Trustworthy Computing

Project Report
Information Trust and Compliance Issues under Sarbanes-Oxley Act:
Case Study from Financial Service Industry

Professor: Dr. Michael J. Shaw

Submitted by: Shu-shu Chou,

MS-TECH schou3@uiuc.edu

May 4, 2006

TABLE OF CONTENTS

Abstract

This project is to explore the relationship with information trust and the SOX issue. The SOX compliance requirement require IT department to play a more proactive role in overall company management infrastructure. Therefore, a close look about the IT trust issues and governance topics are extremely important in post-SOX era. There are many research projects and papers address to this topic and the purpose of this project will focus on the application side in a financial industry

The content of the project includes the introduction about major SOX and IT compliance concepts and tools, the analysis of the application in financial industry. Included on the case study are two financial service companies, Allstate and Moody’s KMV. Conclusion and findings re-emphasize the importance on the close relationship with IT’s role in building a trust and compliance enterprise in the future.

I. Overview

This project is to explore the relationship with information trust and the SOX issue. The SOX compliance requirement require IT department to play a more proactive role in overall company management infrastructure. Therefore, a close look about the IT trust issues and governance topics are extremely important in post-SOX era. There are many research projects and papers address to this topic and the purpose of this project will focus on the application side in a specific industry.

The content of the project includes the introduction about major SOX and IT compliance concepts and tools, the analysis of the application in financial industry. Included on the case study are two financial service companies, Allstate and Moody's KMV. Both companies use IT control framework and tools to improve internal management risk and control process. COBIT framework is adopted in Allstate. On the other hand, Moody's KMV, with the assistance of a software solution, solved the possible internal security assess control issues to meet the SOX audit requirement.

Conclusion and findings re-emphasize the importance in the close relationship with IT's critical role in building a trust and compliance enterprise in the future.

II. Review of Literatures

1. Key Concepts and Managerial Issues

(1) Sarbanes-Oxley Act (SOX): (Summary from Protiviti Speaker about SOX speech)

Under Sarbanes-Oxley Act (SOX) was enacted in 2002; its goal is to create new accounting standards and accountability for financial statement. Not only the SOX specifies internal controls over financial data must be maintained, audited and reported; it also added penalties if CEO and CFO does not comply with the regulations. SOX contains 11 titles and each title has sections. Sections with impact on risk management include:

- Title 1: Section 101: creation of Public Company Oversight Board (PCAOB), reports to SEC
- Title 2: Auditor Independence rules
- Title 3: Section 302 states: principal financial officers or officers must attest to the accuracy of the financial report to be issues. Principal must certify that they are responsible for maintaining internal control, must also attest to the design of internal controls that maintain the accuracy of financial date, must report and changes in controls that my affect financial statements for the quarter.
- Title 4: Section 404 states: All annual reports must contain an internal control report. This states the responsibility of management to establish and maintain adequate internal controls. An assessment of the effectiveness of internal controls by management and the certified public accountant. A statement to the internal *control framework* chosen in the design of internal controls.
- Under the Section 302 require companies to choose a "sustainable" framework for internal controls be established and maintained. The available framework include: COSO, CoBIT, ITIL/CMMI. ISO 17799/27001. COSO and CoBIT will be introduced in the following sections.
- Title 9, section 905: Asks sentencing commission to consider the serious nature of fraud and ensure the penalties are severe enough to deter future fraud.

Role of IT in SOX has been critical because IT link critical business process and resources. In order to assist companies comply with SOX requirement, a close alignment with IT and business departments and functions is vital. Section 302 and 403 address most about IT's role in SOX compliance, the challenges to companies are: 1) Scope and identify controls, most companies do not have well-defined guidelines, or need to re-score controls for following audits, 2) Testing the controls: the control process need to examined and well-executed. Testing and controls will act as an indicator for operational effectiveness, 3) close the gaps: companies need to identify the SOX compliance issues during year 1 and year 2 testing must be fixed.

(2) IT Governance:

According to IT Governance Institute, “IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.”(ITGI, 2003)

Given the increasing importance and impact on IT in nowadays’ business operation, IT governance issues have gained more and more attention and become one of the management issues. From the figure shown below, it shows the focus areas of IT governance include the following areas:

1) Strategic alignment, how IT operations align with business goals , objectives and most importantly, business strategies.

2) Value delivery: how IT can provide value to business and optimize it’s performance

3) Risk management: how IT assist business to manage risk, such as safeguarding of IT assets, disaster recovery and continuity of operations.

4) Performance measurement, how IT performs and how to measure.

