procedures to progress toward solution or conclusion. In addition, the framework provides guidance to identify stakeholders and their information needs for data or reports. Moreover, with regard to the aspects closely related to IT, it is very much required to take into account the number of vulnerabilities discovered, the number of firewall breaches, as well as some accesses occurring more often than the average or at times which are not compatible with working hours. Also, some best practices indicate that it is necessary to establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage. These controls protect the quality of information impacting on the seven categories of business requirements for information. They have an impact mainly on components related to information and communication and control activities.

Finally, the three processes included in the MEA domain are to monitor all processes to ensure that the direction provided is followed. All the IT processes need to be regularly assessed over time to guarantee quality and compliance with control requirements. These processes address performance management, monitoring of internal control, regulatory compliance and governance. In this domain, best practices imply to continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. In addition, these practices require to enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Management should plan, organize and maintain standards for internal control assessment and assurance activities. These detailed control objective have an impact on the component related to the monitoring of activities.

The COBIT framework states that all processes work in an integrated manner to ensure the achievement of business objectives including those relating to financial reporting. In fact, as it emerges from an examination of Table III, each domain, although dedicated to achieving specific goals, has an impact on more than one component of COSO. The analysis between IT processes and COSO's components highlights how COBIT is able to provide a greater level of detail in the control processes by limiting the level of abstraction inherent in the COSO and strengthening its components. The processes of COBIT cover all COSO's components by reflecting the great importance coated from IT in any set of a company. IT represents one of the most valuable corporate asset, taking into

account that the majority of companies, including smaller ones, use computers to process information.

Having said that, with regard to the role that COBIT plays in individual categories of MWs, it is possible to observe the following. The framework, as a whole, is a tool for IT governance that focuses on governance and management processes of information systems. All the 37 IT processes of COBIT, each of them is related to the objectives set up by the domain that is linked, are aimed to ensure the effectiveness and reliability of information systems, as well as of the appropriate communication processes. Therefore, the framework has a direct impact on the MWs that belong to the Information and Communication category, as can be seen from an examination of some processes. The APO.01 and APO.05 processes define, maintain and provide appropriate tools and guidelines to provide effective security and controls over information systems to support operations and reporting requirements. The APO.07 process activities ensure access and security controls over information systems and also conduct periodic reviews to ensure that roles and access rights are appropriate and in line with the established agreements. Furthermore, the BAI.07, DSS.04 and DSS.05 processes deal with back-up systems, applications, data and documentation according to a defined schedule by taking into account the frequency, mode, critical end-user computing data, security and access rights and, also, the encryption. These processes ensure the presence of adequate financial reporting infrastructure for collecting, analyzing and consolidating information to prepare the consolidated financial statements.

The overcoming of MWs related to IT allows an organization to cope with the remaining weaknesses. The implementation of the IT governance framework such as COBIT, or, more generally, the adoption of effective IT controls, provides important benefits to the entire company or organization, as demonstrated by numerous studies and research. Messier *et al.*, (2004) state that many financial reporting errors are due to the ineffectiveness of the IT controls. Li *et al.* (2007) find that companies with managers skilled with IT experience have less IT control weaknesses than those companies which do not have those skillful managers. Klamm *et al.* (2012) find that companies with material IT control weaknesses show more non-IT deficiencies, entity- and account-level weaknesses in the same year. They state that companies showing IT MWs will be more likely to exhibit the persistence of MWs in the future than those actually affected by MWs which are not derived from or are related to IT. Morris (2011), highlights that companies which have implemented enterprise resource planning (ERP systems) are less likely to have ICW than those characterized by non-ERP control companies. Similar findings have been delivered by Li *et al.* (2012) asserting that in case of an improvement in the IT control quality, also a decrease in forecast errors was noted. Consequently, it is possible to state that COBIT and IT processes have a directly impact on the IT MWs and an indirect impact on those included in other categories. However, although the framework is entirely focused on the IT governance and management, it is possible to highlight how the framework supports other MWs categories.

