IT Governance
Dr. Michael Shaw
Term Project

IT Auditing Framework and Issues Dealing with Regulatory and Compliance Issues

Submitted by: Gajin Tsai
gtsai2@uiuc.edu

May 3rd, 2007
Table of Contents:

Abstract…………………………………………………………………………………....3
Introduction………………………………………………………………………………..4
Review of Literatures……………………………………………………………………...5
  Sarbanes-Oxley……………………………………………………..……………..5
  ITIL…………………………………………………….………………………….6
  ISO 17799……………………………………………………...………………….7
  COBIT…………………………………………………………………………….9
Controls and Benefits………………………………………….…………………………11
Allstate Case Study…………………………………………………………...…………11
  Abstract…………………………………………………………………………..12
  Background………………………………..…....……..…………………………12
  Implementation Overview…………………………....…...……………………..12
  COBIT and SOX……………………………………….………..……………….13
    Allstate’s IT Governance Assessment…………………………...………………16
Conclusion and Findings……………………….………………………………………..17
Reference…………………………..………………………………………...…………..18
Abstract

Since the Sarbanes-Oxley Act of 2002, many public companies have faced challenges while trying to comply due to the high cost and inexperience. After the bill passed, auditors did not have a set of guidelines to follow when first auditing the companies. As auditors gain more experience throughout these years, they have developed more of a routine, or best practice for IT auditing.

One headache for compliance with Sarbanes-Oxley Section 404, is that the section makes no specific mention of what controls need to be implemented to be in compliance with SOX. How can companies comply with it, if they do not know what they need to do to comply? Although there are varying practices within different organizations, many choose to follow the guidelines of ITIL, ISO 17799, or COBIT.

ITIL, ISO17799, and COBIT are guidelines companies are able to follow to be compliant with SOX. However, many companies have been able to find significant benefits in not only complying with SOX, but with adopting one of these guidelines beyond SOX’s scope.
Introduction

This term project is to explore IT auditing framework and general or best practices. I will focus on the regulatory and compliance issues, namely the Sarbanes-Oxley Act of 2002. Many companies choose to follow the guidelines of ITIL, ISO 17799, or COBIT in order to comply with SOX. I will give an overview of each and how their practices meet the requirements of SOX. These guidelines were not created in order to specifically comply with SOX. Many companies have found that following these guidelines not only provide themselves with compliance to SOX, but have also experienced significant benefits. I will focus more so on COBIT, and include a case study of Allstate Insurance and how they have adopted COBIT to comply with SOX as well as provide benefit for the company’s overall strategy.
The Sarbanes-Oxley Act of 2002 is a United States federal law passed amidst numerous corporate and accounting scandals. Some important notables in SOX is the creation of the Public Company Accounting Oversight Board whose purpose is to “protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.” The PCAOB is in charge of overseeing, regulating, and punishing accounting firms in their role as auditors for public companies. It also addresses issues such as independence and financial disclosure of the auditors. Here is a summary of sections 302 and 404 of the Sarbanes-Oxley act:

**Section 302: Corporate Responsibility for Financial Reports**

- The signing officers have reviewed the report and is directly responsible
- The report does not include misrepresentations or omit any information considered misleading
- Financial Statements and information is presented fairly
- The signing officers are responsible for internal controls and have evaluated them within ninety days of signing.
- Report any deficiencies in internal controls and report any fraud with management involving internal activities
- Signing officers must report any significant changes in internal controls

**Section 404: Management Assessment of Internal Controls**

Annual reports must include an assessment concerning the management’s responsibility for adequacy of the structure, procedure, and effectiveness of the internal
control. The accounting firm auditing are to attest to the management’s assessment of the organization’s statement that their internal controls are in place, operational, and effective.

