Volume 7
Number 1
2012

ISSN: 1935-8156

http://www.aisej.com

Integrating IT Frameworks into the AIS Course

Jing Qian
University of Nebraska at Omaha
Kerry Ward
University of Nebraska at Omaha
Jennifer Blaskovich
University of Nebraska at Omaha

Published by the AIS Educator Association
http://www.aiseducators.com

AIS Educator Journal

Published by the AIS Educator Association

Conference Chair & President: **Ron Premuroso, University of Montana**

Vice President : **Kathryn Klose, University of Maryland University College**

Training Chair: **Constance "Conni" Lehmann, University of Houston, Clear Lake**

Research Chair: **Gary Schneider, Quinnipiac University**

Integrating IT Frameworks into the AIS Course

Volume 7, Number 1
2012
page 1-26

Jing Qian
University of Nebraska at Omaha, jqian@unomaha.edu, tel. 917-831-8118
Kerry Ward
University of Nebraska at Omaha, kward@unomaha.edu, tel. 402-554-3369
Jennifer Blaskovich
University of Nebraska at Omaha, jblaskovich@unomaha.edu, tel. 402-554-3984

ABSTRACT

The contemporary business and regulatory environment dictate that accountants develop greater expertise in information technology, particularly in its risk and control aspects. Several approaches exist to assist with these aspects of information technology, with the primary ones being COSO ERM, COBIT, ITIL, and the ISMS family of standards, each developed by different groups with different objectives. While accounting students likely receive training in COSO ERM and COBIT, exposure to ITIL and the ISMS family is less common. This paper is motivated from the view that all four approaches are vital to the accountant's professional toolbox and should be incorporated into the AIS course. In this paper, we provide AIS instructors with a concise overview of the four approaches and offer an integrated framework that can guide teaching plans. We discuss how the approaches should not be viewed as separate and redundant bureaucratic models, but as complementary approaches that help an organization manage risks and controls.

Keywords
IT Frameworks, COBIT, ERM, ITIL, ISMS, AIS Education, AIS Course

INTRODUCTION

Information technology (IT) has evolved into an essential infrastructure for organizations: an infrastructure that is the foundation for enterprise risk management and internal control. This infrastructure has taken on an even greater importance with regulations such as the Sarbanes-Oxley Act (SOX), which requires an increased level of assurance in the quality of corporate information. Accordingly, it is critical that organizations develop and maintain effective risk management practices and controls over the system that produces this information. Several approaches exist to assist with the risk and control aspects of the IT infrastructure. Four established approaches[1] include the Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management-Integrated Framework* (COSO ERM), Control Objectives for Information Related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and the Information Security Management System (ISMS) family of standards[2], each developed by different groups with different objectives.

Our primary objective in this paper is to encourage the inclusion of all four approaches in accounting information systems (AIS) courses in order to provide exposure to IT risk and control frameworks. Researchers and practitioners alike suggest that the evolution of business and the increasingly demanding regulatory environment dictate that accountants possess greater knowledge of IT (Cegielski 2008). O'Donnell and Moore (2005, 65) cite deficiencies in the accounting curriculum for a shortage of accountants and auditors proficient in information systems/information technology (IS/IT) "control knowledge, or competencies." Indeed, our examination of the most common textbooks in AIS indicates that most of the textbooks introduce COSO ERM and COBIT, but contain little or no coverage of ITIL or the ISMS family. Accounting students must likely venture into the IS/IT department to access meaningful coverage of ITIL and the ISMS family.

In this paper, we develop an integrated framework to present these four approaches and discuss how they can be viewed not as separate and redundant bureaucratic models, but as complementary approaches that help an organization manage IT risks and controls. We hope to provide AIS instructors with a concise overview of four approaches to IT risks and controls that have been developed and utilized in both disciplines, and offer an integrated framework that can guide teaching plans. Our goal is to expose students to these accepted IT approaches, develop some understanding of their purposes and uses, and thus provide a basis for further study and development.

We begin by providing our rationale for including this topic in AIS courses, and then we introduce the four approaches. We next discuss how these approaches differ from and complement each other and present our integrated framework. The final section offers some concluding remarks.

---

[1] See, for example, Huang et al. 2011; Turner and Weickgenannt 2009; Vaassen et al. 2009; Sahibudin 2008; Schlarman 2007; Tuttle and Vandervelde 2007; Wendle 2007; Hill and Turbitt 2006; Panko 2006; Symons 2005; von Solms 2005.

[2] The ISMS family is also known as the ISO/IEC 27000 series. Previous versions of the ISMS family have been codified into the 27000 series (i.e., ISO 17799 has been renamed 27002). In this paper, we refer to the 27000 series because it is the most current.

BACKGROUND

The primary objective of an AIS is to originate, capture, process, store, and distribute information for decision-making (Hurt 2010). Although AIS existed long before computers (Hall 2011), one would be hard-pressed to find a company that does not rely on IT to achieve this objective. Today, documents are electronic, transactions are automated, and paper trails are non-existent (Coe 2006; Helms and Mancino 1998). Traditional financial accounting practices such as fixed asset valuation and impairment have been changed by process automation, web services architecture, and Internet-based supply chain management (Ho et al. 2008). Business reorganization resulting from enterprise system adoption requires cost reallocation and business process redesign (Ho et al. 2008; Kinney 2000). In sum, IT has revolutionized contemporary business—a reality that creates new expectations of the accounting profession.

As the demands on the profession have expanded with IT, so have the demands on education. In 1995, the International Federation of Accountants (IFAC) stated that IT "requires special attention due to its explosive growth and its rapid rate of change" (IFAC 1995, 1-2). Their 2001 exposure draft again addressed the pervasiveness of IT in business and reiterated, "Competence with this technology is an imperative for the professional accountant" (IFAC 2001, 6). The need for accounting students to develop IT control knowledge was further defined in IFAC's 2003 and 2007 education papers and statements (IFAC 2003; 2007). Similarly, other researchers, educators, and professional organizations have called for teaching efforts directed towards IT risk and control concepts (Coe 2006; American Accounting Association 2003; Kinney 2001; Albrecht and Sack 2000). Clearly, the need for a quality IT education for accountants remains a relevant issue.

Keeping pace with the increasing complexity of IT and the demands of contemporary business requires some convergence of the accounting and IT disciplines (Walters 2007). Prior researchers have addressed the relationship between the AIS and IS/IT curriculum, (e.g., Murthy and Ragland 2009; Sutton and Arnold 2002; Sutton 1992), often debating whether AIS is in danger of being subsumed by IS/IT. We do not propose a further blurring of the disciplines, but rather propose that IT risk and control frameworks represent one area where accounting students can benefit from exposure to IT concepts. We offer several reasons for this position.

First, the impact of IT on internal controls cannot be overstated, and internal controls are critical to virtually all accounting specializations. It is nearly impossible to successfully develop or audit internal controls and financial reports without understanding the computer-based information system (Cegielski 2008). SOX redoubles the importance of controls over the AIS and IT infrastructure (Walters 2007), where management's responsibility for internal controls (Section 404) and the accuracy of financial report information (Section 302) are explicitly identified. Given that the reliability of financial information is dependent on an organization's IT (Fox and Zonneveld 2003), competence in IT is a requisite condition for SOX compliance (Walters 2007). Accounting professionals, whether they are managerial accountants who must embed controls or auditors who must evaluate them, clearly require knowledge of IT controls to meet regulatory demands (Ho et al. 2008).