Regarding the ICFR, it is crucial to identify and manage the control activities over the information processed by information systems. A structured system of IT processes requires the involvement of a number of appropriate human resources that manage the processes. This indirectly implies the provision of an adequate number of people who also run the processes related to financial reporting. The existence of specific IT controls, which rely on information systems requires the initiation of appropriate

training processes for staff. To design appropriate IT processes, it would be necessary to identify a number of elements such as the type of activities, the resources to be used, the critical elements to be encountered and the expected results. This require the definition of the business processes describing the necessary steps that a company should follow to achieve the financial reporting reliability. At the same time, it is important to take into account top management requirement such as integrity and ethical values. This involves an efficient organization of people, materials, energy and equipment, as well as the definition of policies, procedures and processes into work activities designed to produce a specific end result (Pall, 1987; Davenport and Short, 1990). The definition and management of all these elements imply that the implementation of COBIT necessarily has to deal with the control environment component and related MWs. The EDM.01 process determines the implications of the overall company control environment with regard to IT. The APO.01 process metric requires to verify the number of risk exposures due to the inadequacies in the design of the control environment. Furthermore, the MEA.02 process implies to continuously monitor and evaluate the control environment. It is evident that COBIT cannot influence the tone from the top or improve the quality of internal audit or the audit committee. However, on the other hand, the framework provides an adequate design of policies and execution of processes related to the financial reporting (APO.01, and EDM.03 processes), the allocation of levels of authority (APO.06, APO.08, BAI.01 and BAI.05 processes) and responsibility (MEA.01 and MEA.03 process practices). These aspects constitute the basic elements for the implementation of information systems (Sowa and Zachman, 1992; Sandhu *et al.*, 1996).

The definition of IT controls involves the provision of adequate policies and procedures, the design of controls and personnel resources with appropriate qualifications in accounting, finance or information systems. The setting of policy allows managers to have effective guidelines that ensure consistency and compliance with the company's strategic direction. The procedures define the specific instructions which are necessary to perform a task or a part of a process. The processes indicate where there is a separation of responsibilities and control points. They also address who is responsible to perform the process, what major functions are performed and when the function is triggered. These elements are connected to the component relating to the control activities for which the COBIT offers a valid support. A recurring weakness in the ICFR is represented by the inadequacy of procedures and segregation of duties. For these issues, COBIT requires one to evaluate, review and adjust policies, principles, standards, procedures and methodologies to ensure the achievement of the degree of financial reporting's reliability (MEA.03, APO.07, BAI.06 and DSS.01 processes). Furthermore, the segregation of duties is a key element of the structure of IT controls and COBIT specifies a set of processes that are intended to ensure compliance with this principle to support all business objectives (DSS.06 and APO.01 processes and best practices). The segregation of duties represents an important IT general control. In fact, its primary objective is to prevent frauds and errors. This objective is achieved by disseminating the tasks and the associated privileges for a specific business process among multiple users (Botha and Eloff, 2001). An effective internal control system provides that no single individual should handle all aspects of a transaction from the beginning to the end (Beretta and Pecchiari, 2007). This element represents a critical factor in the process of financial reporting as it is highly emphasized in numerous studies conducted on the issue of internal control weaknesses (Ge and McVay, 2005;

Raghunandan and Rama, 2006; Grant *et al.*, 2008; Huang, 2009; Calderon *et al.*, 2012; Boritz *et al.*, 2013). At the same time, the IT processes covered also the lack related to the account-specific as information systems provide many substantive testing. Moreover, it should be forgotten the important role that the RACI charts play in guaranteeing the well-functioning of the control processes, the development of procedures and allocation of responsibilities to personnel at all levels.

On the same perspective, it is possible to observe how COBIT also impacts on MWs related to the component of the risk assessment. The EDM.03 process ensures that the company's risk appetite and tolerance are understood, articulated and communicated and that risk of the company value related to the use of IT is identified and managed. The activities related to this process ensure that risk thresholds are defined and communicated and that the key IT-related risk is well known. The APO.12 process allows the risk identification, the aggregation of risk profiles and management actions. Furthermore, the best practices of this process require the reporting of the current risk profile to all stakeholders, including effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile. The COBIT contemplates some process that deal with the change management trying to identify in advance the occurrence of certain types of risk (DSS.04, DSS.05, MEA.0 and BAI.06 processes). These activities are also important for the reduction of MWs related to the component of the Risk Assessment.

