An IT Compliance Course Emphasizing Information System Design and Software Testing

Mayur R. Mehta
mm07@txstate.edu

Sam Lee
sl20@txstate.edu

Jaymeen R. Shah
js62@txstate.edu
Department of CIS & QMST
Texas State University–San Marcos
San Marcos, Texas 78666, USA

ABSTRACT

Sarbanes-Oxley Act (SOX) of 2002, passed by the United States Congress**,** requires that publicly traded companies conduct annual audits of their internal controls for financial reporting. Information Technology (IT) compliance is increasingly important due to the impact of SOX. This paper reports our initiatives to address the need of IT compliance education at Texas State University – San Marcos. As a result, a course is proposed based on the Control Objectives for Information and related Technology (COBIT) framework. Since the existing courses in the Master of Science in Accounting and Information Technology (MSAIT) program have addressed parts of the requirements for teaching IT compliance, the proposed course will emphasize COBIT framework as it applies to the methods and tools for information system design and software testing.

Keywords: IT Compliance, system design, software testing, Sarbanes-Oxley Act, auditing

1. INTRODUCTION

In the past few years, the information technology (IT) profession in the United States has undergone dramatic and fundamental changes. Although programming skills are still essential, there is a significant increase in the need for IT professionals with the ability to apply information technology to support the execution of critical business operations and strategies. In other words, the focus has shifted from developing business software to developing enterprise applications that incorporate appropriate regulatory and industry compliance processes as well as controls. One of the best examples of this transition is the emerging importance of IT compliance due to the impact of the Sarbanes-Oxley Act (SOX) of 2002.

IT compliance means an accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications, or legislation (Kim, In Press). The SOX Act attempts to address recent egregious and unethical corporate activities through increased governmental oversight in the United States. Of the Act's eleven sections, section 404 has had the greatest impact on financial report processes. Section 404 requires assurance of internal controls over financial data flowing through to the company's financial statements. To assure compliance with the SOX Act, most United

States corporations have come to rely on the internal control framework that is developed by the Committee of the Sponsoring Organizations of the Treadway Commission (COSO). Further, to assure the reliability of financial reporting, most would agree that companies must use and maintain a well-controlled IT environment.

According to the IT Governance Institute (2004):

> "Performing a thorough review of IT control processes and documenting them as the enterprise moves forward will be a time-consuming task. Without appropriate knowledge and guidance, organizations will run the risk of doing too much or too little. This risk is amplified when those responsible are not experienced in the design and assessment of IT controls or lack the necessary skill or management structure to identify and focus on the areas of the most significant risk."

Public Company Audit Oversight Board (PCAOB), created as a consequence of SOX, is a nonprofit public corporation with responsibility to oversee auditors of public companies. According to Bennett and Cancilla (2005), the PCAOB defined auditing requirements that are related to at least two IT areas: application change management, and application and data security. This means that companies are required to establish complete documentation, testing, and control processes for their applications. They pointed out that the IT industry quickly enhanced Computer-Aided Software Engineering (CASE) tools to respond to address related issues, seeing SOX compliance projects as business opportunities. However, Accounting/IT curricula at most academic institutions have been slow to adopt discussion of IT compliance and its implementation, especially from the perspective of application acquisition or development. To be successful, an IT compliance professional must be capable of developing and executing an IT compliance plan for the applications involving financial reporting. The plan, which is used to fulfill the IT auditing requirements of SOX, must be based on the PCAOB standard (PCAOB, 2007). This role essentially requires a thorough grounding in IT and Accounting fundamentals and skills. Thus, the IT compliance education is a challenge to a university's business school.

This paper reports our initiatives to address the need for IT compliance education at Texas State University – San Marcos. The university recently established a graduate program in Accounting and Information Technology leading to the Master of Science degree (MSAIT). The primary objective of this new program is to prepare students for successful careers in business information systems consulting (with specialization in business process engineering and business process controls) and IT auditing. Before being officially admitted to the program, the students are required to either hold an undergraduate degree in Accounting or complete additional leveling coursework in Accounting if their undergraduate degree is in other disciplines. The key of this initiative is to propose a course that focuses on the integration of information systems development and IT auditing topics from the perspective of regulatory and IT compliance.

2. BACKGROUND

Several graduate courses in IT were developed to support the MSAIT program, which are described below.

