COMPARATIVE ANALYSIS OF IMPLEMENTATION OF THE SARBANES-OXLEY ACT SECTION 404 CASE STUDY IN COMPANY A AND COMPANY B

THESIS

ALI ANDI IMRAN

0606146002

UNIVERSITY OF INDONESIA
FACULTY OF ECONOMICS
MAGISTER OF MANAGEMENT PROGRAM
JAKARTA
AUGUST 2009

COMPARATIVE ANALYSIS OF IMPLEMENTATION OF THE SARBANES-OXLEY ACT SECTION 404 CASE STUDY IN COMPANY A AND COMPANY B

THESIS

Submitted to fulfill one of the requirements to obtain degree of Magister Management

ALI ANDI IMRAN

0606146002

UNIVERSITY OF INDONESIA
FACULTY OF ECONOMICS
MAGISTER OF MANAGEMENT PROGRAM
JAKARTA
AUGUST 2009

STATEMENT OF ORIGINALITY

This final paper represents my own effort,
any idea or excerpt from other writers in this final paper, either in form of publication or in other form of publication, if any, have been acknowledged in this paper in accordance to the academic standard or reference procedures

Nama : Ali Andi Imran
Student Number : 0606146002
Tanda Tangan :

Tanggal : August 28, 2009

HALAMAN PENGESAHAN

Karya Akhir ini diajukan oleh	:
Nama	: ALI ANDI IMRAN
NPM	: 06 06 14 600 2
Program Studi	: **MAGISTER MANAJEMEN**
Judul Karya Akhir	: Implementation of the Sarbanes-Oxley act section 404 in Indonesia.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Manajemen pada Program Studi Magister Manajemen, Fakultas Ekonomi, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : **DR. ANCELLA A. HERMAWAN** ( )

Penguji : THOMAS H. SECOKUSUMO, MBA ( )

Ketua Penguji : DR. LINDAWATI GANI ( )

Ditetapkan di : Jakarta

Tanggal : 21 Agustus 2009

PREFACE

If thousand words can not describe a picture, then even thousand pictures will not be enough to describe my feeling when this report was finished. Nothing would be more relieving than getting one step closer to the end of the MM MBA program. What I was before, I am now and I will be someday is pretty much influenced by my surroundings. They all have significant impact to the course of my journey, and for that, I want to give my warmest and sincerest thanks to these following individuals.

1. Prof. Rhenald Kasali, Ph.D as Director of Master Management Program of Faculty of Economics, all lectures and all staffs of MM-FEUI for their assistance and support during the period of my study in MM-FEUI
2. Dr. Ancella A. Hermawan, my thesis supervisor who patiently guide me through this final phase of the program, with her endless comprehension, support, and suggestion.
3. My beloved parents, my sisters, and my big family for everything which I can not mention in detail. I hope you all proud of me.

If every end is actually a new beginning then this report, along with all of its imperfection, should never end at the moment when study time ends. Constructive critic, suggestion, and recommendation would cover the knowledge's constraint reflected in this report. It would also help its development into something better, more complete, and needless to say, more useful. By this, hopefully, this report would at least, not follow the same faith as others - lost and forgotten in the silence of time.

Jakarta, August 2009

Author

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah

ini:

Nama : Ali Andi Imran

NPM : 0606146002

Program Studi : Magister Manajemen

Jenis karya : Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Comparative Analysis of Implementation of the Sarbanes-Oxley Act Section 404 Case Study in Company A and Company B

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 28 Agustus 2009

Yang menyatakan

(Ali Andi Imran)

ABSTRACT

Name : Ali Andi Imran
Study Program : Magister Manajemen
Title : Comparative Analysis of Implementation of the Sarbanes-Oxley Act Section 404 Case Study in Company A and Company B

There are some Indonesian companies that must comply with the Sarbanes-Oxley Act (SOX). This requires a great effort that will cost a substantial amount of money and time. The aim of this thesis is to compare how two companies have managed to implement SOX Section 404. This study concentrates only on two Indonesian companies which are registered with the Securities and Exchange Commission (SEC), and are thereby required to comply with SOX. A bibliography and qualitative study was conducted to analyze the two companies. The research showed that SOX has had a great impact on Indonesian companies. The process of implementing SOX into Indonesian companies has been an extensive project. There is a difference between the approaches used for the implementation. Public Accounting Firms or Consultants Firms have been used to a large extent by the two companies.