ITIL

Information Technology Infrastructure Library (ITIL), is a published set of best practices for IT services. It outlines a set of management and control procedures that are intended to support businesses in achieving both high financial quality and value in IT operations. The eight books in the ITIL are:

- Service Delivery
- Service Support
- ICT Infrastructure Management
- Security Management
- The Business Perspective
- Application Management
- Software Asset Management
- Planning to Implement Service Management

The Service Delivery, Service Support and Security Management books are regarded as the central components of the framework. Service Delivery is primarily concerned with services that the business requires of its IT in order to provide appropriate support to the business users. Service Support focuses on the user of the IT services within an organization, and assuring they have access to the proper functions to support ongoing business. Security Management is the knowledge and structure of an organization’s information assets, and the development, documentation and
ISO 17799

ISO 17799 is a comprehensive set of controls comprising best practices in information security. It was first issued as a British standard by the British Standard Institute (BSI) in 1995 as BS7799, but was adopted by the International Organization for Standardization (ISO) in 2000, and later revised in 2005 to reach a larger international audience. ISO 17799’s list of control objectives are just a set of guidelines. None of the

<table>
<thead>
<tr>
<th>Tactical</th>
<th>Operational</th>
<th>Other process</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Service Management</td>
<td>Service Delivery</td>
<td>Service Support</td>
</tr>
<tr>
<td>Service Delivery</td>
<td>Capacity Management</td>
<td>Incident Management</td>
</tr>
<tr>
<td></td>
<td>Financial Management for IT service</td>
<td>Problem Management</td>
</tr>
<tr>
<td></td>
<td>Availability Management</td>
<td>Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Service Level Management</td>
<td>Change Management</td>
</tr>
<tr>
<td></td>
<td>IT continuity Management</td>
<td>Release Management</td>
</tr>
<tr>
<td></td>
<td>Customer Relationship Management</td>
<td>Service Desk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICT infrastructure Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planning to Implement Service Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Management</td>
</tr>
</tbody>
</table>
controls listed are mandatory, so each individual organization much decide which controls they choose to adopt while using the standard for guidance. ISO 17799 has a list of 39 control objectives and hundreds of specific controls. ISO 17799’s scope is very broad, which allows a variety of different organizations to adopt it. Here are some main sections in ISO 17799:

- **Risk Assessment and Treatment** – This section was added to the latest version (2005) and deals with the fundamentals of security analysis

- **System Policy** – To provide an organization’s management direction and support for information security.

- **Organizing Information Security** – Objectives are to 1) Manage the information security within an organization, and 2) Protect information from third party products or services. (Dealing with providers, customers, etc.)

- **Asset Management** – 1) To organize information assets to a nominated owner for responsibility. 2) Information is to be classified according to the security level needed and noted accordingly.

- **Human Resources Security** - 1) Security responsibilities are to be enacted prior to recruiting permanent employees. 2) Ensure that employees are aware of their security responsibilities. 3) Secure information during change of employment.

- **Physical and Environmental Security** – 1) Control unauthorized physical access to an organization’s information. 2) Prevent theft or damage of assets.

- **Communications and Operations Management** – This section is lengthy and describes security controls for systems and network management such as:
operational procedures and responsibilities, third party service, media handling, exchange of information, etc.

- **Access Control** – This section’s objectives are to secure and limit access to sensitive information, prevent unauthorized user access to networked services, operating systems, and application systems.

- **Information Systems Acquisition, Development and Maintenance** – This section addresses issues for the process of building, acquiring, testing, and implementing IT systems. It has guidelines for security requirements for information systems, security of system files, security in development and support processes, correct processing in application systems, and cryptographic controls.

- **Information Security Incident Management** – The objectives are to 1) identify incidents and weaknesses in information security and report and properly manage them. 2) Ensure a consistent and effective approach is applied to information security issues within the management of an organization.

- **Business Continuity Management** – This section addresses disaster recovery and how to counter act those ongoing business interruptions.

- **Compliance** – This objective of this section is to comply with legal security requirements and internal security policies and standards. Audits should be conducted with minimal disruption to operational systems and ongoing business.