Second, and relatedly, SOX compliance "requires an integrated evaluation of automated, IT-dependent, and manual controls in relation to each other" (Chan 2004a, 33). Accountants must possess a combination of knowledge in accounting, internal controls, and IT to effectively

complete this integrated evaluation (Kay and Ovlia 2012). The accounting program of study is ideally suited to provide this instruction. Murthy and Ragland (2009) indicate that comprehensive teaching of internal controls remains firmly in the domain of AIS courses, thereby representing a unique value-added skill for accountants.

Third, a recent survey of Big 4 firms suggests that they actively recruit students who possess an educational background in both accounting and information systems (Cegielski 2008). Unfortunately, audit firms have accepted "that the traditional education model for professional accountancy offered by many colleges and universities around the nation is inadequate to address the current demands within the profession for technology-based knowledge and skills" (Cegielski 2008, 34). Addressing this deficiency seems imperative if accounting education is to remain relevant.

Finally, accountants play critical roles in organizational IT, far beyond the responsibilities of internal control assessment, compliance, and financial reporting. For example, because IT is fundamental to company performance (Hermanson et al. 2000), accountants can help organizations use it to develop competitive advantages. Accountants are often called upon to direct strategic planning and capital budgeting activities for investments in IT systems (Hermanson et al. 2000; IFAC 1995), while at the same time dealing with the resulting organizational restructuring and business process redesign (Kinney 2000). Also, as traditional boundaries are relaxed and procedures reconfigured, controllers and internal and external auditors must assess and manage the organization-wide risks that IT has introduced (Hermanson et al. 2000). Accountants must now be concerned with many aspects of IT, including proper governance and service performance in addition to risks and controls.

Recognizing this need, and to address the call for increased exposure to IT concepts, we propose that the study of risks and controls in AIS be complemented with an introduction to risk and control approaches rooted in the IS/IT discipline. Specifically, we suggest students should be exposed to COSO ERM, COBIT, ITIL, and the ISMS family of standards. These four approaches have been recognized in research and practice as established, reliable, and valid (e.g., Huang et al. 2011; Vaassen et al. 2009; Sahibudin 2008; Schlarman 2007; Tuttle and Vandervelde 2007; Wendle 2007; Hill and Turbitt 2006; Symons 2005; von Solms 2005). While none are sufficiently comprehensive to meet IT risk and control objectives on their own (Sahibudin 2008; Schlarman 2007; Hill and Turbitt 2006), presenting them together provides a comprehensive approach to IT risk and control.

Others have recognized the need to integrate these approaches in order to achieve IT control objectives. Sahibudin et al. (2008), Schlarman (2007), and ITGI et al. (2005) suggest the use of COBIT, ITIL, and the ISMS family; Huang et al. (2011) and Chan (2004b) discuss COSO ERM and COBIT; Hill and Turbitt (2006) couple COBIT and ITIL; and von Solms (2005) maps COBIT and the ISMS family. All but one (Huang et al. 2011) of these publications are aimed at managers, and none link all four approaches. We add to this literature by presenting an integrated framework of all four approaches for AIS instructors to use in their courses.

We use COSO ERM as the starting point for our integrated framework because it provides a high-level focus on risk and control. An integrated framework for accountants is not complete without COSO ERM since "risk and control are virtually inseparable – like two sides of a coin – meaning that risks first must be identified and assessed; then managed and mitigated by the implementation of a strong system of internal control" (IIA 2003, 1). COSO ERM provides the highest-level approach for identifying and assessing enterprise-wide risks, including IT. COBIT then offers high level guidance for governing the IT infrastructure. Finally, for de-

tailed IT processes, ITIL and the ISMS family cover specific areas of concern and provide the how (Hill and Turbitt 2006; von Solms 2005).

In sum, we propose that instruction on all four approaches and their complementarities provides our students with an introduction to the IT concepts expected in today's technology-dependent business environment. The accountants and auditors of tomorrow are expected to possess knowledge and awareness of IT-related issues, including security, controls, and risks. While COSO ERM and COBIT provide some guidance for meeting these expectations, ITIL and the ISMS family are important approaches in the IS/IT discipline. The integration of these four approaches form a hierarchy of guidelines for meeting IT risk and control objectives.[3] We expand on this discussion in the Comparison and Complementarities section of this paper.

Instruction on the integrated framework is appropriate for either undergraduate or graduate students. While COSO ERM and COBIT both appear to have established a foothold in the standard undergraduate AIS course, coverage of ITIL and the ISMS family appears scarce. Our examination of AIS textbooks offered by the major publishers indicates that most cover COSO ERM and COBIT, while ITIL and ISMS receive very little, if any, coverage (see Appendix 1 for a list of textbooks examined). However, ITIL and ISMS, along with COBIT, are consistently recognized as the most widely-used IT approaches (e.g., Schlarman 2007; Vaassen et al. 2009; ITGI et al. 2005). Either level of student can benefit from exposure to the widely-used IT control approaches and gain some recognition of their potential use as an integrated hierarchy of guidelines. Basic learning objectives include the following:

1. To become aware of commonly used approaches for IT risk and control.
2. To recognize the governing bodies that created each approach.
3. To understand the primary purpose of each approach.
4. To understand how the different approaches can be used together by focusing on the common elements.

Instructors wishing to offer greater coverage of the approaches may use Internet-available documents provided by the governing bodies of each approach.

In the following sub-sections, we provide a brief narrative overview of the four approaches. We offer a more detailed summarization of the primary components of each in Tables 1 through 4. We then compare and describe the complementarities between the approaches and introduce our mapping diagram.

OVERVIEW OF THE APPROACHES

COSO ERM

In the early nineties, leading professional accounting and finance associations[4] collaborated to create COSO. This committee develops and disseminates frameworks and guidance on

[3] Other frameworks related to internal controls and IT exist i.e., Turnbull, Trust Services, and CMMI. We did not include these for various reasons, such as that their concepts are addressed in one of our selected frameworks (i.e., Turnbull), they have not established wide-spread use or acceptance (i.e., Trust Services), or their focus is extremely narrow and specific (i.e., CMMI).

ERM, internal controls, and fraud deterrence. In the aftermath of the financial scandals of the early 2000s and consequent stakeholder demands for improved corporate governance, the committee released *ERM-Integrated Framework* (COSO 2004). The key purpose of this now widely -used framework (Power 2007) is to integrate various concepts and viewpoints of risk management into a framework that provides a common definition and understanding of enterprise-wide risk management.

COSO's previous publication, *Internal Control-Integrated Framework* (COSO IC), remains a well-accepted standard for satisfying SOX compliance needs, and is not replaced by COSO ERM (COSO 2004). However, COSO ERM incorporates the COSO IC framework within it, and expands on it to provide a broader and more robust focus on enterprise-wide risk management (COSO 2004). There is growing recognition that compliance with SOX necessitates an integrated focus on risk management and internal control (IFAC 2011). COSO suggests that companies may use COSO ERM "both to satisfy their internal control needs and to move toward a fuller risk management program" (COSO 2004, v). We include COSO ERM in this paper precisely because it provides the risk management focus to our integrated framework.

The COSO ERM framework consists of eight interrelated components that are derived from the way a business is run and integrated with the management process. These components start at the highest abstract level, the internal environment, and move down to the level of policies and procedures, with a continuous monitoring process to ensure the framework is being properly employed. Each is briefly described below and summarized in Table 1.

The first component is the internal environment. The internal environment is a high-level perspective of risk and provides the basic structure and discipline of how risk and control are viewed and addressed by the organization's employees. It is the tone of the organization, including management philosophy, integrity and ethical values, and risk appetite. The second component of COSO ERM is objective setting, including high-level strategic objectives, operational objectives, reporting objectives, and compliance objectives. In objective setting, it is important to establish objectives that are consistent with the entity's philosophy and risk appetite reflected in the internal environment.