- Database Management Systems (DMS) – it includes techniques for analysis, design, and development of database systems, creating and using logical data models, database query language, and procedures for evaluating database management software.
- Information Security (ISec) – it introduces students to the analysis, design, development, implementation, and maintenance of information systems security.
- IT Systems Project Management (ISPM) – it provides an in-depth study of the project management body of knowledge as applied to information technology with an emphasis on the management of scope, costs, schedules, quality, and risks.

On the Accounting side, Accounting Information Systems (AIS) is a required accounting core course. This course covers advanced accounting information systems technologies used to enhance business process operations, management of risks and controls, and management of information resources. According to the study of Jackson & Cherrington (2001), the major emphases of the AIS course are the business cycles, controls and auditing, and systems analysis and design. Typically a spreadsheet application or a general ledger software application is used to provide hands-on learning experiences.

3. COURSE DESIGN

To design a new IT compliance course, we first identify IT-related auditing requirements from the PCAOB standard as follows.

- Evaluating period-end financial reporting processes such as procedures used to initiate, authorize, record, and process journal entries in the general ledger.
- Testing selected processes
  - Testing design effectiveness
  - Testing operational effectiveness
  - Obtaining the relationship of risk to the testing results
- Use of service organizations. If the service organization's services are a part of company's information system, then they are part of the information and communication component of the company's internal control over financial reporting.
- Benchmarking of automated controls
  - Entirely automated application controls are generally not subject to breakdowns due to human failure. This feature allows the auditor to use a "benchmarking" strategy.
  - After a period of time, the baseline of the operation of an automated application control should be reestablished.

Considering the complexity of IT compliance, it is impossible for one course to achieve all of the learning goals of IT compliance education. While topics and subject area matter related to regulatory compliance in general, and the SOX Act in particular, are appropriately addressed across the entire MSAIT program, a focus on overall compliance framework is somewhat lacking. Therefore, an IT compliance framework is introduced in the proposed course for (a) presenting the overall perspective of IT compliance; (2) providing an overview of conceptual material to address regulatory and IT compliance standards, and (3) providing a linkage to related topics available in other required courses in the program. The primary objective of the course is to introduce students to regulatory and IT compliance framework from an integrated perspective so that students acquire a deeper appreciation for related topics addressed through the MSAIT curriculum. The proposed course will thus establish the fundamental and conceptual foundation of the importance of compliance with regulatory standards as well as the generally accepted methodology to implement and monitor such compliance.

Course Modules

The proposed course is divided into four modules. The learning objectives of this course will be presented in a later part of this paper, which will show that these modules cover topics to address the PCAOB requirements.

Module One (IT Compliance Framework): Control Objectives for Information and related Technology (COBIT) is a framework that organizes IT control objectives and best practices by IT domains and processes, and links them to business requirements (IT Governance Institute, 2005). With COBIT, managers communicate high-level controls to stakeholders with respect to control requirements, technical issues and business risks. Based on the COBIT control objectives, the managers develop guidance on how to ensure compliance for the IT environment. The COBIT framework contains 34 high-level control objectives in four domains (*Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate*). Appendix A shows the relationship between the key control objectives of COBIT and IT/Accounting courses in the program where these control domains are addressed.

Module Two (Information Systems Design): Using this module, the student is introduced to an integrated CASE tool that supports the model driven approach (MDA) to modern application development. With this approach, the focus shifts from informal modeling and manual coding to precise models and automated code generation (Conn & Forrester, 2006). This approach is based on Unified Modeling Language (UML) - the de facto standard for object oriented analysis and design.

Module Three (Software Testing): To assure IT compliance, it is critical that there are consistencies in documentation for requirements, design specification, software testing, user verification and deployment. Before being signed off in the various phases of application development, software must be tested by developers, quality assurance (QA) engineers, users and IT compliance professionals. Thus a tool is incorporated in this module to demonstrate automated software testing, which includes features for source code control, component testing and system testing.

Module Four (Computer-Aided Auditing Tools): In this module, the student is introduced to the practices of self-auditing for IT compliance documentation. ACL (Audit Command Language) is the most used data extraction and analysis audit software (McCombs & Sharifi, 2004). Also, the Zero-Footprint Audit Tool (ZFPAudit) is available for gathering and reporting computer system settings useful to the IT auditor in assessing compliance and risk elements arising from improper configuration (Bek, 2004).

