Term Project

Sarbanes-Oxley Act (SOX)

Hiroshi Tachibana (MBA 2nd)

Sarbanes-Oxley Act (SOX) was established in 2002 in order not to repeat company and accounting scandals which occurred from later 1990's to early 2000's, such as that of Enron and WorldCom. To avoid these scandals, the purpose of SOX is to increase the transparency and accuracy of the financial report and business accounting. Additionally, SOX requires the company to reform the corporate governance and audit system and defines the duty and responsibility for business executives. It is composed of 11 titles and 69 sections and is including the installation of Public Company Accounting Oversight Board (PCAOB), the independent of the auditing firm, the expansion of financial disclosure, the mandatory of internal control, stricter penalties for business executives who committed a fraud, the regulation for investment analysts, the protection for whistle-blower and so on. We should take particular note of SOX section 404. It is regarding the assessment of internal control. The internal control is one of the biggest parts and that company takes much time to do it.

First of all, we should understand what an internal control is. The purpose of an internal control is also to avoid a fraud within the company. Establishment of an "internal control system" for preventing illegal acts by directors and employees has been made mandatory. This is directed to ensuring the achievement of the two goals of corporate governance, namely, improvement of efficiency and competitiveness and maintenance of corporate soundness and compliance (with the law and corporate ethics). The system is seen as a foundation for ensuring a company's credibility. To certify that an internal

control is adequate, the company has to submit a report approved from an external auditing firm. This is costly a lot for the company to implement because it has to prepare a lot of documents for important financial manuals and conduct tests for automated controls. Also, the section 404 requires managements to make up an "internal control report" as one of annual Exchange Act report. For these reports, we need to use framework for the internal control. The framework is also known as "COSO" report which was proposed by the Committee of Sponsoring Organization of the Treadway Commission for the framework of an internal control. As a matter of practice, COSO has become a global standard in recent years.

When it comes to an internal control, we have to know what COSO is because this method is a global standard for an internal control. As a background of COSO, there were some accounting frauds and failed companies from 1970's to 1980's in the United States of America. The American Institute of Certified Public Accountants (AICPA) had a sense of crisis about these scandals. It approached several institutions and established the Treadway Commission as industry-academic-government project in 1985. Treadway Commission released "Report of the Commission on Fraudulent Financial Reporting" in 1987 and advised public companies, external auditing firms, Securities and Exchange Commission (SEC), several administrative agencies, and some educational agencies. There was one of the biggest issue that was how and what we should define an internal control and develop a common framework for an internal control at that time. However,

the biggest issue left because Treadway Commission ceased its activity before solving the issue. Although COSO was originally an association which supported Treadway Commission financially, it started its activity for a prevention of fraud and an internal control as the main body after the Treadway Commission advised. COSO also delegated the tasks to Coopers & Lybrand, current PricewaterhouseCoopers, made up the report, "Internal Control – Integrated Framework". It was also called COSO report and composed of five different documents. In this report, it showed us specific methods and framework for internal control such as an evaluation tool for internal control in addition to basic theory and vision of an internal control. This framework is still called the internal framework of COSO or COSO framework. COSO framework changed the concept of an internal control which was thought as the activity for the adequate financial report. The concept was compliance and observation of management policy and operation rules in the COSO framework.

I would like to mention how COSO defined an internal control. The goals for an internal control are operating effectiveness and efficiency, reliability of financial statement, and compliance of related regulations as exhibit 1 shows. To achieve these goals, the organization has to secure radical processes provided by board of directors, employees, and corporate managers thorough an internal control. Additionally, COSO defines monitoring activity, information and communication, control activity, risk

evaluation, and environment for control as standards when we evaluate an internal control.

[Exhibit 1]

COSO framework is a reference model for thoroughly implementing an internal control to organization members including corporate manager. Each policy which was customized in accordance with each condition was released in each country and field and was based on original COSO framework. That is why COSO framework became a global standard as a matter of practice. The Control Objectives for Information and related Technology (COBIT), known as framework for information technology (IT), is also based on COSO framework. When we deal with an internal control, we cannot get by with avoiding

IT control. COBIT plays a major roll in IT control and governance. Next I would like to show you what COBIT is.