Once the objectives have been determined, the third step is to identify any potential events that might have an impact on the organization's ability to achieve their objectives. The identified threats should be categorized based on management's understanding and identification of interrelationships among the events in order to form a basis for risk assessment and an enhanced common risk language across the entity. The fourth component of COSO is to assess and analyze the identified risks based on their likelihood of occurrence and the magnitude the events would have on organizational objectives if they do occur. The fifth component is for management to plan appropriate responses to the assessed risks. The primary categories of risk responses include the choice to avoid, accept, reduce, or share the risk.

Control activities represent the sixth component. The aim of control activities, especially on information, is to provide assurance that the selected risk responses will be effectively carried out. The seventh component is information and communication. Internal and external pertinent information used for identifying, assessing and responding to risks should be sourced, identified, captured, analyzed, processed, reported, and communicated at each level of an entity

[4] Associations include the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants .

in a form that enables people to carry out their responsibilities. This challenge can be met via clear and effective communication by an established information systems infrastructure. Finally, the enterprise risk management process must be monitored on an ongoing basis by assessing the functioning of its components and the quality of performance over time, with corrective modifications made as necessary.

While the COSO ERM framework presents an integrated procedure for enterprise risk management, it does not directly address IS/IT. However, IS/IT is used to support risk responses and to ensure smooth communication throughout the organization. Within COSO ERM, IS/IT control is introduced at a high level. The requirement for more detailed IS/IT control objectives and related control activities leads us to the next approach, COBIT.

TABLE 1
Summary of COSO ERM Components

COSO ERM Component	Description
Internal Environment	This represents a high-level perspective of risk and provides the basic structure and discipline of how risk and control are viewed and addressed by the organization's employees.
Objective Setting	This includes high-level strategic objectives, operational objectives, reporting objectives, and compliance objectives. In objective setting, it is important to establish objectives that are consistent with the entity's philosophy and risk appetite reflected in the internal environment.
Event Identification	This identifies any potential events that might have an impact on the organization's ability to achieve their objectives. Events should be categorized based on the interrelationships among them in order to form a basis for risk assessment and an enhanced common risk language across the entity from a portfolio perspective.
Risk Assessment	This assesses and analyzes the identified risks based on their likelihood of occurrence and magnitude the events would have on organizational objects if they do occur.
Risk Response	This plans appropriate responses to the assessed risks. The primary categories of risk responses include the choice to avoid, accept, reduce, or share the risk.
Control Activities	This refers to policies, procedures, and activities to ensure that the selected risk responses will be effectively carried out.
Information and Communication	Internal and external information used for identifying, assessing and responding to risks should be sourced, identified, captured, analyzed, processed, reported, and communicated at each level of an entity in a form that enables people to carry out their responsibilities.
Monitoring	The ERM process must be monitored on an ongoing basis, by assessing the functioning of its components and the quality of performance over time, with corrective modifications made as necessary.

COBIT

In 1993, the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA) created COBIT as an internal control approach for IT. Since then, COBIT has become an internationally accepted standard for the control and governance of IT (Lainhart 2000). The COBIT control approach is designed for achieving business objectives. It covers the full range of IT activities. COBIT addresses IT concerns such as IT decision-making, controls, and maintenance. It ensures that the IT systems which perform data movement, transformation, and storage, are secure, and it acts as an umbrella IT governance approach, helping manage the risks and benefits associated with IT (ITGI 2007).

The COBIT approach has four main characteristics: it is business-focused, process-oriented, controls-based, and measurement-driven. Aspects of COBIT's business orientation include the linking of IT goals to business goals, providing metrics to measure their alignment, and identifying the associated responsibilities and ownership of IT processes.

The underlying principle of COBIT is that IT resources (applications, information, infrastructure, and people) are managed by IT processes, are based on control objectives, and are monitored using metrics to deliver information and achieve IT goals that respond to the business requirements for information and governance. The process approach of COBIT subdivides IT into four domains in line with the responsibilities of planning, building, running, and monitoring (See Table 2 for a summary). These domains map to 34 corresponding processes, each of which is a high-level control objective, essentially following a systems development lifecycle (Panko 2006).

TABLE 2
Summary of COBIT Domains

COBIT Domain	Description
Plan and Organize (PO)	This domain covers strategic and tactical levels and provides direction to solution delivery (AI) and service delivery (DS). The PO domain mainly identifies the way IT can best contribute to the achievement of business objectives. Additionally, it addresses whether IT objectives and IT risks are understood, communicated and managed throughout the organization and whether the enterprise optimizes its use of IT resources.
Acquire and Implement (AI)	This domain covers the controls needed to identify, develop (or acquire), implement, and integrate IT solutions and turn those solutions into services. In addition to developing the new solutions, this domain includes the maintenance of or changes in the existing systems to make sure business objectives continue to be met.
Deliver and Support (DS)	This domain is concerned with service delivery and service support for users, security and continuity management, data management, and operational facilities management. Here the solutions are received and made usable for end users.
Monitor and Evaluate (ME)	This domain monitors all IT processes and evaluates their quality over time to ensure that the direction provided is followed and that the processes comply with control requirements. It mainly pertains to internal control monitoring, performance management, and regulatory compliance and governance.

ITIL

ITIL was initially developed in the late 1980s by a branch of the British Government referred to as the Office of Government Commerce (OGC). The original objectives of ITIL were to improve IT services, increase IT business effectiveness, and reduce costs (Laurent 2005). The focus of ITIL is on IT service management (ITSM) and alignment of IT with the business (Hill and Turbit 2006). ITIL can be viewed as an approach of best practices for managing IT services. It is currently going through its third revision to reframe service management as a lifecycle, extending the approach by focusing on the service lifecycle of design, transition, and operation. ITIL describes how to organize and implement IT service management. This approach provides standards that are designed to show goals, activities, inputs and outputs of a variety of processes incorporated within IT organizations. Additionally, the ITIL approach provides a clearly structured context in which to evaluate existing methods and activities so that companies can meet or anticipate customers' needs (OGC 2010). While ITIL is not directly related to IT risk management, its support for IT service quality indirectly impacts organizational and IT-related risks. ITIL practices address system performance, problem resolution, and security, which are all critical issues in risk management (Worthen 2005). The latest version of the ITIL approach, v3, is separated into five service areas based on the service lifecycle (See Table 3).

TABLE 3
Summary of ITIL Service Areas

ITIL Service Area	Description
Service Strategy	This area is designed to focus the service lifecycle of IT on customer outcomes and services as the foundation for the other core lifecycle service areas. Aligning IT with the business is a key function of the service strategy.
Service Design	This area provides guidance on the design of the services and solutions that make up the IT infrastructure. Specifically the focus of this area is on all aspects of the design process including IT policy and documentation. The goal is to design innovative solutions that meet not only current needs but also future requirements.
Service Transition	This area seeks to reduce risks and maximize the benefits of the system by focusing on the release, delivery and deployment processes.
Service Operation	This area covers delivery and control activities related to day-to-day operational issues. Consideration is given to forward-looking aspects and medium- to long-term planning, which subsequently has an impact on the quality of IT services. The goal for service operation is continuous delivery of high quality IT services during daily operations.
Continual Service Improvement	This area focuses on identifying and implementing service improvements on an ongoing basis to maintain best practices. It also includes processes for dealing with service retirement.