Finally, it should be noted that each IT process has a life cycle that involves its definition, creation, operation, monitoring and also its update. Generic process practices such as those defined in the COBIT process assessment model can assist the monitoring and the optimization of processes. Therefore, the COBIT also supports the component of the monitor activities and the related MWs. As previously mentioned, the framework ensures proper change management by also requiring that the update of processes and procedures are implemented in a timely manner. Moreover, in the framework, many processes are identified that ensure the overall monitoring of the all set of activities covered in the individual domains (EDM.02, BAI.03, BAI.04 and DSS.01 processes, and almost all the processes involved in the domain APO).

The analysis conducted shows that the implementation of IT controls allows companies to keep track of the greatest problems affecting the reliability of financial reporting. The IT processes, provided by COBIT, affect the entire corporate structure and impact positively on the MWs covering all five components of the COSO. Recent research carried out on a web-based survey and conducted by Kerr and Murthy (2013) illustrate the utility of COBIT 4 from the perspective of the reliability of corporate financial reporting. The results show that the IT processes rated as the most important for effective ICFR are:

- ensure system security;
- manage changes;
- assess risk;
- manage data;
- assess internal control adequacy,;
- develop and maintain procedures;
- monitor process and educate; and
- train users.

This testifies the relevance assumed by the framework in the professional arena to achieve the reliability of financial reporting. However, taking into account that COBIT does not represent an independent framework for the assessment of ICFR, it should be noted that the reliability of financial reporting can be improved through the combined use of the two frameworks as shown in Figure 1. The integration between the control's structure provided by COSO framework and the specific attributes provided by COBIT facilitates a substantial reduction or elimination of the MWs.

Conclusions

The aim of this study was to assess how the COBIT framework, integrated into the wider internal control system, enables an organization to reduce or eliminate the MWs. The paper starts from the analysis of the limitations inherent to the internal control's framework such as the COSO, as a means to pursue the reliability of financial reporting. COSO stands as the main framework that companies use to assess their ICFR. Since 1992, this framework has been facilitating organizations' efforts in their aim to achieve important business objectives and to develop cost-effective systems of internal control, as well as sustaining and improving performance. Although the COSO framework is internationally accepted and recognized, it shows some limitations due to its lack of ability in addressing specific risks and complexities of IT and in providing detailed control objectives. Conversely, COBIT focuses on IT and provides high-level control objectives that are represented by the IT processes. The structure of COBIT, although it focuses on governance and management of information systems, is quite consistent to ensure valid support for the reliability of financial reporting. The seven business requirements for information provide valid references for the implementation of 37 IT

