Journal of Information Systems and Technology Management – Jistem USP
Vol. 14, No. 3, Sep/Dec., 2017 pp. 361–370
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752017000300004

INTEGRATING INTERNAL CONTROL FRAMEWORKS FOR EFFECTIVE CORPORATE INFORMATION TECHNOLOGY GOVERNANCE

Abdou Ahmed Ettish https://orcid.org/0000-0002-4687-3240
Faculty of Commerce, Kafr El-Sheikh University, Egypt

Samir M. El-Gazzar
Rudolph A. Jacob
Lubin School of Business, Pace University, NY, USA

ABSTRACT

This paper analyzes and proposes how several internal control frameworks can be integrated to achieve effective corporate information technology governance. The fundamental tenet of the current literature in this area is that neither a single framework nor non-integrated multiple frameworks would suffice in achieving effective information technology security and governance. Using the extant literature, a deductive approach, and focusing on three popularized internal control frameworks ERM, COSO, and COBIT5, we propose a framework that can help organizations effectively and efficiently achieve information technology governance through their interaction. An integrated framework is one that links the key control objectives to strategic business objectives and, in doing so, addresses IT governance principles at both a strategic and operational level, whilst aligning IT and business management understanding of the key risk areas that characterize the organization's goals (Goosen and Rudman, 2013). In addition, this fundamental alignment is expected to eliminate unnecessary controls and processes which in turn help improving IT governance. We expect firms seeking to adopt the proper IT governance to utilize the proposed integrated framework.

Keywords: IT Governance, IT Risks, Integrated ITG Framework, Internal Control

Manuscript first received: 2017/Jul/11. Manuscript accepted: 2017/Nov/21

Address for correspondence:

Abdou Ahmed Ettish, Accounting Assistant Lecturer, Faculty of Commerce, Kafr El-Sheikh University, Egypt.
E-mail: ab_sh_er@yahoo.com

Samir M. El-Gazzar, KPMG Professor of Accounting, Lubin School of Business, Pace University, NY, USA.
E-mail: selgazzar@pace.edu

Rudolph A. Jacob, Professor and Graduate Chair of Accounting, Lubin School of Business, Pace University, NY, USA.
E-mail: rjacob@pace.edu.

INTRODUCTION

Information technology has become one of the most important strategic assets and a critical tool in ensuring the sustainability and development of a business. It is argued that the responsibility for designing, implementing and maintaining many of the controls over any organization's business processes is dependent on Information Technology (IT). The IT function is responsible for collecting, converting, archiving, protecting, processing, delivering and securely retrieving information as necessary (Abu-Musa, 2008). Many organizations have been using several frameworks such as Control of Objectives for Information and Related Technologies (COBIT), Enterprise Risk Management (ERM), and Committee of Sponsoring Organizations of the Treadway Commission (COSO). For optimal IT governance, we contend that organizations must integrate these frameworks. An integrated framework is one that links the key control objectives to strategic business objectives and, in doing so, addresses IT governance principles at both a strategic and operational level, whilst aligning IT and business management understanding of the key risk areas that characterize the organization's goals (Goosen and Rudman, 2013). In addition, this fundamental alignment is expected to eliminate unnecessary controls and processes which, in turn, helps in improving IT governance and regulatory compliance.

To achieve its strategic and operational goals, a firm needs timely and relevant information. As this need grows, corporations are expected to adopt well-integrated IT systems with other operational controls. These systems face different security risks that may arise from ineffective internal controls or the nature of the competitive environment as the demand for information increases (Abu-Khadra *et al*., 2012; Abu-Musa, 2006).

IT produces many opportunities for organizations to gain competitive advantages such as increased accuracy, speed of transaction processing, cost savings, improved operational efficiency, and reduction of human errors. It can also significantly increase productivity and enhance an organization's performance, thus adding value to the stakeholders. However, if an improper IT system is adopted, many negative consequences can affect the business. In fact, the Information Technology Governance Institute (ITGI 2003) expressed concern of the negative consequences of inadequate IT design, such as fraud, waste of computer assets, competitive disadvantage, privacy violation and incorrect record keeping.

Recently, the business paradigm has shifted to governance as an effective framework to enhance accountability, leadership, operational processes, organizational structures, and human resources of an organization through an alignment of IT with future business objectives and strategies (Yang *et al*., 2011; Peterson, 2004). Therefore, to achieve optimal IT governance, it is imperative that most organizations coordinate internal control frameworks, which may have been incipiently implemented on an *ad hoc* basis.