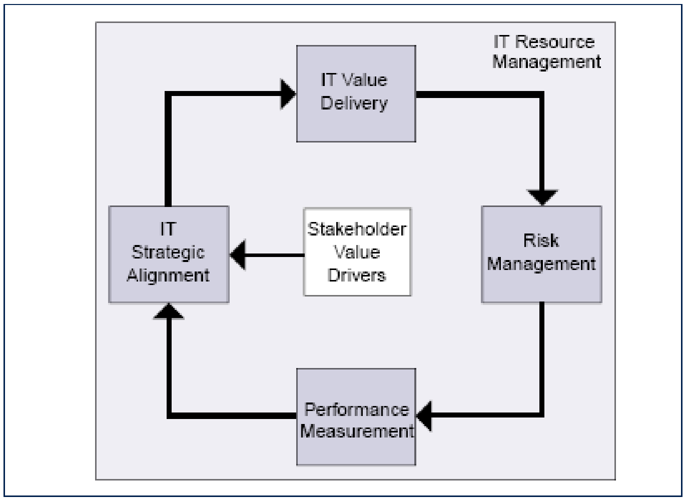


Figure 1. Focus Areas of IT Governance, source: ITGI

As we further look into the risk management area, there are several issues need to be examined:

- How to identify enterprise risks: financial risk, technology risk, information security, IT infrastructure vulnerability, etc.

- How does the board manage the enterprise risk? According to the IT governance Institute, it is recommended that the board should take the following ways to manage risks: 1) Ascertaining that there is transparency about the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance polices of the enterprise. 2) Being aware that the final responsibility for risk management rests with the board s, 3) Being conscious that the system of internal control put in place to manage risks often has the capacity to generate cost-efficiency, 4) Considering that a transparent and proactive risk management approach can create competitive advantage that can be exploited, and 5) Insisting that risk management be embedded in the operation of the enterprise, respond quickly to changing risks and report immediately to appropriate levels of management, supported by agreed principles of escalation. (ITGI, 2003)

- What is an effective risk management? An effective risk management should be able to implement control practices so that the risks can be mitigated or transferred. Otherwise, the enterprise should be able to acknowledge that risk exists and monitor it.

2. Key Techniques, Components, and Models

(1) COSO:

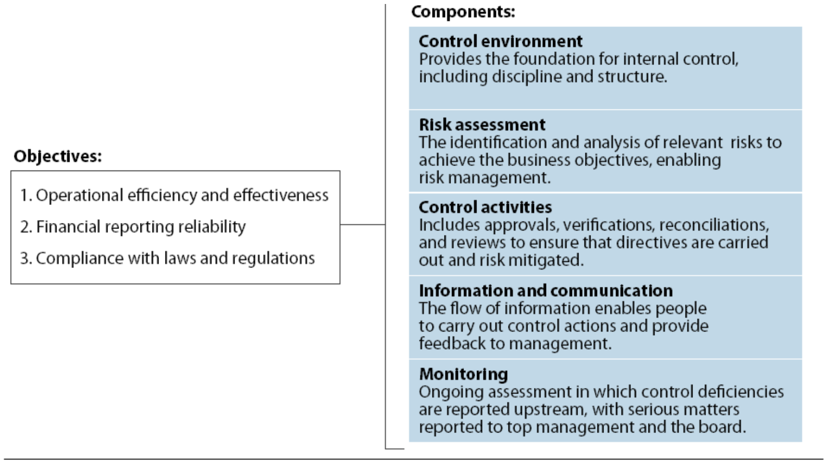
Issued by the Committee of Sponsoring Organizations of Commission (COSO), this Framework has ling served as a blueprint for establishing internal controls that promote efficiency, minimize risks, help ensure the reliability of financial statements, and comply with laws and regulations. (*Tone at the Top*, 2005)

A COSO framework is shown as below. There are five key components of internal control: 1) control environment, 2) risk assessment, 3) control activities, 4) information and communication, and 5) monitoring. The 26 fundamental principles of internal control associated with the above five components are:

- Integrity and ethical values
- Importance of board of directors
- Management’s philosophy and operating style

- Organizational structure
- Commitment to financial reporting competencies
- Authority and responsibility
- Human resources
- Importance of financial reporting objectives
- Identification and analysis of financial reporting risks
- Assessment of fraud risk
- Elements of a control activity
- Control activities linked to risk assessment
- Selection and development of control activities
- Information technology
- Information needs
- Information control
- Management communication
- Upstream communication
- Board communication
- Communication with outside parties
- Ongoing monitoring
- Separate evaluations
- Reporting deficiencies
- Management roles
- Board and audit committees
- Other personnel

The COSO framework as shown below



Objectives:

1. Operational efficiency and effectiveness
2. Financial reporting reliability
3. Compliance with laws and regulations

Components:

Control environment
Provides the foundation for internal control, including discipline and structure.

Risk assessment
The identification and analysis of relevant risks to achieve the business objectives, enabling risk management.

Control activities
Includes approvals, verifications, reconciliations, and reviews to ensure that directives are carried out and risk mitigated.

Information and communication
The flow of information enables people to carry out control actions and provide feedback to management.

Monitoring
Ongoing assessment in which control deficiencies are reported upstream, with serious matters reported to top management and the board.

Source: Forrester Research, Inc.

Figure 2 COSO Objectives and Components, Source: Forrester Research, Inc.

(2) COBIT

Control Objectives for Information and related Technology (COBIT®) was published by the IT Governance Institute® (ITGI). According to ITGI " The COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks . "

The COBIT includes four domain area, they are 1) planning and organization, 2) acquisition and implementation, 3) delivery and support, 4) Monitoring and evaluate. It continues with 34 high-level control objective, each address one IT process. A hierarchy diagram as shown below.