The ISMS Family of Standards

Under the auspices of the World Trade Organization, the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) develop international standards related to topics with a technical component. The ISO is a network of representatives from 161 countries designed to develop standards that cross national boundaries. The IEC is a similar organization focusing on the development of international standards for electrical, electronic, and related technologies. The ISO and the IEC are jointly developing a series of standards, frequently identified as the ISMS family of standards (also referred to as the ISO/IEC 27000 series), to establish and maintain an effective information security management system (ISMS) that supports business objectives (ISO/IEC 2009). The ISO/IEC views the use of the ISMS family as an approach for managing the security of information assets and as a standard for supporting the independent assessment of information security. The ISMS family is categorized into four structural and interrelated components, each containing one or more standards. The four categorized components and corresponding standards consist of terminology (standard no. 27000), general/normative requirements (standards nos. 27001, 27006), general/informative guidelines (standards nos. 27002 – 27005, 27007), and sector-specific guidelines (standards nos. 27011, 27799) (See Table 4 for a summary).

COMPARISON AND COMPLEMENTARITIES

Having presented an overview of each approach, we compare the approaches via Table 5. This section also discusses how the four approaches complement each other. All of the four approaches are business-oriented and independent of organizational structures, architectures, or technologies, which allows them to be implemented in most organizations. These approaches can be integrated to form a comprehensive approach to IS/IT risk and control with COBIT nested within the control aspects of the COSO ERM framework, ITIL nested within the processes of the COBIT approach, and the ISMS family contributing to the information security risk objectives of COSO ERM and COBIT.

The integration of COSO ERM, COBIT, ITIL and the ISMS family of standards is summarized and illustrated using Figure 1. [5] Figure 1 represents both a top down and bottom up analysis of the four frameworks. First, the conceptual aspects of the four frameworks were integrated. For example, COSO is an organization-wide approach to risk management, while COBIT focuses on information technology. Thus, the integration begins with the establishment of business goals enabled by a continuously improving IS infrastructure that is supported by the best practices. These conceptual level relationships were used to lay out the overall diagram. Next, the basic concepts of each framework (e.g. "control activities," "monitor and evaluate") were examined to determine how the individual concepts fit together within the overall conceptual diagram. These conceptual relationships are explored in more details in the following section.

After we mapped the concepts of all the frameworks, we examined each framework from the bottom up. Each framework provides practitioners with detailed guidance on how to imple-

[5] For the ISMS family of standards, we only introduce ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005 into this mapping diagram, as all the other ISO/IEC 27k standards are either under development or not related to the theme of this paper.

TABLE 4
Summary of the ISMS Family of Standards

ISO/IEC Standard	Description
27000	27000 is an introduction and overview document that includes the vocabulary and other basic information for understanding the family of standards.
27001	27001 specifies the general requirements for establishing, implementing, maintaining and improving an information security management system to achieve business objectives, thereby acting as the 'core' of the ISMS family of standards. 27001 promotes a process approach to information security based on a Plan-Do-Check-Act (PDCA) cycle for all of the associated processes. 27001 therefore lays out the high level PDCA cycle for the ISMS: establish the ISMS (Plan), implement and operate the ISMS (Do), monitor and review the ISMS (Check), and maintain and improve the ISMS (Act). Included in 27001 is Annex A, which provides a list of controls and control objectives directly derived from the guidance in 27002, which is discussed next.
27002	27002 is the most significant part of the 27000 series of documents. It is a code of practice that provides extensive coverage of information security, including processes and controls. The initial sections focus on general, non-IT related information security such as asset management, human resources security, and physical and environmental security. The later sections focus on information system security including access control, information systems acquisition, development and maintenance, and information security incident management. 27002 lays out 39 information security control objectives together with hundreds of related best-practice control measures to assure the confidentiality, integrity, and availability of information assets. These controls are generic in the sense that they can be customized to accommodate various types of organizations. 27002 does not mandate any suggested controls but allows the organizations to identify, select, and implement the most suitable controls for their business. The flexibility of 27002 allows it to be applied even in the context of changing technology and security risks. The controls and objectives identified in 27002 are designed to support the outcomes of the risk assessment outlined in 27005.
27003	Still under development; this is an implementation guide to assist organizations that are new adopters of the 27000 family in setting up an information security management system.
27004	Still under development; it focuses on metrics to measure the effectiveness of an information security management system.
27005	27005 addresses information security risk management. A systematic approach is presented that addresses all aspects of information security risk management including assessment, treatment, acceptance, and communication. This standard promotes a continuous process of risk management via monitoring and review.
27011 and 27799	Still under development; these are adaptations of 27002 specifically applicable to unique industry sectors.

ment the frameworks. The detailed guidance was examined and mapped from a bottom-up perspective to the conceptual diagram in Figure 1. The support for Figure 1, including the detailed mapping, is provided in the Appendices.

Note that in Figure 1, we use abbreviations to replace full names, making the figure more concise and easier to follow. The counterpoint between abbreviation and full name for Figure 1 is outlined in Appendix 2. Also, Figure 1 is based on our assessment of the quantity of mapping areas among these frameworks (See Appendices 3-5). The number of mapping areas represents the extent to which a certain component of one framework maps with a certain domain or section of another framework.

COSO ERM and COBIT

COBIT complements COSO ERM in two main ways: as a mechanism for aligning IT with enterprise objectives, and as detailed support for IT controls. After establishing the internal environment, the COSO ERM framework promotes the development of business goals built on the enterprise's philosophical approach to risk. COBIT supports these business goals by establishing policies, processes, and procedures for the overall IT infrastructure that promote the alignment of IT with business goals. COSO ERM establishes the business objectives COBIT uses to drive alignment of IT governance with the organization.

The second aspect of complementarity between COSO ERM and COBIT is in development of detailed internal controls. COSO ERM and COBIT differ in the depth of control coverage due to their different purposes and domains. COSO ERM's focus on enterprise risk management necessitates strong internal controls to ensure the accuracy of data and to provide controls for financial processes and accounting procedures. COSO ERM falls short, however, in providing detailed functional area guidance for establishing this strong internal control environment. This is an area where COBIT can be of value.