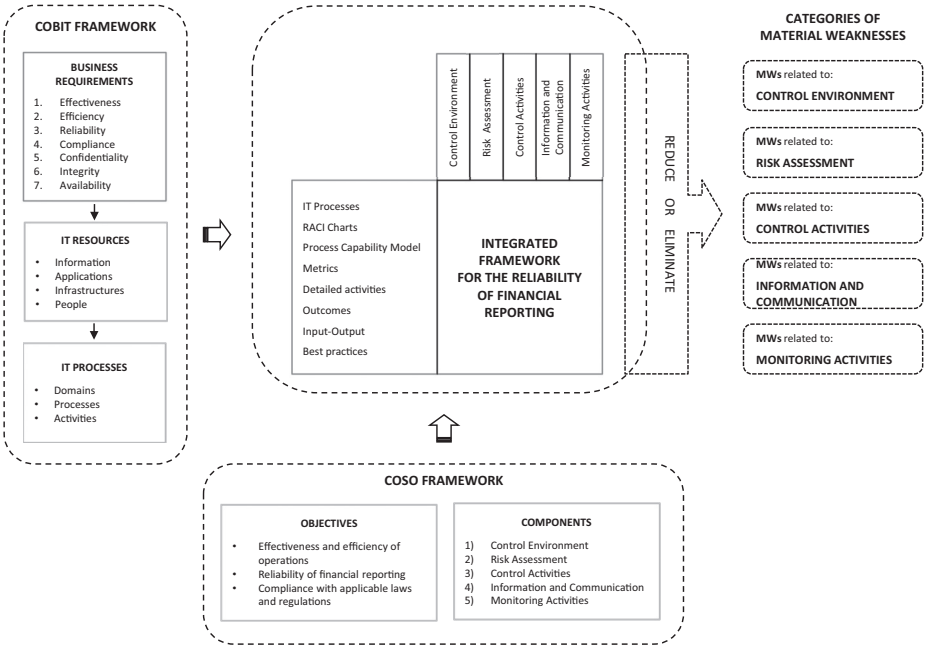

Figure 1.
An integrated framework for the reliability of financial reporting

processes. These processes supply detailed control objectives that auditors require in the design of audit tests. COBIT has evolved over the years by assuming a prominent role in the international arena and also in relation to SOX compliance. 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. The RACI charts and the process capability model are some detailed elements that improve the COSO's components when facilitating the reduction or elimination of the MWs. In addition, the prediction of each single process's metrics and set of best practices and activities constitutes a valuable tool that facilitates both management and the auditors to identify the main MWs that may affect their companies. The processes of COBIT working in an integrated manner, enable and support all the COSO's components. Every single process, according to the goals of the domain to which it relates, provides additional tools that help to identify the MWs of the ICFR.

What contributes to the dissemination and appreciation of COBIT is the very fact that it has transposed some observations on professional practice and academic studies related to the internal control's issues. This has enabled the framework to develop valid best practices that lead toward an effective control of processes, which, in turn, ensure greater reliability in terms of data and information. The peculiar aspect that allows the model to make significant improvements in ICFR is represented by the structure of the processes itself. The process approach combines IT activities with their design to achieve the same output. Such orientation involves a transversal vision of the organization that is structured according to a series of activities that constitute the chain links of the value process and to a series of processes that constitute the chain links of the organizational value. The process-based approach enables the delivery of significant improvements, whereas it gives priority to value creation and correction of malfunctions, as well as to the prevention of errors and an optimal usage of resources. The basic concept of the framework is that, for IT control, it is necessary to consider the information needed to support the implementation of the company's objectives but also the information resulting from the combined application of resources connected to IT which are run through their own IT processes.

The results of the paper deliver useful and important information to be available to company's managers. First of all, from a general viewpoint, it should be observed that the adoption of the COBIT framework provides companies with an opportunity to implement an internal control framework that creates a series of advantages for the entire organization. Indeed, COBIT helps companies to maintain a high quality of the information that supports business decisions-making and also to achieve operational excellence through an efficient and reliable technology. The framework also ensures that laws, regulatory provisions and contractual agreements are observed, thus enabling regulatory compliance (ISACA, 2012b). This allows the framework to facilitate the achievement of the other two objectives of the internal control system: effectiveness and efficiency of operations and compliance with applicable laws and regulations. Furthermore, COBIT keep risks associated with IT to an acceptable level and supports risk management activities (Rubino and Vitolla, 2014b).

COBIT provides managers with the most advanced tools for the purposes of compliance with the obligations imposed by SOX and, in general, to improve the financial reporting's reliability also in relation to the provisions of the PCAOB's

Auditing Standards Nos 2 and 5. Furthermore, the analysis of the framework's impact on the MWs shows that an effective implementation of the internal control system requires managers to pay more attention to the role played by the informative system and its relative controls. Indeed, managers often focus their attention on the internal control components and underestimate the role of the information system, especially during the processes' phase of structuring and review and also when clearly defining the roles and responsibilities. In this context, the framework offers managers the opportunity to improve IT processes by identifying the operational weaknesses and highlighting the opportunity to redesign or improve the IT processes. Therefore, the adoption of the framework involves an improvement of the relationships between the IT and business function. Consequently, companies are allowed to assign roles and responsibilities of the process in a clear and correct manner. This should also lead managers to check the operations of their own information system before attempting to implement an internal control system.