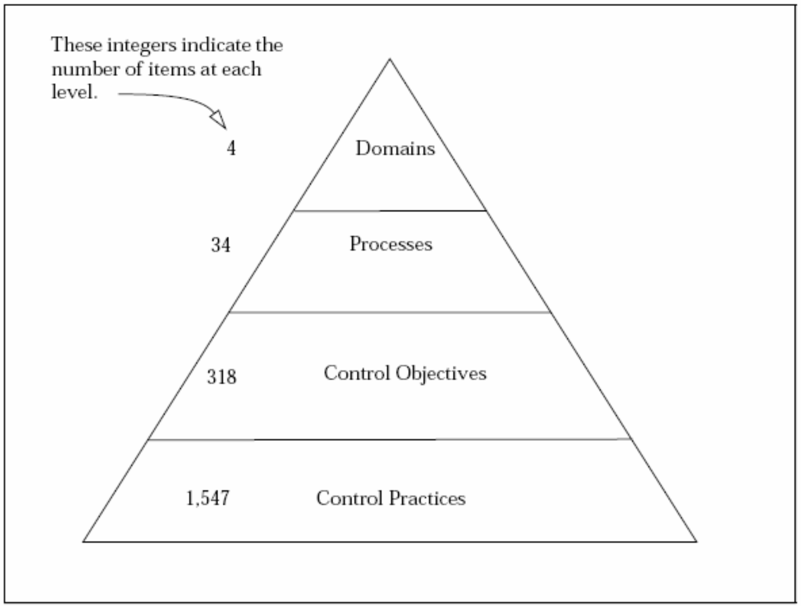


Figure 3. COBIT’s Hierarchy, Source: Campbell, 2005

According to Lainhart IV,J. (2000), the main objective of COBIT is to enable the development of clear policy and good practice for IT control throughout organization, worldwide. It is COBIT ‘s goal to provide these control objectives, within the defined framework, and obtain endorsement from world-at-large commercial, governmental, and professional organizations. Thus, COBIT is intended to be the breakthrough IT governance tool that helps in understanding and managing the risks associated with information and related IT.

III. Review of Applications and Practices

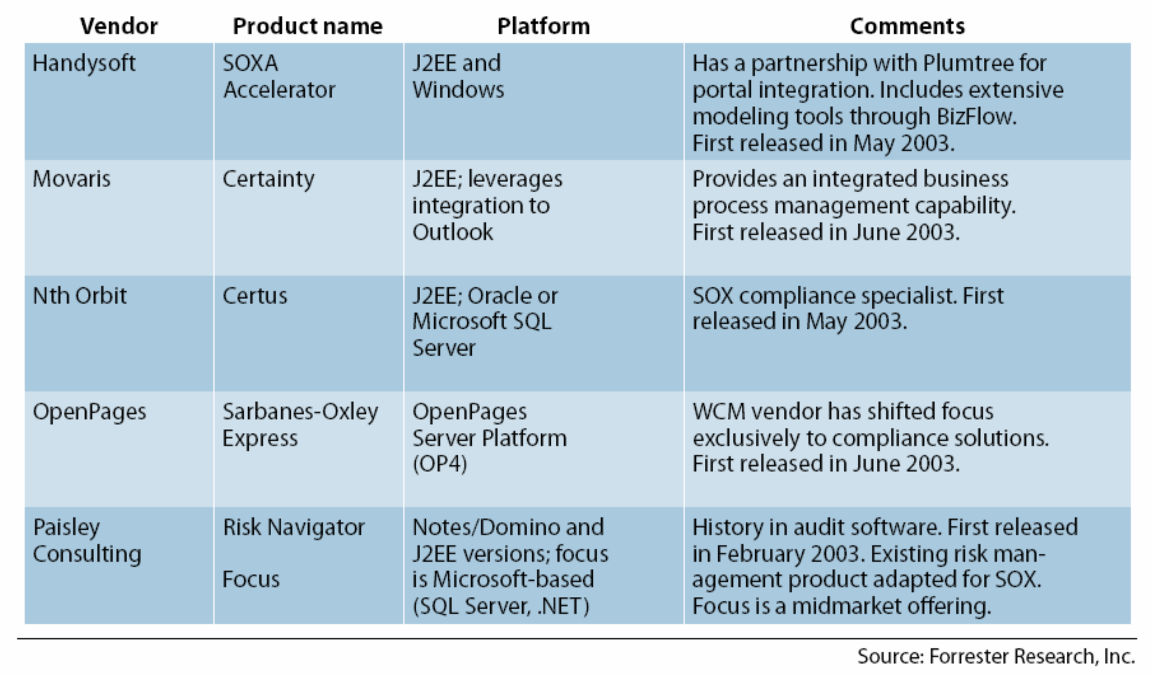
1. Technical Developments:

In order to assist companies to address the SOX compliance issues, there are many solutions available to provide services or packages. According Forrester research, the available SOX tools in the market including the following three type of vendors (Forrester, 2004)

(1) Specialist: These vendors have been the first to emerge and in most cases provide a more mature functionality. The struggle with integration to ERP systems – and currently, partnership with ERP vendors are weak.

