What Should IS Majors Know About Regulatory Compliance?

Craig A. VanLengen
craig.vanlengen@nau.edu
The W. A. Franke College of Business,
Northern Arizona University
Flagstaff, AZ 86011-5066

Abstract

Because of the severe penalties associated with non-compliance of legislative acts and regulations it is important for information systems (IS) majors to recognize and understand the need for the implementation, evaluation, and reporting on internal controls. IS majors need to be aware of legislation and regulations that have an impact on information technology (IT). IS majors also need to understand business processes and how to select, implement, and report on controls embedded into software that is developed. The best way to understand the business processes and associated controls is to become familiar with control frameworks.

Keywords: IS Curriculum, Regulatory compliance, Model curriculum, COBIT, Control Frameworks

1. INTRODUCTION

When it comes to regulatory compliance how much do we know and teach about the following: Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), US Patriot Act, document retention, European Union Data Protection Directive (EUDPD), ISO 17799:2005 Code of Practice for Information Security Management (ISO 17799), and possibly others (Budd, 2006; Carter, Cobb, Earhart, & Noblett, 2006)?

The IT Governance Institute (2006) states that, "Good IT governance over planning and life cycle control objectives should result in more accurate and timely financial reporting." The U. S. Congress made accurate financial reporting a legal requirement by passing the Sarbanes-Oxley Act in 2002. "Sarbanes-Oxley compliance requires more than documentation and/or establishment of financial controls; it also requires the assessment of a company's IT infrastructure, operations, and personnel" (Lahti, Peterson, & Lanza, 2005). HIPAA as the title indicates is specific to health care and associated organizations. The intent is to protect the privacy of patient data (McLean, 2007). GLBA requires safeguards for protecting customer financial data (Carter et al., 2006). EUDPD regulates the protection and limitations of sharing of data on the citizens of the European Union (Carter et al., 2006). "ISO 17799 is a comprehensive information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)" (Carter et al., 2006, p. 5). The remainder of this paper will concentrate on SOX and control frameworks. The principles of control frameworks can be applied to the other legislative acts and regulations.

2. SARBANES-OXLEY AND IT

The Sarbanes-Oxley Act (SOX) requires the chief executive officer (CEO) and chief financial officer (CFO) of publicly traded companies that have either stocks or debt traded on U.S. exchanges to verify that their financial statements are true and accurate based on a system of internal controls that they have evaluated. The CEO and CFO must certify that they are responsible for creating, maintaining, and evaluating the system of

internal controls. If any material weaknesses are discovered they must disclose them (Ecora, 2004; Hewlett-Packard, 2006; Network, 2006; Swanson, 2006). SOX also requires the auditors of these companies to test and verify management's assessment of the effectiveness of the organization's system of internal controls (Ecora, 2004; Green, 2006; McLean, 2007; Network, 2006).

SOX does not mention IT specifically in the act, nor is it specific on the IT controls that have to be established (Lahti et al., 2005). "In the modern enterprise, financial reporting systems, such as ERP systems, are almost completely reliant on IT assets: software, servers, workstations, infrastructure and more" (Hewlett-Packard, 2006, p. 3). Would the CEOs and CFOs certify that they have a properly operating system of internal controls that is used to create their financial reports without assistance from their IT system, where the controls are documented, implemented, and managed (Ecora, 2004)? "IT is at the heart of the issue, because the accuracy of financial reports relies in large part on decisions made by IT professionals" (Hewlett-Packard, 2006, p. 2). In fact "an increasing number of companies are also requiring their CIO's to sign a 'sub-certification' regarding the controls, processes and overall accuracy of the IT assets they manage" (Hewlett-Packard, 2006, p. 2). "Because IT is crucial to support and enables financial reporting and other company operations, security technologies and measures must be adapted to meet" (Swanson, 2006, p. 12) the control, evaluation and disclosure requirements of SOX.

To successfully meet SOX compliance IT must support and cooperate with the business units and the business units must cooperate and support the IT function (Lahti et al., 2005; Network, 2006). If the IT systems were developed using "best practices" the organization could use "established IT practices and technologies, such as change management and IT asset management" (Hewlett-Packard, 2006, p. 2) to produce "reliable, replicable, and audit proof detail about control of, and access to the infrastructure that supports financial data" (Ecora, 2004, p. 7).