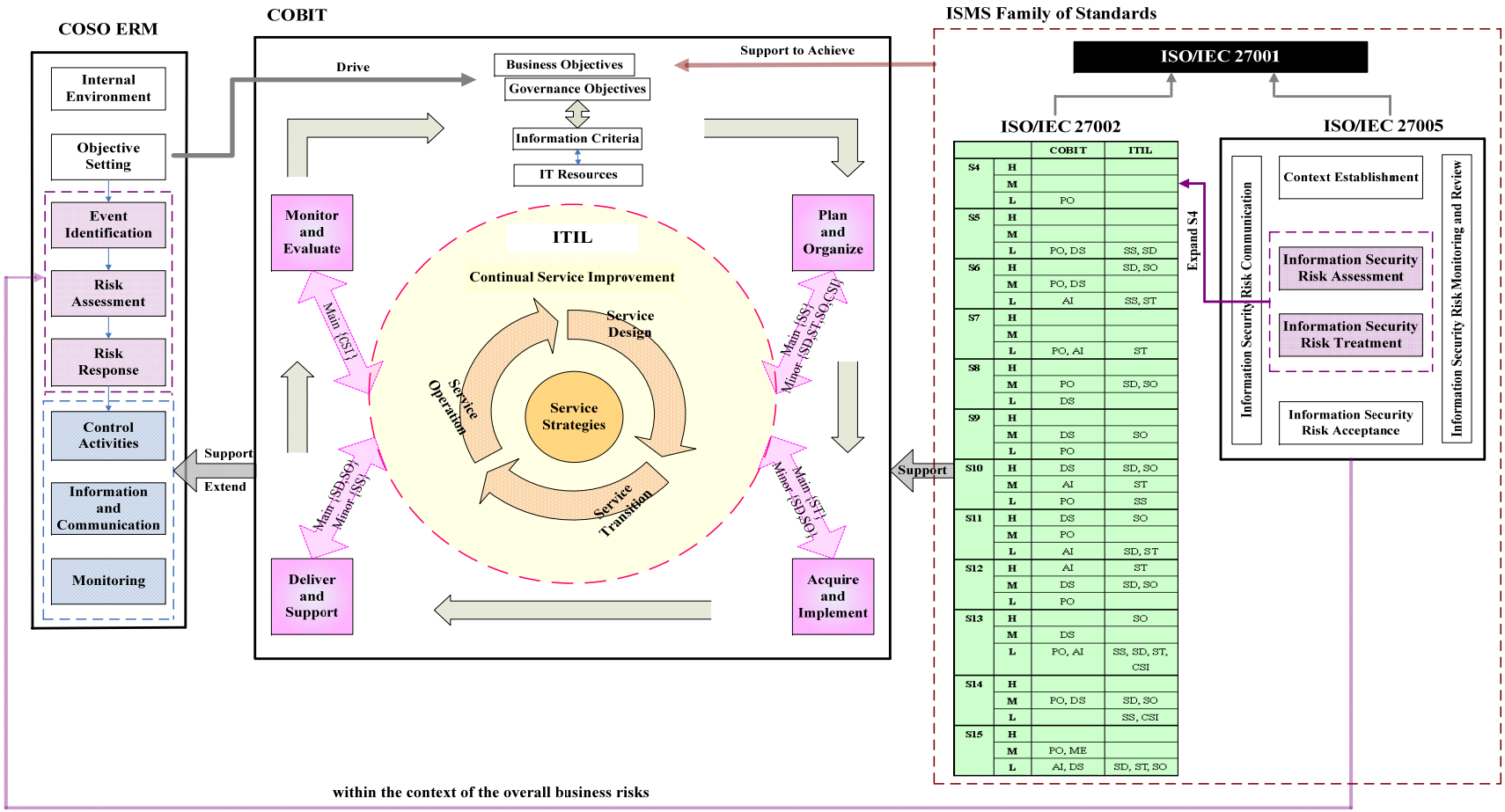
COBIT covers arguably the most important foundation of the creation and movement of financial information in the organization: the information systems technology infrastructure. It acts as an umbrella IT governance approach and can fulfill the COSO ERM requirements for the IT control environment. COBIT is an approach for control over IT "that fits with and supports" COSO ERM (ITGI 2007, 5). One way to think about this is to view COSO ERM as the generally-accepted enterprise internal control framework, while viewing COBIT as the generally-accepted IT internal control approach (ITGI 2007, 7).

A more detailed analysis reveals that COBIT supports and extends COSO ERM's components of Control Activities, Information and Communication, and Monitoring. COBIT addresses the high-level IT governance and overall control aspects of IT, aligning IT with business requirements. It also aids in implementing a control system for improved regulatory compliance and improves the quality and measurability of IT governance across the entire life cycle of application implementation. COBIT further supports COSO ERM by reducing IT-related risks and by increasing the quality of information.

Integrating ITIL

ITIL complements the role of COBIT by further supporting IT service management, including continuously improving IT customer service quality and IT operations efficiency. As such, ITIL largely complements COSO ERM via COBIT and in the same two aspects as CO-

Figure 1
Mapping Diagram of
COSO ERM, COBIT, ITIL and ISMS



		COBIT	ITIL
S4	H		
	M		
	L	PO	
S5	H		
	M		
	L	PO, DS	SS, SD
S6	H		SD, SO
	M	PO, DS	
	L	AI	SS, ST
S7	H		
	M		
	L	PO, AI	ST
S8	H		
	M	PO	SD, SO
	L	DS	
S9	H		
	M	DS	SO
	L	PO	
S10	H	DS	SD, SO
	M	AI	ST
	L	PO	SS
S11	H	DS	SO
	M	PO	
	L	AI	SD, ST
S12	H	AI	ST
	M	DS	SD, SO
	L	PO	
S13	H		SO
	M	DS	
	L	PO, AI	SS, SD, ST, CSI
S14	H		
	M	PO, DS	SD, SO
	L		SS, CSI
S15	H		
	M	PO, ME	
	L	AI, DS	SD, ST, SO

TABLE 5
Summarized Comparison Among COSO ERM, COBIT, ISMS, and ITIL

MODEL	COSO-ERM	COBIT	ISMS Family	ITIL
Created by	Leading Accounting Organizations including AICPA.	IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA)	Joint development by the International Standards Organization and the International Electrotechnical Commission (ISO/IEC). Some of the standards were initially created by the British Standards Institute (BSI) e.g, 27002, 27005.	British Government's Office of Government Commerce (OGC)
Purpose	To enable and facilitate management's ability to address enterprise risks, to prevent fraudulent reporting through stronger internal controls.	To maximize the business value of IT via effective IT governance and controls on all IT processes across the implementation lifecycle of IT	To facilitate management's ability to protect confidentiality, integrity and availability of enterprise information assets	To improve IT services, increase business effectiveness, and reduce costs by optimizing service management
Domain	Entire Enterprise	Information Technology	Enterprise Information Security	Information Technology
Focus	Enterprise Risk Management	IT Governance	Information Security Management Systems	IT Service Management
Framework	An integrated enterprise risk management approach with eight components	A process model subdivided into four domains and 34 IT processes	A series of standards for information security classified into four categories	A lifecycle model containing five components concerning IT service management
Complementary Aspects	N/A	Complementary to COSO ERM by: (a) promoting strategic IT alignment with business goals (b) Supporting and extending controls on IT (c) Improving regulatory and audit compliance (d) Enhancing risk management	Complementary to COSO ERM and COBIT by: (a) supporting enterprise risk management (b) Extending controls especially on information security	Complementary to COSO ERM and COBIT by: (a) promoting IT alignment with business (b) Strengthening IT controls (c) Providing best practices for IT service processes.

BIT: IT alignment with business and IT controls. First, ITIL impacts both the IT strategy and the organizational structure, thus impacting IT alignment. ITIL focuses on business value through the management of IT services and is designed for continuous process improvement. It is by providing better IT services to the business that ITIL promotes alignment of IT with the business (Kashanchi and Toland 2006).

Second, ITIL's process approach complements COBIT's control focus. Although COBIT is process-oriented, its focus is on control and audit functions. Therefore, COBIT is viewed as a control approach. This control focus makes COBIT normative, addressing the processes necessary to meet the needs for control and audit. ITIL, alternatively, can be viewed as a process approach that focuses on prescriptive processes for IT service management. This can be seen in the description of each approach. COBIT documentation refers to COBIT as "good" practice (ITGI 2007), underlying the point that COBIT is focusing on process control, not prescriptive performance-oriented processes. ITIL, on the other hand, discusses "best" practices and is oriented towards performance and continuous improvement. Thus, using COBIT and ITIL not only optimizes the maturity of IT controls, but also promotes the use of best practice processes for better alignment and performance.