(2) Major enterprise application vendors. The ERP systems provide the most complete integration with documenting controls and risks and reporting/monitoring. Their particular weakness? Document management and integration of records management capabilities.

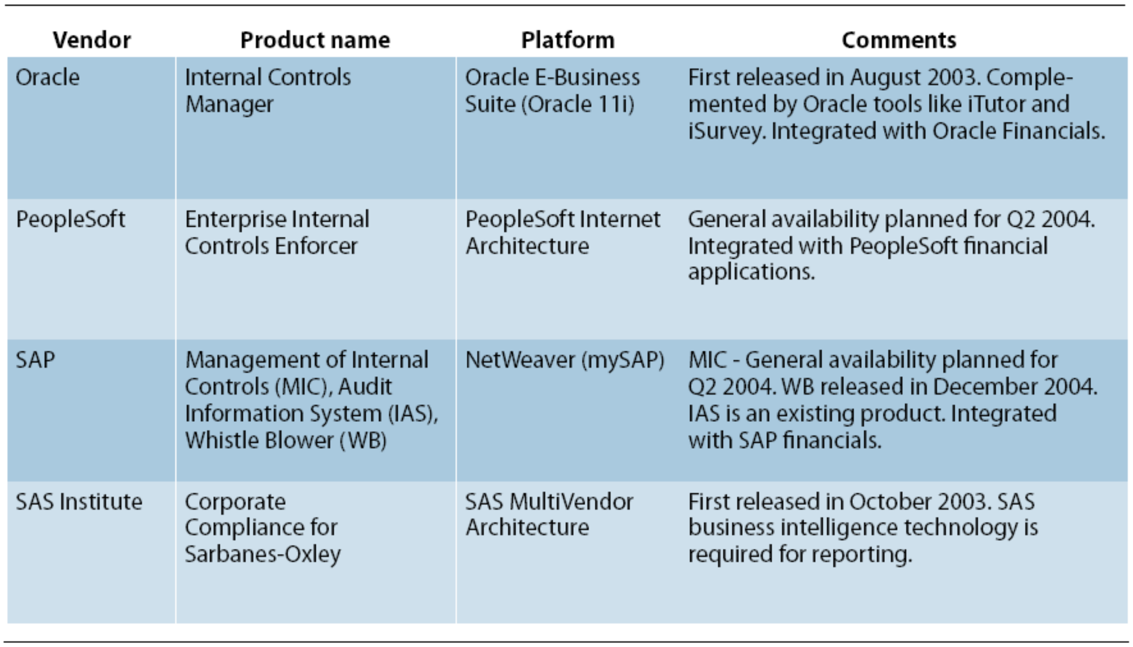
(3) ECM vendors. These vendors are providing both frameworks and SOX applications. The framework is a view of the potential future role for the ECM vendors as an integrated framework for SOX applications with particular strengths in document management, workflow, and records management. These solutions have light support for the COSO framework, which is a major component of Section 404 compliance.



Vendor	Product name	Platform	Comments
Handysoft	SOXA Accelerator	J2EE and Windows	Has a partnership with Plumtree for portal integration. Includes extensive modeling tools through BizFlow. First released in May 2003.
Movaris	Certainty	J2EE; leverages integration to Outlook	Provides an integrated business process management capability. First released in June 2003.
Nth Orbit	Certus	J2EE; Oracle or Microsoft SQL Server	SOX compliance specialist. First released in May 2003.
OpenPages	Sarbanes-Oxley Express	OpenPages Server Platform (OP4)	WCM vendor has shifted focus exclusively to compliance solutions. First released in June 2003.
Paisley Consulting	Risk Navigator Focus	Notes/Domino and J2EE versions; focus is Microsoft-based (SQL Server, .NET)	History in audit software. First released in February 2003. Existing risk management product adapted for SOX. Focus is a midmarket offering.

Source: Forrester Research, Inc.