Based on our proposed integrated frameworks (ERM, COSO and COBIT), there are five domains that are expected to guide the design of IT governance: strategic alignment; value delivery; resource management; risk management; and performance measurement. The recommendations herein are applicable to medium- and large-sized companies that need to comply with regulatory requirements and are operating in complex, risky environments where an alignment of IT and business management objectives is a *sine qua non* for success.

RESEARCH PROBLEM

Currently organizations are utilizing more than one framework for management internal controls, IT, and information security. These frameworks such as ERM, COBIT, COSO, and ISO 27002 have been developed to assist firms in their planning of IT controls and the safeguarding of information assets (Lin *et al.,* 2012). However, recent research argues that applying these frameworks separately can lead to sub-optimization of an organization's strategic and operational goals. In fact, Trautman & Price (20ll) contend that corporations should adopt IT controls that fit with and support the Committee of Sponsoring Organization of Treadway Commission's (COSO) Internal Control-Integrated Framework. This research intends to develop a practical integration of corporate internal control frameworks to fill the gap in this area of information technology governance.

RESEARCH OBJECTIVE

This research aims at developing an integrated framework of COBIT5, ERM, and COSO for effective information technology governance (ITG). This effective integration entails a proper mapping of the corporate strategic and operational goals with those of IT.

LITERATURE REVIEW

Prior studies in this area can be classified under two main categories: importance of IT, and control frameworks.

A. Studies addressing the importance of IT governance

A number of the previous studies (Weil and Ross, 2004; KO and Fink, 20l0; Teo *et al*., 2013) discuss the importance of IT governance as an important critical factor for business success. These studies recommend not only the implementation of a broader corporate governance and the integration of the IT framework with other control frameworks, but also the adoption of best practices and standards associated with information technology governance to manage the risks linked with them.

B. Studies examining the relationship between internal control frameworks and IT governance

Other studies focus on the relationship between different internal controls frameworks and the successful implementation and adaption of IT governance (see, for example: Tuttle and Vandervelde, 2007; Robles *et al*., 2009; Abu-Musa, 2009; Eckert, 2012; Asgarkhani, 20l3). These studies state not only that COBIT is an effective control but also could be most effective if integrated with other internal control frameworks. In addition, integration between COBIT and other control frameworks would be consistent with COSO internal controls guidance.

The most commonly used frameworks that characterize many internal control and governance systems dealing with COBIT, ISO and ITIL are further documented in Violino, 2006; Nastase and Unchiasu, 2012; Goosen and Rudman, 2013. By and large, the fundamental tenet that emerges from this genre of early studies is that an organization ought to utilize more than one framework to manage its internal controls, IT, and information security system.

RESEARCH METHODOLOGY

This research uses the deductive approach to develop an integrated risk management framework to categorize a comprehensive list of threats and risks facing the organization. It also assesses these risks and ultimately identifies the appropriate responses for the prospected risks. This deductive approach utilizes the findings of prior studies and the underlying theory of corporate governance. An analytical diagnosis of the internal control frameworks and anecdotal corporate practices would portray the IT and governance landscape. Such a landscape would help in determining the interrelations, and any overlap and shortcomings of the overall framework. Under the proposed integrated internal control frameworks, a firm would be able to tailor the frameworks to fit its overall strategy and operational environment.

SCOPE OF THE RESEARCH

The scope of this paper is restricted to the COSO Report (issued in 1992 and revised in 2013) and the ERM that was introduced in 2004. Such frameworks now represent the most widely referenced models. But because they are highly condensed and do not identify the control objectives with the needed level of specificity, their effectiveness is somewhat limited (Rubino and Vitolla, 2014). Indeed, given this current scenario, the possibility of attaining optimal levels of effectiveness in IT governance is unlikely. Hence, the paper incorporates COBIT5 which provides a detailed set of prospect controls and checklists, thus making it possible to overcome these frameworks' weaknesses.