3. IT AND BUSINESS PROCESSES

"Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders' value" (IT Governance, 2007, p. 5). In most cases business processes and IT are interdependent. So an evaluation of compliance with regulations must include the business processes and the IT system that captures transactions from the beginning. (IT Governance, 2007). Corporate management and IT must map "control objectives for financial reporting to IT control objectives. Which means that IT management must become familiar with and conversant in common financial concepts" (Ecora, 2004, p. 8). Regulatory compliance must be looked at as a non-penalty activity because it offers opportunities "to improve processes, create competitive advantage, and further integrate IT into your business to improve ROI" (Carter et al., 2006, p. 14). We need "to ensure that the enterprise's IT supports the business objectives" (IT Governance, 2007, p. 5).

Owners of the business processes, IT personnel, auditors, and security analysts must work together to understand the business processes and how to select and implement internal controls over those processes and to document the controls that are in place. "In defining internal controls it is important to articulate the central technology components of business processes and increase the understanding between IT and business members of the Sarbanes-Oxley team" (Ecora, 2004, p. 8). Any modifications of the processes and/or the controls must be documented and handled using change management techniques (Ecora, 2004; Swanson, 2006). The technology can be used to monitor our compliance efforts and to provide information on changes that are needed to ensure the system continues to meet regulatory requirements (Swanson, 2006). "No longer will an informal or even a loosely documented procedure suffice; rather, proof will now be the cornerstone to an organization's passing its SOX compliance. To pass SOX compliance, an IT organization will have to show proof of formal documentation, management buy-off and sign-off, and effectiveness of the implemented controls" (Lahti et al., 2005, p. 51).

This means that IS curriculum must not only teach the technology but also business

processes and internal controls. In many cases we should be emphasizing business processes and internal controls over the technology. Most of our IS programs are within a college of business, so we would expect our majors to retain some knowledge of business processes and accounting. It may also require us to do a better job of teaching the integration and interdependence of business processes, internal controls, financial reporting and technology.

4. CONTROL FRAMEWORKS

Even though most of SOX is not specific on requirements the Public Company Accounting Oversight Board (PCAOB) indicated that the assessment of internal control should follow a recognized control framework, such as that provided by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (Ecora, 2004; Green, 2006; Hewlett-Packard, 2006; IT Governance, 2007; Network, 2006; Softlanding, 2006; Swanson, 2006). The COSO framework covers: The internal control environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring (Ecora, 2004; Green, 2006; Network, 2006; Rothman, 2007; Softlanding, 2006).

COSO provides internal control guidance for the accounting and finance people; it is not information-technology specific. COBIT can then be used to map the COSO objectives into IT specific objectives (Ecora, 2004; Rothman, 2007). "COBIT provides a methodical approach to the IT function for Sarbanes-Oxley implementation and support" (Lahti et al., 2005, p. 32). With COSO and COBIT "frameworks in place, executive management should have the confidence in their organization's internal controls to sign off as Sarbanes-Oxley requires" (Softlanding, 2006, p. 10).

IS students should be aware of the COSO framework when creating or modifying business processes and conversant in COBIT to design and implement IT controls over the processes. IS students can be taught how to map regulations and standards to the control frameworks instead of working on individual controls and regulations (Carter et al., 2006).

5. Using Risk Assessment

The original view of SOX compliance was "that companies' management design an internal control system that can substantiate every assertion in their financial statements" (Green, 2006). The latest guidance from the SEC and the PCAOB are for the organization to take a top-down/ risk-based approach (U. S. Securities, 2005). With a risk-based assessment management, auditors and IT would define significant accounts, their associated business processes, software that does the processing and the controls embedded in the software (Mackey, 2007; Softlanding, 2006; Swanson, 2006). "A risk assessment will force an organization to look at the information and processes that may have an effect on the accuracy, transparency and accountability associated with the company's financial statements" (Mackey, 2007). The top-down/risk-based process assists management and auditors in defining the risks and associated compliance activities (Mackey, 2007).

The IT Governance Institute (ITGI) (2006) has provided additional guidance on applying a top-down, risk-based approach, prioritization of controls, identifying and addressing application controls, and segregation of duties in its 2nd edition of "IT Control Objectives for Sarbanes-Oxley." The ITGI has also provided a mapping of PCAOB Auditing Standard No. 2 and COBIT for 12 IT control objectives (IT Governance, 2006).

Good IT documentation will make the risk-assessment process easier and also "to understand dependencies across your entire IT infrastructure and helps you optimize network and system configuration, standardize configuration settings, and accelerate problem resolution and troubleshooting" (Swanson, 2006, p. 13). Good system documentation and associated software also makes it easier to "create audit-ready documents on demand" (Swanson, 2006, p. 13).