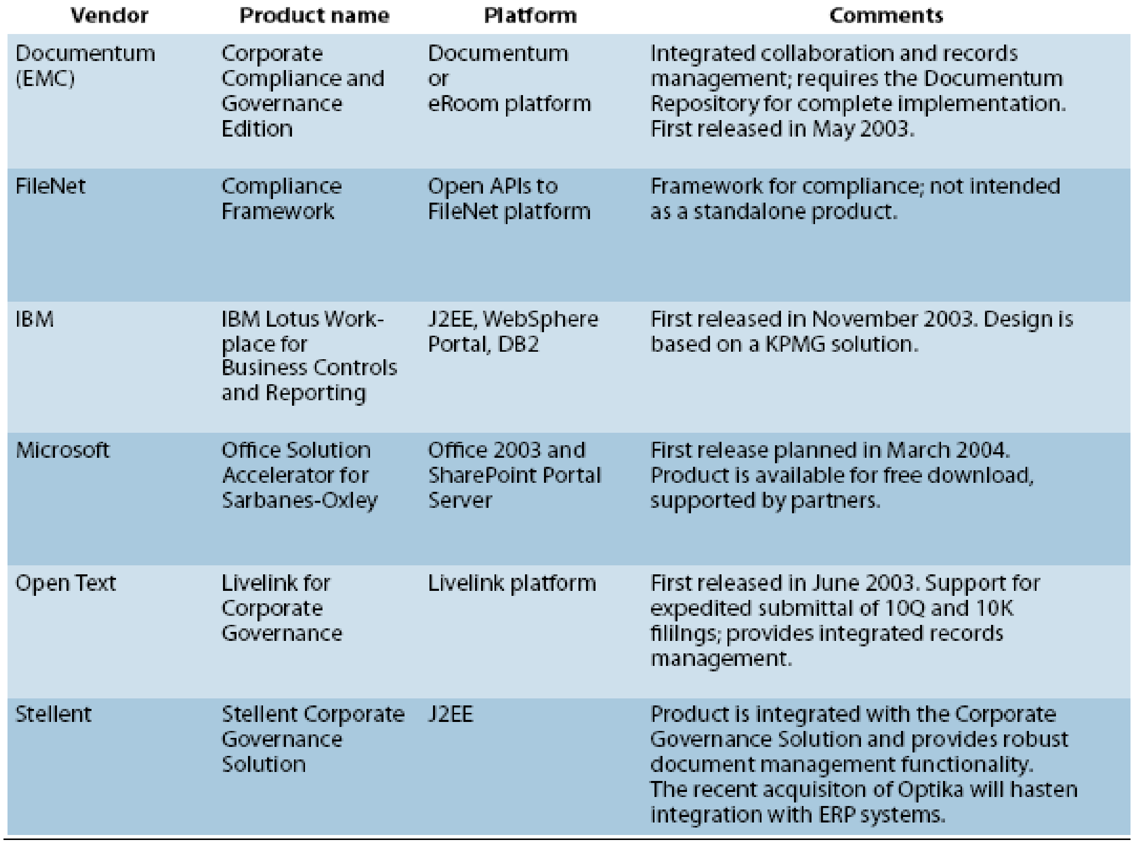
Figure 4: Specialist SOX Compliance Vendors, source: Forrester Research, Inc.



Vendor	Product name	Platform	Comments
Oracle	Internal Controls Manager	Oracle E-Business Suite (Oracle 11i)	First released in August 2003. Complemented by Oracle tools like iTutor and iSurvey. Integrated with Oracle Financials.
PeopleSoft	Enterprise Internal Controls Enforcer	PeopleSoft Internet Architecture	General availability planned for Q2 2004. Integrated with PeopleSoft financial applications.
SAP	Management of Internal Controls (MIC), Audit Information System (IAS), Whistle Blower (WB)	NetWeaver (mySAP)	MIC - General availability planned for Q2 2004. WB released in December 2004. IAS is an existing product. Integrated with SAP financials.
SAS Institute	Corporate Compliance for Sarbanes-Oxley	SAS MultiVendor Architecture	First released in October 2003. SAS business intelligence technology is required for reporting.

Source: Forrester Research, Inc.

Figure 5 SOX Compliance Solution from Enterprise Application Vendors, source: Forrester Research Inc.



Vendor	Product name	Platform	Comments
Documentum (EMC)	Corporate Compliance and Governance Edition	Documentum or eRoom platform	Integrated collaboration and records management; requires the Documentum Repository for complete implementation. First released in May 2003.
FileNet	Compliance Framework	Open APIs to FileNet platform	Framework for compliance; not intended as a standalone product.
IBM	IBM Lotus Workplace for Business Controls and Reporting	J2EE, WebSphere Portal, DB2	First released in November 2003. Design is based on a KPMG solution.
Microsoft	Office Solution Accelerator for Sarbanes-Oxley	Office 2003 and SharePoint Portal Server	First release planned in March 2004. Product is available for free download, supported by partners.
Open Text	Livelink for Corporate Governance	Livelink platform	First released in June 2003. Support for expedited submittal of 10Q and 10K fiilngs; provides integrated records management.
Stellent	Stellent Corporate Governance Solution	J2EE	Product is integrated with the Corporate Governance Solution and provides robust document management functionality. The recent acquisiton of Optika will hasten integration with ERP systems.

Source: Forrester Research, Inc.

Figure 6 : SOX solution from Enterprise Content Management Vendor, source: Forrester Research, Inc.

2. Managerial Practices:

How companies deal with the IT Governance and SOX issues? According to Forrester research, to comply effectively with SOX internal control requirements, companies need to move toward to the following best practices: (Forrester, 2004)

(1) Make internal control compliance a part of the company's culture. Internal control in the new compliance environment is a collaborative process. One best practice suggests that all line managers and those with direct involvement with financial processes are part of the internal control assessment and monitoring process, rather than confining this to internal audit specialists.

(2) Drive consistency and standardization in business processes. Companies with multiple division, multiple products, and geographically dispersed operations face a big challenge in bringing consistency to business processes that affect accounting and financial reporting. Consistency and standardization in processes and systems will strengthen the internal control environment, making SOX compliance easier.