Key Words:
Sarbanes-Oxley Act, SOX, Internal Audit, Internal Controls

TABLE OF CONTENT

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background

The American company Enron was the seventh largest company notated on the stock market when it went bankrupt due to extensive accounting frauds in December 2001. By manipulating the financial reports, the management of Enron was able to hide huge debts through transactions with external companies. Therefore, they were able to deceive the public by reporting huge profits while the company, in reality, was generating a negative result. As a result of the bankruptcy, 40 billion dollars disappeared and tens of thousands of employees lost their jobs and pension savings. Furthermore, Arthur Andersen, the then fifth largest accounting firm in the world and the external auditor of Enron, was convicted for destroying important documents for the on-going investigation of fraud in Enron. The conviction of Arthur Andersen prohibited them to audit public firms, leading to Arthur Andersen's collapse. After the Enron scandal, further accounting frauds were discovered in the US, such as WorldCom and Tyco. The WorldCom bankruptcy is, as of today, the largest bankruptcy in the world. Following the scandals and the accounting frauds in a number US companies, the US congress passed a law - the Sarbanes-Oxley Act of 2002 (SOX).

The goal of SOX is to protect the investors and give them a better insight into firms, increase the reliability of information given by them and restore the confidence of investors. President Bush described the Act as "one the most far reaching reforms of American business practices." This statement was an understatement on many levels, as the Act does a great deal more than just reform the laws applicable to the US based issuers, a considerable number of the Act's requirements reach abroad to have an effect on foreign private issuers whose securities are traded in the US, including Indonesian companies.

A central part of the Sarbanes-Oxley Act is section 404, Management Assessment of Internal Controls that obliges the management the responsibility to establish a system for internal control that guarantees the quality of the financial reports. According to SOX 404 sufficient internal control will assure that no material weaknesses appear in the financial statements. CFOs and CEOs have to certify in writing that appropriate operational controls are adapted. The written report is then reviewed by an external auditor who can remark on errors as well as possible flaws and material or substantial deficiencies.

In the case of SOX, the SEC is responsible for setting rules to implement the Act's provisions. The Securities and Exchange Commission (SEC) is the agency responsible for administrating federal securities laws in the US. Those rules include, for instance, guidance for reporting by the CEO and CFO on the company's internal control over financial reporting and disclosure controls.

1.2 Problem Statement

The legislation of the Sarbanes-Oxley Act has received critique for being enacted too quickly and has been considered as a hasty and rash law. The first year of compliance with Section 404 resulted in large expenses and complicated issues to solve for companies with deadlines in year 2004. Many companies did not know how to approach the legislation or how to institute the implementation.

Due to the lack of clear guidelines when implementing Section 404, some companies have requested external entities such as Public Accounting Firms or Consulting Firms to assist them in implementing Section 404. The researchers would like to increase their understanding on how to create conditions to successfully implement and comply with the Sarbanes-Oxley Act. Other interesting issues would be which problems companies have experienced, how they resolved them and if there are any significant factors to success.

The study will be conducted at two Indonesian companies that have to comply with the Sarbanes-Oxley Act, that are registered with the Securities and Exchange Commission.

Considering the problem discussion, the researcher formulated the following research question:

How have two companies implemented the Sarbanes-Oxley Act of 2002 section 404?

In addition to the main research question, the researchers intend to investigate:

Have there been any similarities or differences between between the organizations when implementing SOX section 404?

1.3 Purpose of Study

The purpose of the study is to compare how two companies have managed to implement SOX Section 404. The researcher will explain how different Indonesian companies have approached the issue and how they have chosen to implement SOX section 404 in their organization. The researchers' aim is to discuss the different approaches and enlighten the problem areas that organizations have experienced during the SOX implementation

1.4 Limitations

SOX cover several areas around internal control and reporting. The research will mainly study Section 404, which treats internal control over financial reporting, and is the section that has demanded most effort to comply with. And due to the limitation of data, research will be conducted at two Indonesian companies.