COBIT is practical standard advocated by Information Systems Audit and Control Association (ISACA) for companies and autonomous communities as the policy of IT governance. COBIT is useful for not only SOC 404 but also section 302 requiring a suitable framework for internal controls established and maintained. The first edition published in 1996 and the current version is COBIT 4.1. However, COBIT 4.1 has no big changes from COBIT 4.0 and has little refinement for more useful. One of the most characteristic things for COBIT 4.0 is the maturity model of management process. The maturity model has 5 levels of maturity. These are called “Initial, Repeatable, Defined, Managed, and Optimizing” for each level. When the management uses this maturity model, the management gets to know the actual ability and condition of the company and the industry, what the objectives for improvement are, and what growing path is between the current and future. It is very practical and easier for company to implement. COBIT is used for evaluation for IT investments, decision for IT risks and control, and standard for system audit. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company. COBIT is composed of four domains,

34 high-level control objectives, and 318 corresponding detailed control objectives as exhibit 2 shows.

[Exhibit 2]

COBIT Control Objectives			
Planning and Organizing	Acquisition and Implementation	Delivery and Support	Monitoring
-Strategic Planning -Information architecture -Technological direction -IT organization and relationships -Manage the IT investment -Communicate aims and direction -Manage human resources -Ensure compliance -Assess risks -Manage projects Manage quality	-Identify solutions -Acquire and maintain application software -Acquire and maintain technology architecture -Develop and maintain IT procedures -Install and accredit systems -Manage changes	-Define service levels -Manage 3rd-party services -Manage performance and capacity -Ensure systems security -Identify and attribute costs -Educate and train users -Assist and advise IT customers -Manage the configuration -Manage problems and incidents -Manage data -Manage facilities -Manage operations	-Monitor the processes -Assess internal control adequacy -Obtain independent assurance -Provide for independent audits

As I already mentioned, the company has to spend much costs and time for SOX especially an internal control, although it is very important for the company. We have to find needless work for SOX and reduce costs and time for it. As a good example, I would like to show you an approach of a company from the end of 2004 to the beginning of 2005 when SOX started. Most companies which close account from the end of November to the end of December developed systems for governance, set up smoke detector, sent

receipts to accounting firm and so on. These were for SOX and those companies were so hectic days. However, most processes CIOs developed for an internal control were hand working. Companies which purchased software regarding SOX were less than a thousand in 2004. Those software had been put in action yet. Additionally, companies added extra items for an internal control because they were worrying about being pointed out flaw. As a result, they had to have many unnecessary operations. If they continued to have these unnecessary works for SOX, they would have to have huge waste costs and time for it because check points would not be the same with that of last year. For example, if CIO assigned someone in charge for checking auditing log, the company has to be certified what the job is effective periodically. In short, we have to know that SOX is the process conducted by the company semi-permanently.

How should we work on SOX? First of all, we should cut items which are not required by SOX. Second, we should automate processes for SOX as much as possible. If you can check the log of auditing and do the documentation on the computer, your company reduces much costs and time for it. To achieve this, CIO has to prioritize control items to automate. Although CIO may take a couple of years to do it, not only CIO and IT department but also auditing firm are able to reduce much costs and time when it happens. It is also necessary for the company not to be too willing to agree with external auditing firm. Admittedly, the company has to get certification for the external auditing

firm for the report of SOX. However, the company may have unnecessary works when it is too willing to agree with the firm.