(3) Make business managers and processes owners accountable. Although ultimate compliance accountability rests with the CEO and CFO, accountability must be distributed throughout the enterprise. This should be organized not only by the chain of command, but also by assigning responsibility to specific element owners of the char of account

(4) Invest in making compliance sustainable year after year. Most companies have efforts well under way for Section 404 compliance, as it becomes effective for companies with fiscal years endings after Nov. 15, 2004. Going forward, companies will move toward automating the management and execution of the compliance process.

IV. Case Study from financial service industry

In this section, we use two companies in financial industry to illustrate how SOX being reviewed and how IT helped to achieve the compliance issues. In Allstate, they use COBIT as a framework to evaluate IT risk and align business processes. On the other hand, at Moody's KMV, the company implement a software solution to address specific IT security control issues and thus to assist them comply with the SOX audit requirements.

1. Allstate

(1) Background: Allstate insurance is the largest publicly held property and casualty insurance company in the United States. It customer base is about and with asset of in 2005. More about Allstate company information can be found on http://www.allstate.com/

Since Allstate Internal Audit did not have a formal IT control framework in place prior 2000, a new director of internal audit reviewed the department and business environment, and the company decided to adopt COBIT as the IT governance model. It was expected the COBIT can demonstrate management that its use provided a structured means to ensure consistent and appropriate IT controls throughout the company. Goals for implementing COBIT focus on:

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

(2) IT/SOX Compliance Approach: After SOX Act was passed in the US. Allstate use COBIT to evaluate IT governance and control, and use COSO to evaluate business process control. Once of the first steps in Allstate's SOX approach was to define three phases for compliance procedure. Phase 1 focused on organizing and launching the plan, phase 2 included documentation and assessment workshops, and phase 3 concentrated on sustainment activities.

(3) IT/SOX solutions and benefits: At the phase 1, Allstate's IT audit team use three-level approach to define how the company views IT as below. According to ISACA, level 1 was for the business control owner (automated application controls such as interface controls, systems 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)

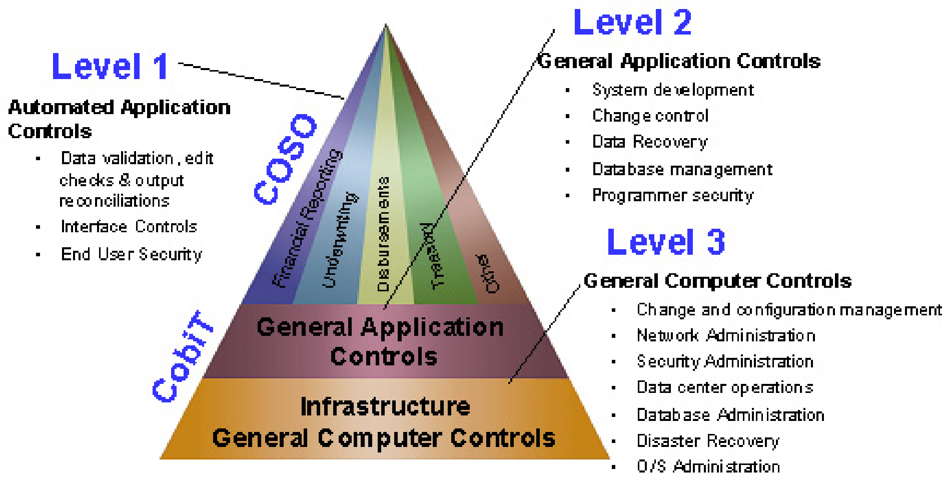


Figure 7 Allstate IT Control Framework, Source: ISACA

AT the stage, the IT risk assessment was performed in order to understand the relationship between IT objectives and SOX. As the risk assessment approach shown below, the company use the COBIT framework to understand and integrate different levels' control objectives. Issues has been defined and attestation readiness review were preformed in order to assure the compliance with internal audit requirements toward SOX.

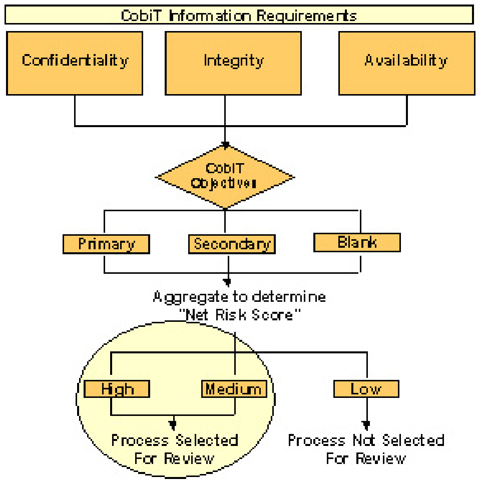

CobiT Information Requirements
Confidentiality
Integrity
Availability
CobIT Objectives
Primary
Secondary
Blank
Aggregate to determine "Net Risk Score"
High
Medium
Low
Process Selected For Review
Process Not Selected For Review

Figure 8 : COBIT Risk Assessment Approach, Source: ISACA

CobiT helps Allstate achieve the efficiency and effectiveness of IT control processes toward SOX compliance. Examples of benefits realized include: (ISACA)

- Edits early in the process reduced 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

2. Moody's KMV

(1) Company background

Moody's KMV is a subsidiary of Mood's Corporation, and is the world's leading provider of quantitative credit analysis tools to lenders, investors, and corporations. Moody's KMV serves more than 2,000 clients in 80 countries. Moody's KMV maintains database of corporate defaults and provide credit decision-support products for customers. More about Moody's KMV company and product can be found at www.moodyskmv.com

(2) IT/SOX Compliance Issues

According to the Industry Case Study by Verdasys, the compliance issues in Moody's KMV are (Verdasys, 2005)

- "Sarbanes-Oxley compliance is a critical business issue for Moody's KMV because it is vital that our company lead by example," said Mario Duarte, director of security, Moody's KMV.