Learning Objectives

After completing the COBIT topics, the students should be familiar with what is involved in each domain of the framework. Therefore, they should be able to use the framework for the following: (1) to obtain business requirements and define related IT processes; (2) to apply relevant measures to identify the significant processes of organizations; (3) to explain benchmarking strategies for auditing.

The MDA provides many of the best practices for the control objectives in the *Acquire and Implement* domain of COBIT. After completing the UML topics, the students should be able (1) to use UML to model functional requirements of the processes; (2) to apply the UML model to identify third-party services in the processes; and (3) to apply the UML model to create test plans and procedures.

After completing the software-testing topics, the students should be familiar with the methods for testing the implementation of IT processes.

After completing the topics of auditing tools, the students should be familiar with the approaches to automatic reporting for IT audit.

4. SUMMARY

To include IT compliance into a curriculum that focuses on Information Technology and Accounting is a worthy, but challenging task. The college will prepare students to meet the increasing needs of business corporations for employees with knowledge of Accounting and Information Technology. The auditing requirements from the PCAOB standard are carefully investigated to create the IT compliance course. It is not surprising that existing courses address parts of the requirements. Eventually this course will provide coverage of topics that are lacking in other courses in the MSAIT program of the college. To provide an applied learning approach, we adopt modern tools and methodologies available in the IT industry for this course.

REFERENCES

Bek, J. (2004). ZFPAudit: A Computer-assisted Audit Tool for Evaluation of Microsoft Operating Systems. *Information Systems Control Journal*, 1.

Bennett, V. & Cancilla, B. (2005). IT responses to Sarbanes-Oxley. *IBM developerWorks*. Retrieved August 8, 2007, from http://www-128.ibm.com/developerworks/rational/library/sep05/cancilla-bennet/

Conn and Forrester (2006). Model Driven Architecture: A Research Review for Information Systems Educators Teaching Software Development. *Information Systems Education Journal*, 4 (43).

Jackson, R. B. & Cherrington, J. O. (2001). IT Instruction Methodology and Minimum Competency for Accounting Students. *Journal of Information Systems Education*, 12 (4), 213 – 222.

Kim, S. (In Press). IT Compliance of Industrial Information Systems: Technology Management and Industrial

Engineering Perspective. *The Journal of Systems and Software*.

McCombs, G. B. & Sharifi, M. (2004). Utilization of Generalized Audit Software in an Information Systems Auditing Course. *Information Systems Control Journal*, 6.

PCAOB (2007). *Auditing Standard No. 5 – An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements*, Retrieved August 8, 2007, from http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

IT Governance Institute (2004). *IT Control Objectives for Sarbanes-Oxley*. Retrieved February 21, 2007, from http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_2nd_research.pdf

IT Governance Institute (2005). *Control Objectives for Information and related Technology (COBIT) 4.0*. Retrieved February 21, 2007, from http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

APPENDICES

Appendix A. The relationship between COBIT and the MSAIT courses

Domain	Control Objective	IT Course (or Module) where this control objective is addressed
Plan and Organize	Define a strategic IT plan	ISPM
	Define the information architecture	DMS, Design[a] Module in ITC*
	Define the IT processes, organization and relationships	Design Module in ITC
	Communicate management aims and direction	ISPM
	Manage the IT investment	ISPM
	Assess and manage IT risks	ISPM
	Management of IT human resources	ISPM
Acquire and Implement	Identify automated solutions	DMS, Design module in ITC
	Acquire and maintain application software	Design Module in ITC
	Manage changes	Design and Testing[b] Modules in ITC
	Install and accredit solutions and changes	Testing Module in ITC
	Acquire and maintain technology infrastructure	Design Module in ITC
Deliver and Support	Manage third-party services	Testing Module in ITC, ISec
	Manage performance and capacity	DMS, Testing Module in ITC
	Ensure systems security	ISec
	Manage problems and incidents	ISec, DMS
	Manage data	DMS
	Manage operations	ISec, DMS
Monitor and Evaluate	Monitor and evaluate IT performance	Testing Module in ITC
	Monitor and evaluate internal control	AIS
	Ensure regulatory compliance	AIS, CAAT [c] Module in ITC

*ITC: IT Compliance, [a]Design: Information Systems Design
[b]Testing: Software Testing, [c]CAAT: Computer-Aided Auditing Tools.