Looking deeper into the complementarity of control, ITIL provides more details to COBIT's control objectives in the area of IT service management. This is similar to how COBIT provides more details on IT control than COSO ERM. In particular, ITIL focuses on optimizing operations management by providing definitions together with functional, operational, and organizational criteria for operations management. ITIL especially extends and deepens two of COBIT's four domains, the Acquire and Implement and the Deliver and Support domains, through its Service Transition, Service Design, and Service Operation areas.

While in general, ITIL can be thought of as addressing a subset of COBIT, COBIT complements ITIL by providing an environment for implementing ITIL. The high-level process control model of COBIT molds the ITIL processes to the business needs, ensuring a successful ITIL implementation and further supporting alignment with business goals. COBIT also provides a control checklist against defined IT processes as an effective mechanism for measuring and managing progress and improvement in implementing ITIL processes. The result is an improvement to internal control and improvement to the organization's ability to manage enterprise risks, the underlying purpose of COSO ERM.

Integrating the ISMS Family of Standards

Similar to COBIT, the ISMS family complements COSO ERM by supporting risk management and by providing detailed control support. First, the focus on information security risk management of ISO/IEC 27005 directly supports the risk management aspect of COSO ERM by focusing on risks that could impact information, including financial information. This is consistent with SOX and the intent of COSO ERM. Second, the controls of the code of practice in ISO/IEC standard no. 27002 [6] support the need for controls suggested in COSO ERM. The ISMS controls cover information security on an enterprise-wide basis and are not as focused on the IT domain as are COBIT and ITIL. For example, sections 5 through 9 of ISO/IEC 27002 cover enterprise physical or human resources security management, while sections 10 to 15 cover various aspects about information security.

[6] These controls are also presented in Annex A of ISO/IEC standard no. 27001.

Although we find similarities and support between the two, COBIT and the ISMS family do differ. First, the ISMS family of standards focuses on an enterprise-wide approach to information security while COBIT, as its names implies, focuses on the IT domain. COBIT addresses the alignment of IT with the organization and performance of IT, while ISMS family of standards focuses on information security via the creation of an information security management system. For example, the scope of such a system is the confidentiality, integrity, and availability (CIA) of information, a traditional information security approach. COBIT addresses CIA but also addresses the effectiveness and efficiency of information as it supports organizational goals. The information security management system is supportive of COBIT, but using solely the ISMS family does not support all of the objectives COBIT covers.

In considering how the ISMS family complements the other models, it is important to note that the ISMS family of standards is international while the others are not: COSO ERM and COBIT are U.S.-centric while ITIL is British. Further, the use of the term "standard" is significant. COBIT as a methodology helps an organization meet its compliance needs and improves the organization's IT performance. Implementing the ISMS family of standards alternatively allows an organization to be certified as compliant with the standard, which is independent of any other audit or compliance needs.

Summary

Because COSO ERM, COBIT, ITIL, and the ISMS family of standards are developed for different purposes and possess distinct focuses and features, they are in essence more complementary to each other than competitive. Their focuses on different levels allow them to be integrated: COSO ERM addresses enterprise-level risk management and controls, COBIT addresses the IT domain, ITIL addresses IT service management, and the ISMS family of standards addresses information security management. The IT governance and control focus of COBIT directly supports the control needs of COSO ERM, and the IT service focus of ITIL supports the process controls of COBIT. Using both COBIT and ITIL assists in the alignment of IT with business objectives. Also, different components of COSO ERM, COBIT and ITIL can be further strengthened and enriched by different components of the ISMS family, with different supportive levels from an information security perspective.

CONCLUSION

The importance of information and the systems that supply this information to contemporary business is undeniable. Increasingly complex and sophisticated information technology that underlies these systems offers greater benefits, but also introduces greater risks. Effective risk management and control over the information system is therefore critical to an organization. In this paper, we have provided an overview of four approaches—COSO ERM, COBIT, ITIL, and the ISMS family—that addresses the risk and control issues surrounding information systems and technology. We propose that these four approaches are not redundant, but rather are complementary models that assist organizations in managing IT risk and controls. To this end, we offer an integrated framework to highlight the complementarities and suggest ways in which the four approaches can be used in concert. Because the accounting and auditing function bears significant responsibility for risk management and control, it is imperative that ac-

countants understand these established approaches. However, two approaches important in the IS/IT discipline, the ISMS family and ITIL, appear largely absent from accounting education.

An accounting student today cannot become a successful, value-adding professional tomorrow without a solid foundation in both accounting and IT. If the primary characteristics of useful information are relevance and faithful representation (FASB 2010), and this information is supplied by an IT system, it must follow that accountants need skills and expertise in IT risk and control to ensure information usefulness. Although one might argue that accounting students can gain this knowledge in IT courses, they would likely miss the complementary aspects that are so important to comprehensive risk management and control. We encourage inclusion of the four approaches in AIS courses by providing a concise overview of each and by offering an integrated framework that can be used to introduce the approaches and to guide teaching plans. This knowledge, we believe, is essential to the success of our students in their future accounting careers.

REFERENCES

Albrecht, W.S., and R.J. Sack. 2000. *Accounting Education: Charting the Course Through a Perilous Future*. Sarasota, FL: American Accounting Association.

American Accounting Association. 2003. 2000-2001 Auditing section education committee challenges to audit education for the 21st century: A survey of curricula, course content, and delivery methods. *Issues in Accounting Education* 18 (3): 241-263.

Cegielski, C.G. 2008. Toward the development of an interdisciplinary information assurance curriculum: Knowledge domains and skill. *Decision Sciences Journal of Innovative Education* 6 (1): 29-49.

Chan, S. 2004a. Sarbanes-Oxley: The IT dimension. *Internal Auditor* 61 (1): 31-33.

Chan, S. 2004b. Mapping COSO and CobiT for Sarbanes-Oxley compliance. *IT Audit – The Institute of Internal Auditors* (October 1).

Coe, M.J. 2006. Integrating IT audit into the AIS course. *The Review of Business Information Systems* 10 (1): 105-119.

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

Financial Accounting Standards Board (FASB). 2010. *Conceptual Framework for Financial Reporting*. Statement of Financial Accounting Concepts No. 8. Stamford, CT: FASB.

Fox, C., and P.A. Zonneveld. 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: IT

Governance Institute. Available at: www.itgi.org.

Hall, J.A. 2011. *Accounting Information Systems, 7e*. Mason, OH: Cengage Learning.

Helms, G.L., and J. Mancino. 1998. The electronic auditor – wave goodbye to the paper trail. *Journal of Accountancy* (April): 45-48.

Hermanson, D.R, M.C. Hill, and D.M. Ivancevich. 2000. Information technology-related activities of internal auditors. *Journal of Information Systems* 14 (Supplement): 39-53.

Hill, P., and K. Turbitt. 2006 *Combine ITIL and COBIT to Meet Business Challenges.* Retrieved September 18, 2009, from http://documents.bmc.com/products/documents/17/09/61709/61709.pdf

Ho, S.Y., G. Pan, and C. Ferguson. 2008. The information systems – accounting nexus: Lessons from an Australian Institution. *Communications of the Association for Information Systems* 22 (February): 197-210.

Huang, S-M., W-H. Hung, D.C. Yen, I-C. Chang, and D. Jiang. 2011. Building the evaluation model of the IT general controls for CPAs under enterprise risk management. *Decision Support Systems* 50: 692-701.

Hurt, R.L. 2010. *Accounting Information Systems, 2e*. New York, NY: McGraw-Hill/Irwin.

Institute of Internal Auditors (IIA). 2003. Managing risk from the mailroom to the boardroom. *The Tone at the Top* 18 (June).

International Federation of Accountants (IFAC). 1995. Guideline 11, *Information Technology in the Accounting Curriculum.* New York, NY: IFAC.