1.5 Methodology

In order to collecting data and conducting analysis, the following activities are performed:

a. Literature research

Data collected from books, journals, and articles with regard to strategy is used as a supporting tool of the analysis and strategy formulation.

b. Field research

Field research has been done through interviews with people within the organizations which are highly involved in the work with SOX. The intention of the interviews has been to test the existing theory and its relationship to empirical evidence, but also to compare and distinguish the chosen approaches for SOX implementation by the organizations covered in this paper.

CHAPTER 2
LITERATURE REVIEW

2.1 Internal Control

The COSO definition states that internal control is a process and that the level of internal control is affected by all personnel within an organization. It is designed to provide reasonable assurance regarding the achievement of objectives in the following categories (COSO, 2006b):

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The first category relates to an organization's basic business objectives, including performance, profitability goals and safeguarding of resources. The second part relates to the publishing of reliable financial statements and selected financial data derived from those statements, such as earnings releases, reported publicly. The last category addresses the compliance to those laws which applies to the organization.

In this study, internal control is a process in which the organization secures the accuracy of the financial statement and corporate disclosure.

2.2 Sarbanes-Oxley Act of 2002 (SOX)

The Sarbanes-Oxley Act is the U.S. public company accounting reform and investor protection act. It was passed and signed by President George W. Bush in 2002 in response to high-profile business failures, such as Enron and WorldCom, in order to reinforce investment confidence and protect investors by improving the accuracy and reliability of corporate disclosure (AICPA, 2007). SOX is a very complex act which demands that organizations goes through major changes to secure that they comply with the regulations. In short and in comparison to the time before SOX was established, the act demands that companies must reach a much higher level of certainty concerning that their company disclosure is accurate.

2.3 SOX Section 404

SOX Sec. 404 has perhaps been the most demanding and difficult part of the act to implement for organizations according to the widespread opinion. The paragraph forces the organization to ensure that the company has sufficient internal control to avoid any errors in the financial statement that might subsequently mislead investors and stakeholders. Section 404 demands that the internal control must be documented and tested so that no errors are made in the financial statement. No further directives or guidelines are made. However, in practice, most organizations must do the following:

- Identify risks
- Decide how to handle the risks and implement controls
- Document and test the processes and controls
- Create a written assessment on how the controls are working that will be signed by the management and reviewed by an independent auditor

Below is Section 404 of the Sarbanes-Oxley act in its original format.

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate

Source: U.S. Government Printing Office, (2002)

2.4 Implementation of SOX Sec. 404

Brown, (1993) describes an implementation as; fulfilling (an undertaking), put (a decision or plan) into effect or satisfying or fulfilling a condition, hence, it is the realization of certain criteria. When implementing a law, an organization should apply it accordingly to its design and purpose. In this study, when mentioning implementation, it refers to organizations that have, or are in the process of improving their internal control for the purpose of permanent compliance with Sec. 404 of the Sarbanes-Oxley Act of 2002.

2.5 Securities and Exchange Commission (SEC)

The Securities and Exchange Commission (SEC) is the US governmental institution that serves to enforce and uphold the laws and regulations that regulates the American financial market. SEC's main mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation (SEC, 2007).

The laws that govern the US securities industry derives from the concept that all investors should have access to certain basic facts about an investment prior to buying it, and as long as they hold it. To achieve this, SEC requires that public companies disclose meaningful financial and other information to the public. Thus, only through the steady flow of timely, comprehensive and accurate information can people make sound investment decisions.

The SEC oversees key participants in the securities industry, including securities exchanges, securities brokers and dealers, investment advisors and mutual funds. In addition, they provide guidance on how to implement SOX. The SEC is primarily focused on promoting the disclosure of important market-related information, maintaining fair dealing and protecting against fraud.

The SEC's effectiveness in these areas highly depends on its ability to enforce the regulation that applies to the securities industry. Each year the SEC brings hundreds of civil enforcement actions against individuals and companies for violation of the securities laws. Typical violations of the laws include; insider trading, accounting fraud, and providing false or misleading information about securities and the companies that issue them (Ibid).

The Sarbanes-Oxley act of 2002 is one of the laws that go under the SEC's jurisdiction. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud. Furthermore, the creation of the Public Company Accounting Oversight Board, also known as the PCAOB, was made due to the establishment of the Sarbanes-Oxley act. The latter reform was done to oversee the activities of the auditing profession.