Change management is an important activity to assess. "Changes to a server, network devices, or directory servers can have a major impact on the security, level, and quality of IT services delivered" (Swanson, 2006 p. 11). "IT teams need to know when change occurs and whether it's desired, not desired, accidental, benign, malicious, intentional, or originating from inside or outside, in order to

address the resultant risks" (Swanson, 2006, p. 11). Everyone in the organization needs "to know that unauthorized activities will be detected and investigated" (Swanson, 2006, p. 12).

Another compliance issue is document retention. Electronic documents, including e-mails, must be maintained and provided in case of litigation (Bentley, 2008).

The Sarbanes-Oxley Act of 2002 implies that strict retention policies and procedures must be in place. I say 'implies' because the act itself does not specifically indicate exactly what should be the storage requirements, but does require corporate officers to institute internal controls on their information to ensure completeness, correctness, and quick access. One exception to the specifics: accounting firms are specifically mentioned in Sarbanes-Oxley. The act calls for accounting firms that audit publicly-traded companies to keep related audit documents for no less than seven years after the completion of an audit. Violators can face fines of up to $10 million and 20 years in prison (Lowe, 2005).

6. COBIT

"COBIT standards emphasize the need for policies and procedures and correctly structured business processes to deal with risk" (Mackey, 2007). COBIT recognizes and builds on COSO and has a business-focus and process orientation (Hewlett-Packard, 2006; IT Governance, 2007; Softlanding, 2006). Because of its business-focus the guidelines and best practices of COBIT have been widely used by auditors and corporate management when assessing SOX compliance (Lahti et al., 2005; Softlanding, 2006; Syngress, 2005). The COBIT framework makes it easier for business managers and IT to work on business processes and to build controls that will reduce exposure from a technical and business viewpoint (IT Governance, 2007; Softlanding, 2006). "The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners" (IT Governance, 2007, p. 5).

COBIT has six major components with approximately 300 platform independent control objectives (Lahti et al., 2005, Syngress, 2005). "Entity level controls consist of the policies, procedures, practices, and organizational structures intended to assure the use of IT will enable the accomplishments of business objectives, and that planned events will be prevented, or detected and corrected." (Lahti et al., 2005, p. 36)

With a risk-based approach the organization will have to determine the most appropriate controls to mitigate the exposure and customize the controls to fit their environment (Lahti et al., 2005). "Coordination between IT and business personnel and processes, with upper management and executive support, is essential to reduce key controls" (Softlanding, 2006, p. 13). Because regulatory compliance is a process not a one time event business management and IT should make every effort to leverage the use of technology for control improvements and to make compliance more efficient, effective, and sustainable (Lahti et al., 2005; Softlanding, 2006). Again change management is very important to monitor the process and control changes needed to obtain or prove compliance and to ensure that as the business and systems change that the organization maintains compliance (Mackey, 2007).

7. WHAT DO WE NEED TO TEACH?

Regulatory compliance could be included in the following courses: Fundamentals of Information Systems, Information Systems Theory and Practice (corporate planning and strategy), Electronic Business Strategy, Architecture and Design, Information Systems Theory and Practice Information Technology Hardware and Software systems, Networks and Telecommunications, Programming, Data, File and Object Structures, Analysis and Logical Design, (control objectives and design and implementation of controls), Physical Design and Implementation with DBMS and Emerging Environments (IS 2002, 2002).

We should start out teaching internal controls along with business processes. Next we should cover the requirements of the regulatory acts that apply to information systems. We can then present the different control frameworks and engage the students in mapping the requirements of the regula-

tory acts to controls using the appropriate framework.

Control frameworks in the fundamentals of information systems and theory and practice courses would be at the level of recognition and how to link business processes and IT controls. Courses in programming, database, and operating and networking systems should include the analysis of control weaknesses and the selection and implementation of appropriate controls based on the frameworks. Courses in analysis, design and implementation should also examine business processes and design and implement appropriate controls. Change management should be covered as a way to demonstrate control over the implementation of internal controls and the monitoring of the control environment.

8. CONCLUSION

In an effort to prevent or detect financial abuses and frauds such as those of Adelphia Communications Corp, Enron, Global Crossing, Tyco, and WorldCom, Congress now requires public corporations to demonstrate compliance with legislative acts and regulations (Storms & Kral, 2003). Information system majors need to be aware of these requirements and how to implement internal controls over business processes to ensure compliance with the regulatory acts.

We should provide our students with the ability to recognize the need to demonstrate regulatory compliance by using available and highly recognized control frameworks; we should not make an academic decision to "assume them away." We need to integrate regulatory compliance in our major courses and make sure our students understand business processes, accounting, and financial reporting from their required business core courses.