**COBIT**

Control Objectives for Information and related Technology (COBIT) is a set of best practices for information technology management based off the COSO framework. It was created by the Information Systems Audit and Control Association (ISACA) and the
IT Governance Institute (ITGI). It provides organizations with a set of best practices, processes, and indicators to help them maximize their benefits in using information technology and IT governance within a company. There have four editions since its creation in 1992. The 4th edition published in 2005 has grown in popularity and usage due to the Sarbanes-Oxley Act. The 4th edition has 34 high level objectives with four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

- **Planning and Organization** – Planning is about developing strategic IT plans that support the business objectives. These plans should be forward looking and in alignment with the company’s planning goals, for example, a two, three, or five year projection.

- **Acquisition and Implementation** – Once the plans are developed and approved, you may need to acquire new applications, or even acquire or develop a new staff skill set to execute the plans. Upon completion of the Acquisition phase, the plans now need to be enacted in the Implementation phase, which should include maintenance, testing, certifying, and identification of any changes needed to ensure continued availability of both existing and new systems.

- **Delivery and Support** – This phase ensures that systems perform as expected upon implementation, and continue to perform in accordance with expectations over time, usually managed via service level agreements (SLA). In this regard, systems can be related to infrastructure components or third-party services.
• *Monitoring* – The monitoring phase uses the SLA or baseline established in subsequent phases to allow an IT organization to gauge how they are performing against expectation, and provides them with an opportunity to be proactive.

**Controls and Benefits**

So now that we have reviewed ITIL, ISO 17799, and COBIT and have seen the basic guidelines of each and how they suggest IT governance, it leaves certain questions to be asked: Are there advantages of going above and beyond the requirements for Sarbanes-Oxley? Does applying controls based on these guidelines help the business as a whole? If so, what are a few benefits?

In a study by the Information Technology Process Institute (ITPI), which was mentioned in Protiviti’s presentation by Andrew Retrum, organizations were surveyed to determine whether there was a relationship between the number of controls implemented, and the 25 operations, security, and audit performance measures determined by ITPI. Some key findings were that:

• Best practices outline in the ITIL and COBIT frameworks improved performance
• 21 Foundational Controls have the biggest impact on performance measures
• Organizations that use Foundational controls have significantly higher performance

Organizations that use Foundational Controls have:

• 12% to 37% less unplanned work
• 12% to 26% higher chance of success rate
• 2.5 to 5.4 times higher server to system administrator ratio

**COBIT and IT Governance Case Study: Allstate**
Abstract

Allstate is the largest publicly held property and casualty insurance company in the United States. It has assets in excess of $134 billion, revenues over $32 billion, and approximately 40,000 employees. In 2000, Allstate’s internal audit adopted COBIT as their formal IT control framework. After the Sarbanes-Oxley Act was enacted in 2002, Allstate began using COBIT to evaluate their IT governance and control. COBIT helps Allstate ensure alignment between their overall business strategy and information technology. Allstate also uses COBIT to achieve a balance of appropriate and consistent controls to improve the effectiveness and efficiency of their business.

Background

Allstate Insurance was founded in 1931 under Sears, Roebuck & Co. and became public in 1993. It is based in Northbrook, Illinois and serves over 16 million households. With over $134 billion in assets and more than $32 billion in revenue, it is the largest public property and casualty insurance company in the US. Before 2000, Allstate’s internal audit group did not have a formal IT control framework. A new audit director reviewed the business environment and decided to adopt COBIT as their IT governance guideline.