Specific managerial implications, related to the reduction or elimination of MWs, are particularly important. The implementation of the framework requires managers to carefully consider specific MWs: accounting documentation, policy or procedures, segregation of duties and IT weaknesses. In particular, COBIT suggests managers to review the existing operating procedures, introduce new policies and procedures and adopt documentary models to formalize the carried-out activities. All of this simultaneously involves a review of the organizational roles and a change in terms of the responsibilities that were assigned to the personnel units. Therefore, it also involves the implementation of an effective segregation of duties and, consequently, a more effective control over the operations conducted by the people working within the organization. The implementation of such operating suggestions supports the pursuit of a better control design and the implementation of a stronger information system, which, with the help of IT, is able to ensure greater safety in terms of transaction and access to information. Therefore, the analysis of the structure and the operating methods of the framework highlights the importance of the aforementioned MWs, which if properly faced, also help in reducing the inefficiencies related to period-end reporting, revenue recognition and account reconciliation.

The relevance of some MWs, for the purpose of achieving the objective of financial reporting's reliability, is also confirmed by the latest research which demonstrates that the inefficiencies related to the accounting documentation, policies or procedures represent the MW that is most often reported by companies (Calderon *et al.*, 2012). The analysis carried out in this paper highlights that COBIT processes, working in an integrated manner with each other, have an impact either on the five components which make up the COSO framework on MWs related to the components themselves. The examination of the structure of COBIT and its inherent specific processes offer managers operational directives aimed at reducing or at eliminating the different MWs of the ICFR.

Nevertheless, the framework suggested shows some limitations which do not affect the overall effectiveness of the model. First, it should be noted that COBIT is not well suited to interpret the managerial dynamics of small–medium companies, which often have difficulties in implementing and managing the IT governance and internal control frameworks. Second, what should not be overlooked is related to the complexity of the integration of the two frameworks from the technical point of view. The added value

that can be detected from adopting the framework is only achieved when management is fully aware it is introducing a substantial change within its company system by implementing new control tools. Those tools cannot be considered as merely costs, as they represent forms of investments. Finally, there is also the need to emphasize on the limitations, related to the lack of specific empirical evidence that this conceptual paper puts forward.

The results achieved and the limitations shown provide important insights for future research. First, the framework could be extended considering other perspectives of analysis of an external or internal nature that would act either as antecedents or as a tool to explain more effectively the variability of the results in terms of the MWs reduction (i.e. the sectorial or dimensional differences that exist amongst companies). Furthermore, it is be desirable to assess the effectiveness of the ICFR improvements achieved, as a result of the integration between the COBIT and the COSO framework from an empirical viewpoint, both through case studies and econometric analyses.

References

Abdolmohammadi, M.J. and Boss, S.R. (2010), "Factors associated with IT audits by the internal audit function", *International Journal of Accounting Information Systems*, Vol. 11 No. 3, pp. 152-154.

Abu-Musa, A.A. (2008), "Information technology and its implications for internal auditing. An empirical study of Saudi organizations", *Managerial Auditing Journal*, Vol. 23 No. 5, pp. 438-466.

Altamuro, J. and Beatty, A. (2010), "How does internal control regulation affect financial reporting?", *Journal of Accounting and Economics*, Vol. 49 Nos 1/2, pp. 58-74.

Armstrong, C.S., Guay, W.R. and Weber, J.P. (2010), "The role of information and financial reporting in corporate governance and debt contracting", *Journal of Accounting and Economics*, Vol. 50 Nos 1/2, pp. 179-234.

Arnold, V., Bedard, J.C., Phillips, J.R. and Sutton, S.G. (2011), "Do section 404 disclosures affect investors' perceptions of information systems reliability and stock price predictions?", *International Journal of Accounting Information Systems*, Vol. 12 No. 4, pp. 243-258.

Arwinge, O. (2013), *Internal Control: A Study of Concept and Themes*, Springer, Berlin.