- After the pre-audit revealed two issues that had to be rectified quickly if Moody's was going to receive attestation for its compliance with SOX. The first vulnerability identified in the company's existing controls was systems and database administrator's ability to freely access and modify executables and other system resources, such as dll files and OS logs – and the lack of any auditing or controls around such activity. The second issue identified in the pre-audit was a need for better separation of duties between different kinds of administrators and better auditing of routines system maintenance and change activities.

- Given the short period of time, it is impossible to implementing a new accounting application or procedure. Therefore the company found a on the self software solution to solve the database control/assess issues.

(3) IT/SOX solutions and benefits

With the help of Software Company (Verdasys) and solution, Moody's KMV established a set of best practices for the operation of its back-office financial application environment and implemented the appropriate controls and audit trail around user activity to satisfy the requirement of Section 404 of SOX as well as the expectations of its client. Today, Moody's KMV knows instantly who accessed its financial applications, systems and data, from which machine and application, and whether the use or modification carried out was appropriate. This allows the company to hold users accountable for the appropriate use of sensitive corporate data and the integrity of financial application and reporting processes.

V. IT Governance Trends and SOX Issue for Financial Service Industry

In this section, we will be discussing the emerging trends, applications, and issues about IT governance for financial service industry.

1. COSO Enterprise Risk Management – Integrated Framework

As current compliance focus on the risk control, COSO extend its previously issued *Internal Control-Integrated Framework* to a more border level into Enterprise Risk Management – Integrated Framework It address " how enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. (COSO, 2004)

The enterprise risk management – integrated framework is consisted of four objectives and eight interrelated components. The four achievement objectives are strategic, operations, reporting, and compliance. These are derived from the way management runs an enterprise and are integrated with the management process. These eight components are: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring.

According to Enterprise Risk Management – Integrated Framework Executive Summary, "there is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them." (COSO, 2004)

From above we may understand the IT compliance issues has been extended into corporate or enterprise level, instead of business operation or process. It is required that corporate officers fully commitment so that the post-SOX issues can be consistently being performed well and correctly.

2. Compliance Issues in managing post-SOX era

According to Deloitte, there are ten threats to compliance toward SOX 404 and organizations should pay attention to avoid. They are described as below.

(1) Lack of an enterprise-wide, executive-driven internal control management programs. A strong enterprise-wide, executive-driven internal control management program is essential to achieving section 404 compliance. The lack of a strong enterprise-wide internal control management program threatens compliance in some way such as absence of enterprise-wide internal control management casts serious doubt on executive's commitment to effective internal control.

(2) Lack of formal enterprise risk management program. Critical to the success of any internal control management program is the establishment of an enterprise risk management program- a formal, regular process designed to identify key financial reporting risks, assess their potential impact, and link those risks to specific areas and activities within the organization.

(3) Inadequate controls associated with the recording of non-routine, complex, and unusual transactions. Many organizations lack the technical accounting knowledge to record complex transaction correctly, and even competent employees are unlikely to have much experience. Errors in recording such transactions can require a company to restate its reported results, which in itself is considered a control weakness.

(4) Ineffectively controlled post-merge integration. Merging companies often neglect to explicitly address the need to establish a consistent internal control environment across the entire consolidation entity.

(5) Lack of effective controls over the IT environment. Section 404 marks the first that companies have been legally required to evaluate and test their controls in the IT environment in such depth and detail. The more complex a company's IT environment, and the less attention it has previously paid to IT controls, the more IT control gaps are likely to exist – and the more challenging and time-consuming they will be to fix.

(6) Ineffective financial reporting and disclosure preparation processes. Some companies may not possess the in-house technical accounting skills needed to prepare financial disclosures accurately. The problem is often compounded by the lack of a solid, rigorous process for collecting and organizing the information required to prepare the disclosures in the first place.

(7) Lack of formal controls over the financial closing process. The goal is to be able to document the closing process in enough detail to enable management to effectively evaluate the design of closing process controls and test their operating effectiveness. In addition, adequate

documentation of the closing process and the related controls enables the independent auditors to perform their required walk-through for the section 404 attestation.

(8) Lack of current, consistent, complete, and documented accounting policies and procedures. The more current, consistent, and complete a company's accounting policies and procedures, the easier they are to evaluate and document, and the more effectively the company can control associated risks.

(9) Inability to evaluate and test controls over outsourced processes. When companies outsourced activities, they often tacitly delegate the responsibilities for internal control to the outsourcers as well. The resulting lack of transparency into outsourcers' internal control environment has serious impact on organizations' section 404 compliance efforts.