Implementation Overview

The audit director presented COBIT to management and demonstrated how COBIT could provide a structured means to ensure consistent and suitable IT controls throughout the company. Also, COBIT provided a common language for IT governance that allowed related control and process functions to share a common ground. Members of Allstate’s implementation team had a risk assessment approach upon COBIT. They
held interviews with strategic IT and business managers to identify overall views of key business objectives and areas with potential risk. Based on the information received, the team developed and ranked, according to risk, critical application and infrastructure inventory. They then designed templates and programs for audits based upon the COBIT objectives they’ve found most useful for Allstate. Allstate’s goals for implementing COBIT focus on:

- Increasing awareness of the importance of IT controls
- Bringing attention to corporate IT governance
- Fostering management and accountability
- Improving client/auditor communication
- Providing a risk assessment framework

**COBIT and Sarbanes-Oxley**

After Sarbanes-Oxley passed in 2002, Allstate used COBIT to evaluate their IT governance and control and their infrastructure environment, while using COSO to evaluate their business process control. COBIT contains 34 high level controls, and very rarely is all used by an organization. Each individual organization has to determine which controls are appropriate to adopt. Allstate’s approach was to divide their activities into three phases. The first phase focused on organizing and launching the plan. Then second phase included documentation and assessment workshops. The third phase focused on continuing operations.

In the first phase, Allstate’s IT divides its processes into three levels that define how the company views IT. According to Allstate, Level 1 was for the business control owner (automated application controls such as interface controls, system edit checks and end
user security). Level 2 was for the application support control owner (general application controls such as change management, programmer security and system development lifecycle). Level 3 was for the infrastructure control owner (general computing controls such as data center operations, security administration and network administration). The three levels defined in phase 1 are shown in the diagram below:

Allstate then analyzed COBIT to determine which controls applied to Sarbanes-Oxley. The diagram below maps out the risk assessed subset of COBIT objectives to Allstate’s level 1, 2, and 3 processes.
Phase 2 focused on the levels 1, 2, and 3 and how documentation workshops can identify the key controls, activities, and gaps. This helped develop decision-making with control and design gaps. In phase 3, assessment of control objectives continue and is performed by the business and IT units within Allstate. Although methods vary, guidelines are as follows:

- All key controls must be self-assessed at least annually, with the majority assessed quarterly
- Key Controls with open design gaps should not be self-assessed.
- The individual who performs the key control activity cannot also perform the self-assessment.
- All self-assessment testing must be evidenced by appropriate documentation.
• Self-assessment scope and results must be summarized and reported to applicable certifiers.

Allstate’s IT Governance Assessment

Through adopting COBIT as their IT governance guideline and continuous assessment and improvement efforts, Allstate has found that inadequate controls expose an organization to risks that could disrupt ongoing business and harm its reputation. The overuse of controls is a burden to successfully running a business in a competitive environment. COBIT helps Allstate meet regulatory obligations such as SOX, and balance an appropriate amount of controls to improve the company’s efficiency and effectiveness while not burdening its ongoing business. Benefits listed include:

• Edits early in the process reduce exceptions and rework.
• Controls that provide consistency in data collection and processing help ensure accurate information and compliance with myriad states’ rules and regulations.
• Properly securing information minimizes the need to recover data and systems, to explain why confidential information was disclosed or to address the loss of competitive information.
• Including controls at the front end of the system development process saved time, effort and expense.
• Technology investment decisions are aligned to the business goals.
• Improved communications between the business and IT communities.
• Management had a framework that promoted scope containment and financial management.
Conclusion and Findings

An organization’s implementation of the guidelines of ITIL, ISO 17799, or COBIT enables them to be compliant with the Sarbanes-Oxley Act of 2002. However, each individual organization has a decision to make. Do they meet the minimal requirements for regulatory compliance, or do they go above and beyond for the debated benefits achieved by the company for doing so? A study conducted by Information Technology Process Institute (ITPI) found that organizations with the highest number of foundational controls have a higher performance level. Activities that differentiate top performers from others are ones that “sustain and continually improve their control systems.” However, it is not practical for an organization to implement as many controls as possible. Each needs to find an appropriate balance cost and effectiveness to determine which controls need to be adopted. In Allstate’s case, their controls in IT Governance produced the benefits listed above. To determine which controls in COBIT to adopt, ask:

- Which controls are appropriate for your environment?
- Of the appropriate controls, which will maximize your efforts?

After successfully identify and answering the questions, organizations will be in a position to balance cost and effectiveness for COBIT controls to improve their overall business.
Reference