Ashbaugh-Skaife, H., Collins, D.W. and Kinney, W.R. (2007), "The discovery and reporting of internal control deficiencies prior to SOX-mandated audit", *Journal of Accounting and Economics*, Vol. 44 Nos 1/2, pp. 166-192.

Bedard, J. (2006), "Reported internal control deficiencies and earnings quality", Working paper, Université Laval.

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.

Beretta, S. and Pecchiari, N. (2007), "Analisi e valutazione del sistema di controllo interno. Metodi e tecniche", *Il Sole24ore*, Milan.

Bernard, P. (2012), *COBIT 5 - A Management Guide*, Van Haren Publishing, Hogeweg.

Beuselinck, C. and Manigart, S. (2007), "Financial reporting quality in private equity backed companies: the impact of ownership concentration", *Small Business Economics*, Vol. 29 No. 3, pp. 261-274.

Blum, D. (2005), "Act promotes survival of the fittest", *Network World*, Vol. 22 No. 5, p. 37.

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.

Botha, R.A. and Eloff, J.H.P. (2001), "Separation of duties for access control enforcement in workflow environments", *IBM Systems Journal*, Vol. 40 No. 3, pp. 666-682.

Brown, N.C., Pott, C. and Wömpener, A. (2014), "The effect of internal control and risk management regulation on earnings quality: evidence from Germany", *Journal of Accounting and Public Policy*, Vol. 33 No. 1, pp. 1-31.

Calderon, T.G., Wang, L. and Conrad, E.J. (2012), "Material internal control weakness reporting since the Sarbanes-Oxley Act", *Accounting & Auditing - The CPA Journal*, pp. 19-25.

Cereola, S. 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", *Issues In Accounting Education*, Vol. 26 No. 3, pp. 521-545.

Chan, C. (2004), "Sarbanes-Oxley: the IT dimension", *The Internal Auditor*, Vol. 61 No. 1, pp. 31-33.

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.

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

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

Davenport, T.H. and Short, J.E. (1990), "The new industrial engineering: information technology and business process redesign", *MIT Sloan Management Review*, .

Donaldson, W. (2005), *Testimony Concerning the Impact of the Sarbanes-Oxley Act. House Committee on Financial Services, U.S. House of Representatives*, Government Printing Office, Washington, DC.

Doss, M. and Jonas, G. (2004), "Section 404 reports on internal control: impact on ratings will depend on nature of material weaknesses reported", Moody's Investors Service - Global Credit Research, available at: www.complianceweek.com/s/documents/Moodys%20Section%20404.pdf (accessed 6 June 2014).

Doyle, J., Ge, W. and McVay, S. (2007a), "Determinants of weaknesses in internal control over financial reporting", *Journal of Accounting and Economics*, Vol. 44 Nos 1/2, pp. 193-223.

Doyle, J., Ge, W. and McVay, S. (2007b), "Accruals quality and internal control over financial reporting", *The Accounting Review*, Vol. 82 No. 5, pp. 1141-1170.

Felo, A.J., Krishnamurthy, S. and Solieri, S.A. (2003), "Audit committee characteristics and the perceived quality of financial reporting: an empirical analysis", Working Paper, PA State University, State University of New York, Binghamton, available at: http://ssrn.com/abstract=401240 (accessed 5 June 2014).

Financial Accounting Standards Board (FASB), (1999), *International Standard Setting: A Vision For The Future*, Norwalk.

Fox, C. and Zonneveld, P.A. (2003), *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting*, Rolling Meadows, IL.

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.

Gelinas, E.J., Schwarzkopf, D.L. and Thibodeau, J.C. (2008), "Introducing students to the integrated audit with Auditing Alchemy", *Journal of Information Systems*, Vol. 22 No. 2, pp. 151-170.

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.

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

Gupta, P.P. (2007), "Management's evaluation of internal controls under Section 404(a) using the COSO 1992 control framework: evidence from practice", *International Journal of Disclosure and Governance*, Vol. 5 No. 1, pp. 48-68.