International Federation of Accountants (IFAC). 2001. Exposure Draft IEG-11. *IFAC Education Committee Guideline 11*. New York, NY: IFAC.

International Federation of Accountants (IFAC). 2003. International Education Paper 2. *Towards Competent Professional Accountants*. New York, NY: IFAC.

International Federation of Accountants (IFAC). 2007. *International Education Practice Statement 2: Information Technology for Professional Accountants.* New York, NY: IFAC.

International Federation of Accountants (IFAC) 2011. *Global Survey on Risk Management and Internal Control*. New York, NY: IFAC.

International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). 2009. *Information technology – Security techniques – Information Security Man-*

agement Systems – Overview and Vocabulary. Geneva, Switzerland: ISO/IEC.

IT Governance Institute (ITGI). 2007. *COBIT 4.1 Executive Summary and Framework.* Rolling Meadows, IL: IT Governance Institute.

IT Governance Institute (ITGI), Office of Government Commerce (OGC), and IT Service Management Forum (ITSMF). 2005. *Aligning COBIT, ITIL, and ISO 17799 for Business Benefit: Management Summary.* Rolling Meadows, IL: IT Governance Institute and Norfolk, UK: Office of Government Commerce.

Kashanchi, R., and J. Toland. 2006. Can ITIL contribute to IT/business alignment? *Informatik* 48 (5): 340-348.

Kay, D., and A. Ovlia. 2012. *Accounting Information Systems, 1e*. Upper Saddle River, NJ:Prentice Hall.

Kinney, Jr. W.R. 2000. Research opportunities in internal control quality and quality assurance. *Auditing: A Journal of Practice and Theory* 19 (Supplement): 83-90.

Kinney, Jr., W.R. 2001. Accounting scholarship: What is uniquely ours? *The Accounting Review* 76 (2): 275-284.

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

Laurent, M.K. 2005. *Getting In-Control - Combining CobiT® and ITIL® for IT Governance and Process Excellence.* Retrieved September 18, 2009, from http://www.itmanagementonline.com/Resources/Articles/Getting_In-Control_-_Combining_CobiT_and%20ITIL_for_IT_Governance_and_Process_Excellence.pdf

Murthy, U.S., and L. Ragland. 2009. Towards an understanding of accounting information systems as a discipline: A comparative analysis of topical coverage in AIS and MIS courses. *AIS Educator Journal* 4 (1): 1-15.

O'Donnell, J. and J. Moore. 2005. Are accounting programs providing fundamental IT control knowledge? *The CPA Journal* 75 (5): 64-66.

Office of Government Commerce (OGC). 2010. *Information Technology Infrastructure Library*. Retrieved September 23, 2010. http://www.ogc.gov.uk/guidance_itil.asp.

Panko, R. 2006. Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks. *Communications of AIS* 17: 2-50.

Power, M. 2007. The risk management of everything. *The Journal of Risk Finance* 5 (3): 57-

64.

Sahibudin, S., M. Sharifi, and M. Ayat. 2008. Combining ITIL, COBIT, and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations, *Proceedings of the Second Asia International Conference on Modelling & Simulation*, IEEE Computer Society.

Schlarman, S. 2007. Selecting an IT control framework. *Information Systems Security* 16: 147-151.

Sutton, S. 1992. Can we research a field we cannot define? Toward an understanding of the AIS discipline. *Advances in Accounting Information Systems* 1: 1-13.

Sutton, S., and V. Arnold. 2002. Foundations and frameworks for AIS research. In *Researching Accounting as an Information Systems Discipline*. Arnold, V. and Sutton, S. (Eds.), American Accounting Association.

Symons, C. 2005. IT Governance Framework. Forrester Research Group, Retrieved September 16, 2010, from http://www.cba.co.nz/download/Forr051103656300.pdf

Turner, L., and A. Weickgenannt. 2009. *Accounting Information Systems: Controls and Processes, 1e*. West Sussex, UK: John Wiley & Sons.

Tuttle, B., and S.D. Vandervelde. 2007. An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems* 8: 240-263.

Vaassen, E., R. Meuwissin, and C. Schelleman. 2009. *Accounting Information Systems and Internal Control, 2e.* West Sussex, UK: John Wiley & Sons.

Von Solms, B. 2005. Information security governance: COBIT or ISO 17799 or both? *Computers & Security* 24: 99-104.

Walters, L.M. 2007. A draft of an information systems security and control course. *Journal of Information Systems* 21(1): 123-148.

Wendle, K. 2007. Top ten things the CIO needs to know about ITIL now. *CIO Magazine*. Retrieved September 16, 2010, from http://advice.cio.com/kewendle/top_ten_things_the_cio_needs_to_know_about_itil_now

Worthen, B. 2005. IT Governance – ITIL Power. *CIO Magazine*. Retrieved September 16, 2010, from http://www.cio.com/article/10522/IT_GOVERNANCE_ITIL_Power

APPENDIX 1
Coverage of the Four Approaches in Current AIS Textbooks

Author(s), Title, Publisher	COSO -ERM	COBIT	ITIL	ISMS Family
Bagranoff, Simkin, & Norman (2010) *Core Concepts of Accounting Information Systems, 11e*. John Wiley & Sons.	a	a		b
Bodnar & Hopwood (2010) *Accounting Information Systems, 10e.* Prentice Hall.	a	a		a
Gelinas, Dull & Wheeler (2012) *Accounting Information Systems, 9e.* Cengage Learning	a	a		
Hall (2011) *Accounting Information Systems, 7e*. Cengage Learning.				
Heagy & Lehman (2011) *Accounting Information Systems: A Practitioner Emphasis 7e*. Cengage Learning.	a	a		
Hurt (2010) *Accounting Information Systems, 2e.* McGraw-Hill/Irwin.	a	a		
Kay & Ovlia (2012) *Accounting Information Systems: The Crossroads of Accounting and IT, 1e.* Prentice Hall.	a	a		
Romney & Steinbart (2012) *Accounting Information Systems 12e*. Prentice Hall.	a	a		
Turner & Weickgenannt. 2009. *Accounting Information Systems: Controls and Processes, 1e*. John Wiley & Sons.	a	a	b	b
Vaassen, Meuwissin, & Schelleman (2009) *Accounting Information Systems and Internal Control, 2e.* John Wiley & Sons.	a	b	b	b

(a) Textbook presents, at a minimum, basic information about the background, objectives, purpose, and/or uses of the approach.
(b) Textbook recognizes the existence of the approach, but does not provide additional information about it such as background, objectives, purpose, and/or uses of the approach.

APPENDIX 2
Abbreviations

Note: In Figure 1, we use abbreviations to replace full names, making the mapping diagram more concise and easier to follow. The counterpoint between abbreviation and full name for Figure 1 is outlined here.