THE RELATIONSHIPS AMONG COBIT5, COSO REPORT AND ERM

The three frameworks are complementary and compatible in many aspects. Firstly, there are business requirements for information that must be satisfied in order to achieve the company objectives. As illustrated in Figure 1:

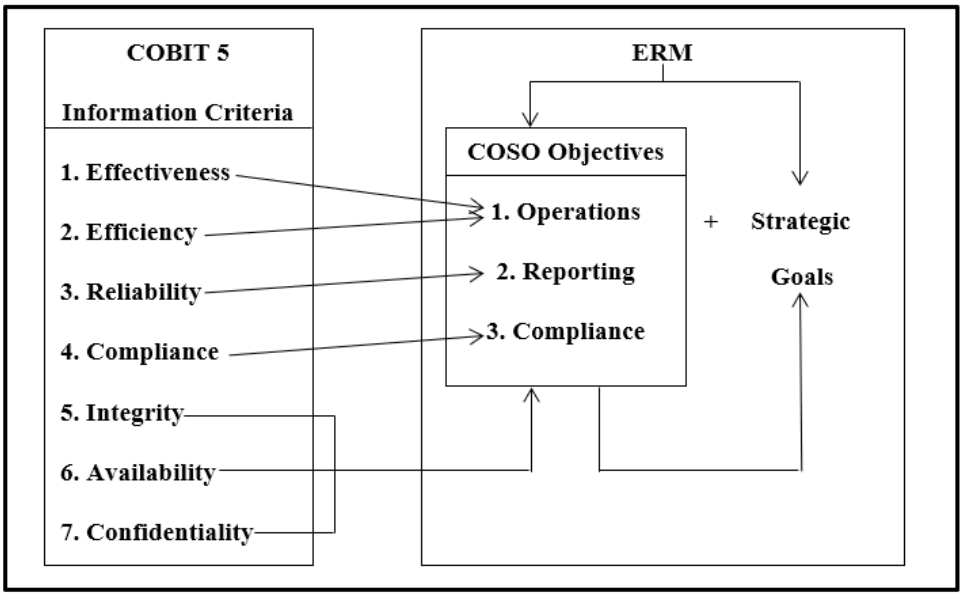

Figure 1. Interaction among COBIT5 information criteria, COSO, and ERM objectives
Source: Rubino and Vitolla (2014); adjusted by authors.

Figure 1 reveals that the first four information criteria correspond to the three objectives of COSO and ERM. The remaining information criteria are typical of the IT control models and assist in improving the quality of information, along with considering the main elements of information security. Thus, achieving these objectives will result in the organization achieving its strategic objectives.

Secondly, COBIT5 is based on 37 high-level control processes, which define and describe in detail a number of governance and management processes. It represents all of the processes that are normally found in an enterprise's IT activities. COBIT5 enumerates a clear difference between governance and management. According to ISACA (2012),

> "Governance ensures that stakeholder's needs; conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises governance is the responsibility of the board of directors."

ISACA (2012) further asserts that management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives, and the aforementioned activities are ultimately the responsibility of the executive management.