Haislip, J.Z., Masli, A., Richardson, V.J. and Sanchez, J.M. (2011), "The impact of information technology material weaknesses on corporate governance: evidence from executive and director turnover, and IT governance changes", paper presented at University of Waterloo Symposium on Information Integrity and Information Systems Assurance", available at: http://jebcl.com/symposium/wp-content/uploads/2011/08/Impact-of-SOX-IT-Material-Weaknesses.pdf (accessed 13 May 2014).

Hogan, C. and Wilkins, M. (2005), "Do internal control weaknesses result in lower earnings quality? Implications and evidence from the audit risk model", Working Paper, Southern Methodist University.

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.

Information Systems Audit and Control Association (ISACA), (2006), *IT Control Objectives for Sarbanes-Oxley. The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, 2nd ed., ISACA, Rolling Meadows, IL.

Information Systems Audit and Control Association (ISACA), (2009), *Cobit and Application Controls. A Management Guide*, ISACA, Rolling Meadows, IL.

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.

International Accounting Standards Board (IASB), (2008), *Exposure Draft on an improved Conceptual Framework for Financial Reporting: The Objective of Financial Reporting and Qualitative Characteristics of Decision-useful Financial Reporting Information*, London.

IT Governance Institute (ITGI), (2005), *Control Objectives, Management Guidelines, Maturity Models in CobiT 4.0*, ITGI, 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.

Jara, E.G., Ebrero, A.C. and Zapata, R.E. (2011), "Effect of international financial reporting standards on financial information quality", *Journal of Financial Reporting & Accounting*, Vol. 9 No. 2, pp. 176-196.

Johnstone, K., Li, C. and Rupley, K. (2011), "Changes in corporate governance associated with the revelation of internal control material weaknesses and their subsequent remediation", *Contemporary Accounting Research*, Vol. 28 No. 1, pp. 331-383.

Jonas, G.J. and Blanchet, J. (2000), "Assessing quality of financial reporting", *Accounting Horizons*, Vol. 14 No. 3, pp. 353-363.

Kerr, D.S. and Murthy, U.S. (2013), "The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: an international survey", *Information & Management*, Vol. 50, pp. 590-597.

Kinney, W.R. (2000), "Research opportunities in internal control quality and quality assurance", *Auditing: A Journal of Practice & Theory*, Vol. 19 No. S1, pp. 83-90.

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.

Krishnan, J. (2005), "Audit committee quality and internal control: an empirical analysis", *The Accounting Review*, Vol. 80 No. 2, pp. 649-675.

Lainhart, J.W. (2000), "COBIT: a methodology for managing and controlling information and information technology risks and vulnerabilities", *Journal of Information Systems*, Vol. 14 No. 1, pp. 21-26.

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.

Lin, F., Guan, L. and Fang, W. (2010), "Critical factors affecting the evaluation of information control systems with the COBIT framework. A study of CPA firms in Taiwan", *Emerging Markets Finance & Trade*, Vol. 46 No. 1, pp. 42-55.

McDaniel, L., Martin, R. and Maines, L. (2002), "Evaluating financial reporting quality: the effects of financial expertise vs. financial literacy", *The Accounting Review*, Vol. 77, pp. 139-167.

Martin, K., Sanders, E. and Scalan, G. (2014), "The potential impact of COSO internal control integrated framework revision on internal audit structured SOX work programs", *Research in Accounting Regulation*, Vol. 26 No. 1, pp. 110-117.

Masli, A., Peters, G.F., Richardson, V.J. and Sanchez, J.M. (2010), "Examining the potential benefits of internal control monitoring technology", *The Accounting Review*, Vol. 85 No. 3, pp. 1001-1034.

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.

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.

Naciri, A. (2010), *Internal and External Aspects of Corporate Governance*, Routdlege, New York, NY.

O'Donnell, J.B. and Rechtman, Y. (2005), "Navigating the standards for information technology controls", *The CPA Journal*, Vol. 75 No. 7, pp. 64-69.

Pall, G.A. (1987), *Quality Press Management*, Prentice-Hall, Englewood Cliffs, NJ.

Power, M. (2009), "The risk management of nothing", *Accounting, Organizations and Society*, Vol. 34 Nos 6/7, pp. 849-855.