(10) Inadequate board and audit committee understanding of risk and control. If the audit committee cannot establish that its members understand risk and control, the financial reporting process, and their responsibilities around section 404 compliance and other SOX issues, the independent auditor are unlikely to have full confidence about the company's internal control.

3. Implications to financial service industry

We use the above mentioned 10 threats to address how financial service industry can manage the continuous compliance SOX issues in the future.

Threats	Implication to financial service industry
(1) Lack of an enterprise-wide, executive-driven internal control management programs	Executive team should demonstrate full financial, logistical, and political support of the SOX compliance.
(2) Lack of formal enterprise risk management program	Perform a risk assessment at least once a year to keep the organization's financial reporting risk profile in line with the evolution of the business.
(3) Inadequate controls associated with the recording of non-routine, complex, and unusual transactions.	Company should involve appropriate subject matter experts to record complex transactions. Maintain, adequately document, and effectively disseminate standards procedure to be followed for unusual and complex transactions.
(4) Ineffectively controlled post-merge	Company should pay attention when proceeding

integration.	merging activities, especially when the acquired entity with very different IT system from its own.
(5) Lack of effective controls over the IT environment	Company should establish an IT-specific internal control framework to guide its section 404 compliance activities with respect to IT.
(6) Ineffective financial reporting and disclosure preparation processes.	Companies should have formal documentation of its disclosure process and controls. The disclosure development and review process should be documented to enable management to explicitly evaluate the design and test the operating effectiveness of the controls related to this process
(7) Lack of formal controls over the financial closing process.	Companies should establish formal procedures for executing and documenting both the financial closing activities themselves and their associated control activities.
(8) Lack of current, consistent, complete, and documented accounting policies and procedures.	Companies should consistently and systematically reviewed and revised during times when changes to the business and to generally accepted accounting procedures (GAAP) render them obsolete.
(9) Inability to evaluate and test controls over outsourced processes.	Companies should maintain a process to monitor the level of service that it receives from outsourcers, including a procedure to monitor changes. In the mean time, service contract should include the right to perform an internal control audit.
(10) Lack of an enterprise-wide, executive-driven internal control management programs	Board members should be well versed in the general requirements for section 404 compliance, and they should be familiar with their own, managements, and the independent auditors' key responsibilities in the attestation process.

VI. Conclusions and Findings

There are three findings in the report as followings:

1. Framework is critical:

When companies managing the SOX compliance issues. The complicated requirement and importance related is critical. Therefore to ease both the implementation work and communication of risk control in organization. A framework is required and adopt by most companies. COSO and CoBIT have been adopted as a starting point for companies to assess the risk control and guide in identify compliance issues under SOX.

2. Tools and application in SOX operation integration:

Given the importance and timing for meeting the SOX and internal audit trial requirement. Companies may look for outside vendors to expedite the process. Several available solutions and packages have been discussed in the report and found most of them are add-on based on enterprise application. Companies may check the existing infrastructure and look for application that can meet special requirement under SOX, such as record, documentation or security management solutions.

3. Synergy in IT trust and governance with SOX regulation

The essence of SOX compliance issues would be “under control”. Therefore a reliable and consistent IT governance framework and operation play key role to companies under SOX requirement. On the other hand, we may say the requirement by SOX help companies address the business risk issue from the top and make it a company task with regulatory by government. The synergy in IT trust and governance help organization builds a trustworthy environment from every business operation and processes.

Appendix: Reference

1. Lainhart IV, J (2001).COBIT: A Methodology for Managing and Controlling Information and Information Technology Risks and vulnerability. *Journal of Information Systems*. *14*, 21-25.

2. "Putting COSO Theory into Practice," *Tone at the Top*, The Institute of Internal Auditors, November 2005 (PDF).

http://www.theiia.org/download.cfm?file=42122

3. The Committee of Sponsoring Organizations of the Treadway Commission (COSO)., (2004) *Enterprise Risk Management – Integrated Framework: Executive Summary*, COSO

4. The IT Governance Institute (ITGI), 2003, *Board Briefing on IT Governance*, second edition, IT Governance Institute

5. ISACA, COBIT and IT Governance Case Study: Allstate. Retrieved April 3, 2006, from IT Governance Institute Web site:

http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=13502&TEMPLATE=/ContentManagement/ContentDisplay.cfm

6. Verdasys, (2005). Privileged User Management and Financial System hardening for Sarbanes-Oxley Compliance. Retrieved April 06, 2006, Web site:

http://www.verdasys.com/pdf/CSMoodys.pdf

7. Forrester, March 11, 2004, *Sarbanes-Oxley Solutions-Invest or Pay Later* by Paul Hameerman and Robert Markham

8. Protiviti, 2006, The Sarbanes Oxley Act of 2002, presented on Feb. 16, 2006 by Mr. Deron Grzetich

9. “Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements," Protiviti, Inc, March 2003

http://www.protiviti.com/portal/site/pro-us/?pgTitle=Sarbanes-Oxley%20Section%2020404%20FAQs

10 Campbell, P., 2004, A COBIT Premier, Sandia National Laboratories,

http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=22339&TEMPLATE=/ContentManagement/ContentDisplay.cfm