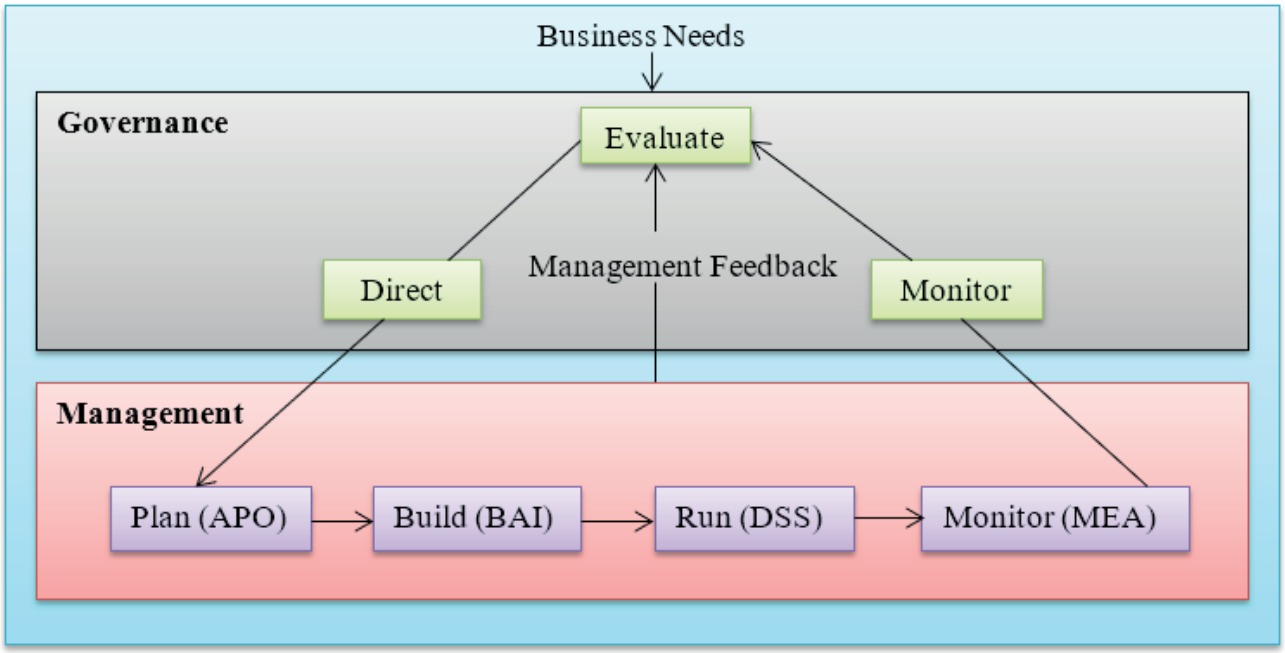

Figure 2. The difference between governance and management)
Source: (ISACA, 2012)

Figure 2 clearly depicts and differentiates the kinds of activities and different responsibilities of governance and management. The role of governance is to evaluate, direct and monitor (EDM). On the other hand, management encompasses four domains: align, plan and organize (APO); build, acquire and implement (BAI); deliver, service and support (DSS) and monitor, evaluate and assess

(MEA). The following table maps each of the high level processes of COBIT5 to the components and principles of COSO:

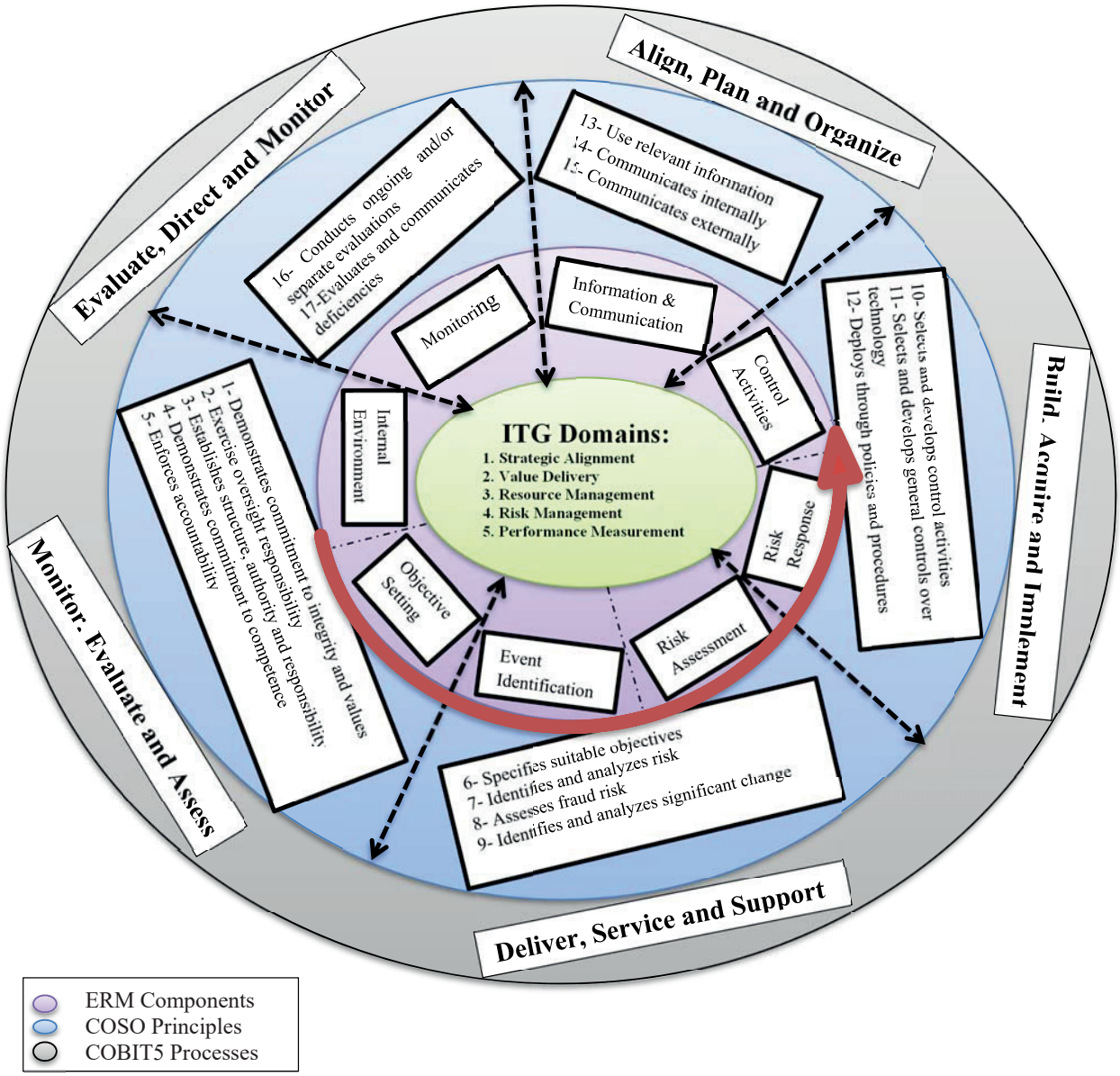

Figure 3. integration among the three frameworks

Based on Table 1, it is clear that the three frameworks are compatible and complementary to each other and there are many similar and different activities. Therefore, the integration among them will help organizations eschew a repeat of the design and application of many internal controls, thereby eliminating several non-value added activities. This results in cost reduction and competitive advantages through risk management and the alignment of the organization's strategic and operational goals with the objectives of information technology. Finally, Figure 3 illustrates the integration among the three frameworks:

Table 1. Mapping COBIT5 Processes with COSO Principles - ERM

	COBIT5 Processes		COSO Components and Principles- ERM																		
			Control Environment					Risk Assessment				Control Activities			Information & Communication			Monitoring Activities	
			Demonstrates commitment to integrity and ethical values	Exercises oversight of development and performance of internal control	Establishes structures, reporting lines , authorities and responsibilities	Demonstrates commitment to attract develop and retain competent individuals	Enforces accountability	Specifies suitable objectives	Identifies and analyzes risk	Assesses fraud risk	Identifies and analyzes significant change	Selects and develops control activities	Selects and develops general controls over technology	Deploys control activities through policies and procedures	Uses relevant information	Communicates internally	Communicates externally	Conducts ongoing and/or separate evaluations	Evaluates and communicates deficiencies
EDM	EDM 1	Ensure governance framework setting and maintenance	×	×	×	×	×											×	×
	EDM 2	Ensure benefits delivery			×										×	×	×	×	×
	EDM 3	Ensure risk optimization						×	×	×	×	×	×	×	×			×	×
	EDM 4	Ensure resource optimization				×	×					×	×	×	×	×	×	×	×
	EDM 5	Ensure stakeholder transparency	×		×		×								×	×	×	×	×
APO	APO 1	Manage the IT management framework			×			×	×	×	×	×	×	×	×	×		×	×
	APO 2	Manage strategy	×	×	×	×												×	×
	APO 3	Manage enterprise architecture	×		×	×						×	×	×	×	×		×	×
	APO 4	Manage innovation							×		×	×	×	×	×	×		×	
	APO 5	Manage portfolio										×	×	×	×	×		×	×
	APO 6	Manage budget and costs				×	×	×	×	×	×	×	×	×	×	×		×	×
	APO 7	Manage human resources	×		×	×	×			×		×			×	×	×	×	
	APO 8	Manage relationships	×		×	×	×	×	×	×	×				×	×	×	×	×
	APO 9	Manage service agreements				×						×	×	×	×			×	×
	APO 10	Manage suppliers							×		×				×	×	×	×	×
	APO 11	Manage quality				×		×	×	×		×	×	×	×	×	×	×	×
	APO 12	Manage risk						×	×	×	×	×	×	×	×	×	×	×	×
	APO 13	Manage security										×	×	×	×	×		×	×

Table 1. Cont.