Protoviti (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 23 May 2014).

Public Company Accounting Oversight Board (PCAOB), (2004), *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements. Auditing Standard (AS) No. 2*, PCAOB, Washingotn, DC.

Raghunandan, K. and Rama, D.V. (2006), "SOX Section 404 material weakness disclosures and audit fees", *Auditing: A Journal of Practice & Theory*, Vol. 25 No. 1, pp. 99-114.

Ramos, M. (2004), "Evaluate the control environment", *Journal of Accountancy*, Vol. 197 No. 5, pp. 75-78.

Rose, J.M., Mazza, C.R., Norman, C.S. and Rose, A.M. (2013), "The influence of director stock ownership and board discussion transparency on financial reporting quality", *Accounting, Organizations and Society*, Vol. 38 No. 5, pp. 397-405.

Rozek, P. (2008), "Putting IT governance into action", *Internal Auditor*, Vol. 65 No. 3, pp. 29-31.

Rubino, M. and Vitolla, F. (2014a), "IT governance, risk management and internal control system: the role of the COBIT framework", in Tipurić, 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*, pp. 174-188.

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.

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

Sarens, G. and De Beelde, I. (2006), "Internal auditors' perception about their role in risk management. A comparison between US and Belgian companies", *Managerial Auditing Journal*, Vol. 21 No. 1, pp. 63-80.

Securities and Exchange Commission (SEC), (2002), *Certification of Disclosure in Companies' Quarterly and Annual Reports*, Securities and Exchange Commission, Washington, DC, available at: www.sec.gov/rules/final/33-8124.htm (accessed 20 February 2014).

Shaw, H. (2006), "The trouble with COSO", *CFO Magazine*, Vol. 22 No. 4, pp. 74-77.

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

Sowa, J.F. and Zachman, J.A. (1992), "Extending and formalizing the framework for information systems architecture", *IBM Systems Journal*, Vol. 31 No. 3, pp. 590-616.

Stoel, M.D. and Muhanna, W.A. (2011), "IT internal control weaknesses and firm performance: an organizational liability lens", *International Journal of Accounting Information Systems*, Vol. 12 No. 4, pp. 280-304.

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 Beest, F., Braam, G. and Boelens, S. (2009), "Quality of financial reporting: measuring qualitative characteristics", NiCE Working Paper 09-108, Radboud University Nijmegen.

Walters, L.M. (2007), "A draft of an information systems security and control course", *Journal of Information Systems*, Vol. 21 No. 1, pp. 123-148.

Wittenberg-Moerman, R. (2008), "The role of information asymmetry and financial reporting quality in debt trading: evidence from the secondary loan market", *Journal of Accounting and Economics*, Vol. 46 Nos 2/3, pp. 240-260.

Wixom, B.H. and Todd, P.A. (2005), "A theoretical integration of user satisfaction and technology acceptance", *Information Systems Research*, Vol. 16 No. 1, pp. 85-102.

Further reading

Chang, C.J. and Hwang, N-C.R. (2003), "Accounting education, firm training and information technology: a research note", *Accounting Education*, Vol. 12 No. 4, pp. 441-450.

Ettredge, M., Heintz, J., Li, C. and Scholz, S. (2011), "Auditor realignments accompanying implementation of SOX 404 reporting requirements", *Accounting Horizons*, Vol. 25 No. 1, pp. 17-39.

About the authors

Michele Rubino is Research Fellow at LUM Jean Monnet University, Department of Economics and Management – Casamassima (BA) – Italy. He got 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 Professor of accounting and corporate governance and internal control at the School of Management of the same University. His research interests are in the field of the internal control system, risk management and corporate social responsibility. Michele Rubino is the corresponding author and can be contacted at: rubino@lum.it

Filippo Vitolla is a Tenured Research of Business Administration at LUM Jean Monnet University, Casamassima (BA) – Italy. He took, 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, business strategy for the degree course in Business Administration and also in the Master provided at the School of Management. The research areas of his interest are: corporate social responsibility, management control systems and risk management. He has published several paper and books.