Abbreviation	Full Name
H	Highly supportive
M	Moderately supportive
L	Lowly supportive
COBIT	
PO	Plan and Organize
AI	Acquire and Implement
DS	Deliver and Support
ME	Monitor and Evaluate
ITIL	
SS	Service Strategies
SD	Service Design
ST	Service Transition
SO	Service Operation
CSI	Continual Service Improvement
ISO/IEC 27002	
S4	Section 4 - Risk assessment and treatment
S5	Section 5 - Security policy
S6	Section 6 - Organization of information security
S7	Section 7 - Asset management
S8	Section 8 - Human resources security
S9	Section 9 - Physical and environmental security
S10	Section 10 - Communications and operations management
S11	Section 11 - Access control
S12	Section 12 - Information systems acquisition, development and maintenance
S13	Section 13 - Information security incident management
S14	Section 14 - Business continuity management
S15	Section 15 - Compliance

APPENDIX 3
Mapping ITIL and ISO/IEC 27002 with COBIT 4.1 Control Objectives

COBIT	ITIL				ISO/IEC 27002			
		Best Support	*Minor Support*	*Subtotal*		*Best Support*	*Minor Support*	*Subtotal*
Plan and Organize (PO)	SS	49 (*)	23	72	S5	2	7	9
					S6	6	28	34
	SD	19	32	51	S7	1	4	5
					S8	5	23	28
	ST	10	19	29	S9	2	2	4
					S10	3	8	11
	SO	16	5	21	S11	6	3	9
					S12	2	0	2
	CSI	26	3	29	S13	2	2	4
					S14	5	2	7
					S15	9	2	11
Acquire and Implement (AI)	SS	2	1	3	S6	1	5	6
					S7	1	0	1
	SD	20	16	36	S8	0	2	2
					S9	0	2	2
	ST	59	21	80	S10	3	16	19
					S11	1	2	3
	SO	17	2	19	S12	10	24	34
					S13	1	1	2
	CSI	0	0	0	S15	3	0	3
Deliver and Support (DS)	SS	23	0	23	S5	4	0	4
					S6	17	7	24
	SD	69	11	80	S7	0	5	5
					S8	8	3	11
	ST	7	0	7	S9	20	3	23
					S10	27	21	48
	SO	54	21	75	S11	41	1	42
					S12	9	8	17
	CSI	6	1	7	S13	7	11	18
					S14	7	9	16
					S15	5	4	9
Monitor and Evaluate (ME)	SS	0	4	4	S5	0	5	5
	SD	3	2	5	S6	1	6	7
	ST	4	0	4	S10	0	7	7
	SO	1	0	1	S15	3	15	18
	CSI	20	5	25				

Note:
[1] The numbers in this table represent the quantity of mapping areas by which a certain component of ITIL or ISO/IEC 27002 provides support to COBIT control objectives of a certain domain. For example, (*) represents that there are 49 mapping areas by which SS of ITIL provides best support to COBIT control objectives of PO domain.
[2] Though the subtotal mapping areas equal the quantity of best support areas plus that of minor support areas, the subtotal is just a reference to build the mapping diagram, since the quantity of best support areas has higher weight than minor support areas.

APPENDIX 4
Mapping COBIT 4.1 Control Objectives with ITIL

ITIL	COBIT
SS	PO (90) > DS (41) > ME (4) = AI (3)
SD	DS (107) > PO (46) > AI (32) > ME (6)
ST	AI (85) > PO (30) > DS (14) > ME (2)
SO	DS (78) > PO (30) > AI (24) > ME (2)
CSI	PO (34) > ME (21) > DS (12) > AI (3)

Note:
[1] Appendix 4 further verifies the content of Appendix 3 from a reverse perspective.
[2] The numbers in Appendix 4 reflect the extent to which a certain component of ITIL maps with COBIT control objectives of a certain domain.

NOTES TO ACCOMPANY APPENDIX 5
(Next Page)

Note:
[1] Appendix 5 also verifies and extends the content of Appendix 3 reverse.
[2] The numbers in Appendix 5 mainly represent the extent to which a certain component of COBIT or ITIL maps with a certain section of ISO/IEC 27002.

APPENDIX 5
Mapping COBIT 4.1 Control Objectives and ITIL with ISO/IEC 27002

ISO/IEC 27002	COBIT		ITIL	
Section 4 Risk Assessment and Treatment	PO	1		
Section 5 Security Policy	PO	9	SS	6
	AI	0	SD	6
	DS	4	ST	2
	ME	5	SO	3
			CSI	0
Section 6 Organization of Information Security	PO	34	SS	19
	AI	6	SD	51
	DS	24	ST	19
	ME	7	SO	60
			CSI	4
Section 7 Asset Management	PO	5	SS	1
	AI	1	SD	4
	DS	4	ST	14
	ME	0	SO	4
			CSI	0
Section 8 Human Resources Security	PO	28	SS	6
	AI	2	SD	29
	DS	11	ST	6
	ME	0	SO	29
			CSI	4
Section 9 Physical and Environmental Security	PO	4	SS	0
	AI	2	SD	0
	DS	23	ST	0
	ME	0	SO	36
			CSI	0
Section 10 Communications and Operations Management	PO	11	SS	16
	AI	19	SD	67
	DS	50	ST	46
	ME	7	SO	48
			CSI	8
Section 11 Access Control	PO	9	SS	0
	AI	3	SD	12
	DS	45	ST	5
	ME	0	SO	85
			CSI	0
Section 12 Information Systems Acquisition, Development and Maintenance	PO	2	SS	3
	AI	34	SD	25
	DS	17	ST	71
	ME	0	SO	38
			CSI	0
Section 13 Information Security Incident Management	PO	4	SS	4
	AI	2	SD	10
	DS	18	ST	5
	ME	0	SO	71
			CSI	3
Section 14 Business Continuity Management	PO	7	SS	4
	AI	0	SD	20
	DS	16	ST	1
	ME	0	SO	13
			CSI	3
Section 15 Compliance	PO	10	SS	1
	AI	3	SD	11
	DS	9	ST	6
	ME	13	SO	11
			CSI	1

APPENDIX 6
Additional References

Note: These references were used in development of Table 5, Figure 1, and the mapping detail included in the previous Appendices. The references are not explicitly cited in the text, and are thus listed here.

Ballou, B. Heitger, D.L. 2005. A building-block approach for implementing COSO's Enterprise Risk Management-Integrated Framework. *Management Accounting Quarterly* 6(2): 1-10.

Best Management Practice. (n.d.) *OGC's Best Practice Users: Case Studies and Testimonials.* Retrieved July 28, 2009, from http://www.best-management-practice.com/Knowledge-Centre/OGCs-Best-Practice-Users-Case-Studies-and-Testimonials/?DI=571450.

Gartner. (n.d.) *ITIL Implementation Best Practice.* Retrieved July 10, 2009, from http://www.gartner.com/teleconferences/attributes/attr_89167_115.pdf.

The Hamster. (n.d.) *ITIL Newsletter: News & Information for ITSM.* Retrieved April23, 2009, from http://itsm.the-hamster.com/itsm3.htm.

Hines, G. 2004. *ITIL and CobiT – Similarities, Differences and Interrelationships.* Retrieved July 18, 2009, from http://www.isaca-centralohio.org/archive/presentations/2005_01-ITIL%20and%20CobiT.pdf.

ISACA (n.d.) *COBIT Case Studies.* Retrieved July 20, 2009, from http://www.isaca.org/Template.cfm?Section=CobiT6&CONTENTID=24960&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

ITSM Encyclopedia. (n.d.) *ITIL (R) Disadvantages.* Retrieved July 26, 2009, from http://itsm.certification.info/itildisads.html.

KTH. (n.d.) *Model-Based IT Governance Maturity Assessments with Cobit*. Retrieved July 22, 2009, from http://www.ee.kth.se/php/modules/publications/reports/2007/IR-EE-ICS_2007_026.pdf.

Scribd. (n.d.) *IT and Business Process Performance Management: Case Study of ITIL Implementation in Finance Service.* Retrieved July 24, 2009, from http://www.scribd.com/doc/12636156/IT-and-Business-Process-Performance-Management-Case-Study-of-ITIL-Implementation-in-Finance-Service-Industry.