	COBIT5 Processes		COSO Components and Principles- ERM																
			Control Environment					Risk Assessment				Control Activities				Information & Communication			Monitoring Activities	
			Demonstrates commitment to integrity and ethical values	Exercises oversight of development and performance of internal control	Establishes structures, reporting lines , authorities and responsibilities	Demonstrates commitment to attract develop and retain competent individuals	Enforces accountability	Specifies suitable objectives	Identifies and analyzes risk	Assesses fraud risk	Identifies and analyzes significant change	Selects and develops control activities	Selects and develops general controls over technology	Deploys control activities through policies and procedures	Uses relevant information	Communicates internally	Communicates externally	Conducts ongoing and/or separate evaluations	Evaluates and communicates deficiencies
BAI	BAI 1	Manage programs and projects					×	×	×	×	×	×	×	×	×	×		×	×
	BAI 2	Manage requirements definition						×	×		×				×	×			
	BAI 3	Manage solutions identification and build						×	×	×	×	×	×	×	×	×		×	
	BAI 4	Manage availability and capacity			×	×									×	×		×	×
	BAI 5	Manage organizational change enablement	×		×	×					×	×	×	×	×	×		×	
	BAI 6	Manage changes	×		×			×	×		×	×	×	×	×	×		×	
	BAI 7	Manage change acceptance and transitioning.	×					×	×		×	×	×	×	×	×		×	×
	BAI 8	Manage knowledge	×			×									×	×	×	×	×
	BAI 9	Manage assets			×	×	×	×	×	×	×	×	×	×	×	×		×	
	BAI 10	Manage configuration	×		×	×	×	×	×	×	×	×	×					×	
DSS	DSS 1	Manage operations	×	×	×	×	×	×	×	×	×	×	×	×	×	×		×	×
	DSS 2	Manage service requests and incidents						×	×	×	×	×	×	×	×	×		×	×
	DSS 3	Manage problems						×	×	×	×				×	×		×	×
	DSS 4	Manage continuity						×	×	×	×	×	×	×	×	×		×	
	DSS 5	Manage security services						×	×	×	×	×	×	×	×	×		×	×
	DSS 6	Manage business process controls	×	×	×	×	×	×	×	×	×	×	×	×	×	×		×	×
MEA	MEA 1	Monitor, evaluate and assess performance and conformance						×	×	×	×	×	×	×	×	×		×	×
	MEA 2	Monitor, evaluate and assess the system of internal control						×	×	×	×	×	×	×	×	×		×	×
	MEA 3	Monitor, evaluate and assess compliance with external requirements						×	×	×	×	×	×	×	×		×	×	×

Source: Based on COSO principles (2013) and COBIT5 processes (ISACA, 2012).

As revealed in Figure 3, IT governance focuses on generating and communicating relevant information for decision making in five domains: Strategic Alignment, which is responsible for ensuring alignment of IT operations and goals with the organization's strategic objectives and arranging projects depending on the strategic goals of the organization; Value Delivery that ensures IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value; Resource Management that concentrates on the optimal use of investments and on suitable management of the crucial IT resources; Risk Management which identifies the organization's risk appetite, the compliance requirements, assess, determine the appropriate responses and report on the opportunities and threats that affect the achievement of the organization objectives; and Performance Measurement which follows up the achievement of the strategies, the advancement of projects, the consumption of resources, the delivery and the support services performance (Silva and Neto, 2014; Jairak and Praneetpolgrang, 2013; Kepczyk, 2013).

From the diagram above, ERM, COSO and COBIT5 frameworks have been integrated to provide information on enterprise risk management procedures and identify the interrelationships between enterprise risk management and internal control and the safeguarding of information assets.

CONCLUSION

Using the extant literature in corporate governance and information technology risks and governance, we develop an integrated framework that aligns the corporate strategic and operational controls and processes of ERM, COSO, and COBIT5 with IT governance principles. Based on these operational controls, we portray that IT governance is influenced by five corporate domains. These domains include (but not limited to) IT: strategic alignment; value delivery, resource management; risk management; and performance measurement. Coordinating these domains along with IT controls should lead to the appropriate IT governance structure.

Moreover, this integrated framework not only will allow business and IT management to address the organization's significant IT and strategic risks but also would promote goal congruence between IT and business management, as they strive to maximize shareholders' wealth. This framework also is expected to enhance regulatory compliance. Under our unified framework, it is expected that corporations, in adopting the proper IT governance, will utilize the proposed structural relationships between ERM, COSO, and COBIT5.