9. REFERENCES

Bentley, L. (2008). "Effective Document Retention Starts with Smart Policy." Retrieved June 13, 2008, from <http://www.itbusinessedge.com/blogs/ssg/?p=327>.

Budd, C. (2006). "Don't Get Caught Between a Rock and a Hard Place: Regulatory Compliance and Security Updates." Retrieved May 21, 2008, from <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/regcomparticle.mspx>.

Carter, R., Cobb, J., Earhart, L., & Noblett, A. (2006). "Microsoft Solutions for Security and Compliance: Regulatory Compliance Planning Guide." Retrieved May 24, 2008, from <http://www.microsoft.com/downloads/details.aspx?FamilyId=BD930882-0D39-4900-9A79-B91F213ED15D&displaylang=en>.

Committee of Sponsoring Organizations (COSO) (2008). Retrieved June 26, 2008, from Home page <http://www.coso.org/default.htm>.

Ecora Software, (2004). "Practical Guide To Sarbanes-Oxley IT Internal Controls." Retrieved May 24, 2008, from <http://www.ecora.com/ecora/whitepapers/IDPG_soxIntCtrl.pdf>.

Green, J. W. (2006). "Section 404 for Small Caps." Retrieved April 1, 2008, from <http://www.aicpa.org/pubs/jofa/mar2006/green.htm>.

Hewlett-Packard (2006). "Sarbanes-Oxley and the IT organization: A survival guide." Retrieved May 24, 2008, from <http://h71028.www7.hp.com/ERC/downloads/4AA0-6568ENW.pdf>.

IS 2002 model curriculum for undergraduate degree programs in Information Systems, (2002), Retrieved June 5, 2008, from <http://www.aitp.org/organization/profile/manuals/pdf/is%202002%2012-31-2002.pdf>.

ISACA (2008). ISACA Home page, Retrieved June 26, 2008, from <http://www.isaca.org/Template.cfm>.

IT Governance Institute (2006). "IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition." Retrieved May 30, 2008, from <https://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/MembersOnly.cfm&ContentFileID=14234>.

IT Governance Institute (2007). "COBIT 4.1 Excerpt." Retrieved May 30, 2008, from <http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172>.

Lahti, C., Roderick Peterson, & Steve Lanza. (2005). SOX and COBIT Defined, Retrieved May 30, 2008, from <http://searchsecurity.techtarget.com/searchSecurity/downloads/Lahti_Ch02.pdf>.

Lowe, S. (2005). "Sarbanes-Oxley and its affect on storage compliance systems." Retrieved June 13, 2008, from <http://articles.techrepublic.com.com/5100-10878_11-5783626.html?tag=rbxccnbtr1>.

Mackey, R. (2007). "How compliance control frameworks ease risk assessment burdens." Retrieved May 30, 2008, from <http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1240661,00.html>.

McLean Report (2007). "Compliance Regulation: Understanding the Dirty Dozen." Retrieved Jan 5, 2008, from <http://www.infotech.com/Samples/McLean_Report_Research_Note-Compliance_Regulation-Understanding_the_Dirty_Dozen.pdf>.

Network Instruments, LLC. (2006). "SOX and IT." Retrieved May 24, 2008, from <http://www.networkinstruments.com/assets/pdf/SOX_WP.pdf>.

Rothman, M. (2007). COSO and COBIT: The value of compliance frameworks for SOX, Retrieved May 29, 2008, from <http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1265523,00.html>.

SoftLanding Systems, Inc. (2006). "The IT Manager's Working Guide to Sustainable SOX Compliance." Retrieved May 24, 2008, from <http://www.softlanding.com/sox/docs/workingguide.pdf>

SOX-online: The Vendor-Neutral Sarbanes-Oxley Site. (2008). Retrieved June 26, 2008, from <http://www.sox-online.com/>.

Storms, M., & Kral, R. (2003). "Sarbanes-Oxley for the Rest of Us." Retrieved June 11, 2007, from <http://wistechnology.com/articles/437/>.

Swanson, D. (2006). "Keeping Up Your SOX Compliance And Turning IT into a High Performer by Improving Change Control." Retrieved May 30, 2008, from <http://download.101com.com/pub/itci/Files/Tripwire%20-%20Keeping%20Up%20Your%20SOX%20Compliance%20sm.pdf>.

Syngress (2005). "Introduction to COBIT for SOX compliance." Retrieved May 30, 2007, from <http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1148318,00.html>.

U. S. Securities and Exchange Commission (SEC) (2005). "Staff Statement on Management's Report on Internal Control Over Financial Reporting." Retrieved June 26, 2008, from <http://www.sec.gov/info/accountants/stafficreporting.htm>.