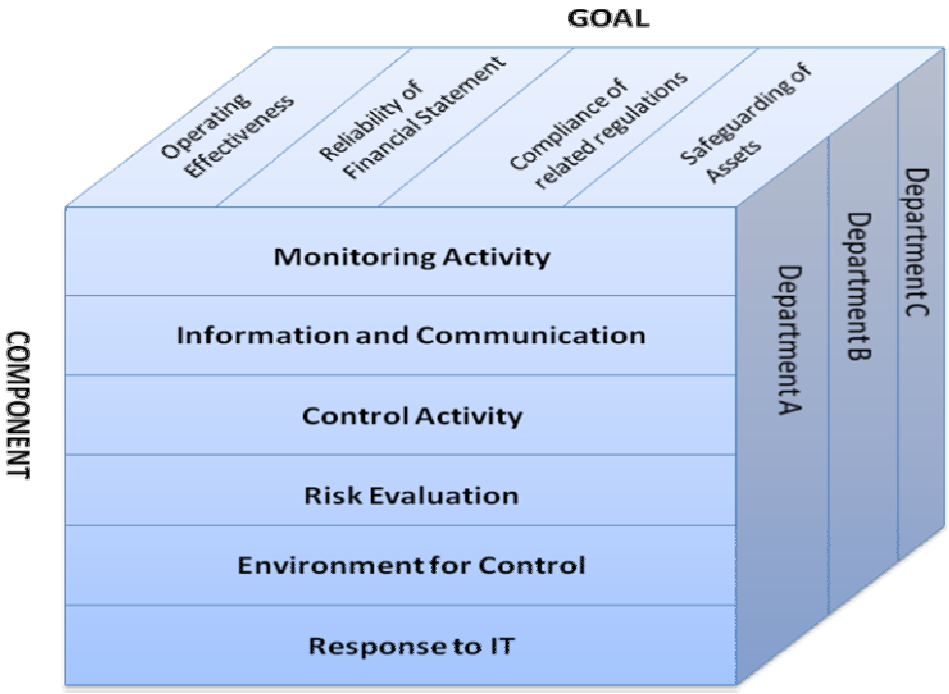
At first, in 2004, most CIOs thought SOX was almost not related to IT department but only to Finance department. However, CIOs realized that SOX was not completely unrelated to IT department a little while later, they had not known how much they would have impact by SOX until late 2004. At least, they had not believed that they would have had to spare their costs and time at all. Those CIOs realized that IT played a major roll in reporting of exact financial data based on SOX. However, they did not have enough time and had no choice to obey instructions from auditing firms and consulting firms. These auditing and consulting firms thoroughly required CIOs to develop framework for IT governance. Most auditing firms adopted COBIT and IT infrastructure Library (ITIL), best practices for IT management, because there were no guidance for IT system audit at that time. Although COBIT was great framework, not all of them needed SOX. CIOs were totally dependent on these frameworks in order to observe SOX. As a result, they spent much waste costs and time.

We can learn from these problems and should know solution not to repeat them again. First of all, CIOs need to take in control required by SOX for the day-to-day business in the IT department. Another thing is that CIOs has to thoroughly understand what SOX section 404 is. They also have to know what they do not need to include all control

related to computer in SOX. We can focus on some of IT control which is very important by ignoring other IT control being less important.

In Japan, Japanese version SOX based on original SOX had been needed because securities market and economy also were threatened by accounting fraud just like the United States. It became effective from April 2008 (accounting settlement in April 2009) because the fiscal year of most Japanese companies ends at the end of March. What is the difference between SOX and Japanese version SOX? Although Japanese version SOX is similar to original SOX, the most different points are that safeguarding of assets is added to the goal of SOX and response to IT is also added to the component as exhibit 3 shows.

[Exhibit 3]



The importance of IT was also mentioned by COSO framework but Japanese version SOX articulated that of IT. It seems Japanese version SOX needed rules suited to the times because original SOX was based on COSO report published in 1992, more than 10 years ago. The application of IT is meaning that the company decides adequate vision or policy and process in advance and adequately responds to internal and external IT. This is divided between respond to environment for IT and IT application and control. Respond to environment for IT is to decide adequate process and policy dependent on IT penetration in the market and society and IT application within the organization. IT application and control are composed of IT business processing control and IT overall control.

Not all operations are needed IT application by Japanese version SOX. Each company can decide which operation needs IT application for the company. However, Japanese version SOX forces companies to invest much cost for IT. Additionally, it is easy for us to predict too hectic for the company to work well because next April will be the first year for Japanese version SOX.

I would like to discuss challenges for the future of SOX. First of all, the company has a lot of trouble for the costs of Japanese version SOX like the company in the United States when SOX became in effective. However, the costs will be going down within a couple of years because initial investment is not necessary for the company after the first year and operational cost will drop by learning operation. Second, we have to recognize

the limit of the internal control. Person in charge of an internal control makes a careless mistake. Unexpected deal is come up. Persons in charge of an internal control commit a fraud do something dishonest in conspiracy. Manager of the internal control ignores rules of the internal control. These things cause defective functional activity for an internal control. Finally, some companies feel to doubt positive effect by SOX or an internal control, although they spent much cost for it. To increase cost performance, companies have to invest not only for SOX but also improvement for their performance by using IT control and an internal control from now on.

Reference

- http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
- http://en.wikipedia.org/wiki/COBIT
- http://en.wikipedia.org/wiki/COSO
- http://www.atmarkit.co.jp/aig/04biz/jsox.html
- http://www.shukuzawa.com/diary/daiary060206.html
- Lecture Summary about IT Governance and Control