REFERENCES

Abu-Khadra, H. A., Chan, J. O. & Pavelka, D. D. (2012). Incorporating the COBIT Framework for IT Governance in Accounting Education, *Communications of the IIMA***,** *12*(2), 81-92.

Abu-Musa, A. A. (2006). Evaluating the Security Controls of CAIS in Saudi organizations: The Case of Saudi Arabia. *The International Journal of Digital Accounting Research*, *6*(11), 25-64.

Abu-Musa, A. A. (2008). Exploring the importance and implementation of COBIT processes in Saudi organizations an empirical study. *Information Management & Computer* Security, *17*(2), 73-95.

Abu-Musa, A. A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study. *The International Journal of Digital Accounting Research*, *9*, 99-126.

Asgarkhani, M. (2013). Corporate ICT Governance: A Tool for ICT Best Practice. *The International Conference on Management*, *Leadership & Governance***,** 1-7.

COSO. (2004). Enterprise Risk Management Integrated Framework. 1-7. http://www.aicpa.org.

COSO. (2013). Internal Control-Integrated Framework, Executive Summary. 5, 1-20. http://*www.coso.org.*

Eckert, C. (2012). COBIT Changes Focus on IT Risk Management. *Pennsylvania CPA Journal*, *83*(2), 8.

Goosen, R. & Rudman, R. (2013). An Integrated Framework to Implement IT Governance Principles at a Strategic and Operational Level for Medium-To Large Sized South African Businesses. *International Business & Economics Research Journal*, 12(7), 835 - 854.

IT Governance Institute. (2003). Board Briefing on IT Governance. 2nd ed. http://www.itgi.org.

ISACA. (2012). COBIT 5 a Business Framework for the Governance and Management of Enterprise IT. http://www.isaca.org.

Jairak, K. & Praneetpolgrang, P. (2013). Applying IT governance balanced scorecard and importance-performance analysis for providing IT governance strategy in university. *Information Management & Computer Security*, *21*(4), 228-249.

Kepczyk, R. H. (2013). IT Governance With in Accounting Firms. *CPA Practice Management Forum*, 9-10.

KO, D. & Fink, D. (2010). Information technology governance: an evaluation of the theory-practice gap. *Corporate Governance*, *10*(5), 662- 674.

Lin, H., Cefaratti, M., & Wallace, L. (2012). Enterprise Risk Management, COBIT, and ISO 27002: A Conceptual Analysis. *Internal Auditing*, *27*(2), 3-12.

Nastase, P. & Unchiasu, S. F. (2012). Assessment of the It Governance Perception within the Romanian Business Environment. *Accounting and Management Information Systems*, *11*(1), 44-55.

Peterson, R. (2004). Crafting Information Technology Governance. *EDPACS*, *32*(6), 1-23.

Robles, R. J., Choi, M., Cho, S., Lee, Y., & Kim, T. (2009). SOX and its effects on IT Security Governance. *International Journal of Smart Home, 3*(1), 81-88.

Rubino, M., & Vitolla, F. (2014). IT governance, Risk Management and Internal Control System: the role of the COBIT framework. *International OFEL Conference on Governance, Management and Entrepreneurship*, 174-188.

Silva, L. M., & Neto, J. S. (2014). Method for Measuring the Alignment between Information Technology Strategic Planning and Actions of Information Technology Governance. *Journal of Information Systems and Technology Management*, *11*(1), 131-152.

Teo, W. L., Manaf, A. A., & Choong, P. L. (2013). Information Technology Governance: Applying the Theory of Planned Behavior. *Journal of Organizational Management Studies*, *9*, 1-15.

Trautman, L., & Price, K. Al., (2011). The Board's Responsibility for Information Technology Governance. *The John Marshall Journal of Computer & Information Law*, *28* (3), 312-342.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of COBIT as an internal Control framework for information technology. *International Journal of Accounting information systems***,** *8* (4), 240-263.

Violino, B. (2006). Sorting the Standards. *Computer World*, *40* (16), 46-57.

Weill, P., & Ross, J. W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. *Massachusetts Institute of Technology*, USA. http://www.sqs.com

Yang, M., Lin, W., & Koo, T. (2011). The impact of computerized internal controls adaptation on operating performance. *African Journal of Business Management*, *5* (20), 8204-8214.