2.6 Public Company Accounting Oversight Board (PCAOB)

The PCAOB is a non-profit organization, created by SOX, to oversee the auditors of public companies to ensure that private investor interests are protected, and to ensure that the audits of public companies are informative, fair, and independent (PCAOB, 2007).

The PCAOB was created in response to an ever-increasing number of accounting "restatements" (corrections of past financial statements) by public companies during the 1990s. The PCAOB is included in the Sarbanes-Oxley act Sec. 101, where the board's duties are stated. PCAOB's main duties are to provide and establish quality control and standards for auditing firms and to provide guidelines for auditing and SOX-compliance. Furthermore, they have the duty to conduct inspections of registered public accounting firms and disciplinary proceedings and impose appropriate sanctions where justified upon.

2.7 The COSO Framework for Internal Control

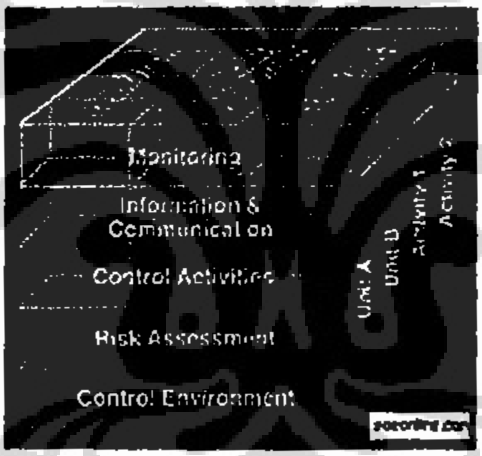
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a report on internal control in 1992. The report's objective was to:

- Establish a common definition which satisfies the needs of different stakeholders.
- Provide a standard that companies and other organizations - large or small, in public or private sectors, with or without profit objectives - can assess their control systems and decide how they can be improved.

Internal control is defined as a process, performed by the management and employees of an organization, designed to give reasonable assurance that the objectives are met in the following categories:

- Provide reasonable assurance of achieving corporate mission, objectives, goals and desired outcome,
- While adhering to laws and regulations
- Allow the company to accurately report successes and outcomes to the public and interested third parties.

The COSO framework consists of five interrelated components; Control environment, Risk Assessment, Control Activities, Information & Communication and Monitoring.



Figures 2.1: COSO Framework.
Source: SOX-Online, (2003-2006c)

The Control Environment: The control environment sets the tone in an organization and affects the control awareness in its employees. It is the foundation of all components in internal control. Factors within the environment are: Integrity, ethical values, competency of employees, management philosophy and style, how responsibility is shared within the organization and the attention and directives coming from the management.

Risk Assessment: The identification of relevant risks that might prevent the organization from achieving its goals.

Control Activities: The control activities are the guidelines and routines in the organization that contributes to secure that the management's directives are being carried out. They contribute to securing that necessary actions are being taken to prevent the risks that the organization will not complete its'goals.

Information & Communication: Is the right information in the right hands at the right time? Relevant information must be identified and supplied in such a form, and within such a timeframe, that the employees can fulfill their duties.

Monitoring: Management's follow-up of the internal controls functions.

2.8 Organization for SOX-Compliance

2.8.1 Implementation Guidance

The COSO-framework is a widely used tool for establishing internal control (Campbell et al, 2006). Furthermore, the COSO-framework is recommended by SEC as a suitable framework for achieving SOX-compliance (SEC, 2006). More importantly, it provides useful guidance on how to enhance internal control over financial reporting within organizations, especially considering the guidance concerning the essential components which need to be assessed in order to ensure internal control. The five internal control components within the framework should be regarded as comprising an integrated process, which indeed internal control is (COSO, 2006a). By using this guidance, management has the flexibility to choose controls that are suitable for achieving their particular entity objectives and also adjust and improve their internal control over time (Ibid). The COSO internal control process could be described as,

> *"management setting financial reporting objectives relevant to the company's particular business activities and circumstances. Once set, management identifies and assesses a variety of risks to those objectives, determines which risks could result in a material misstatement in financial reporting, and determines how the risks should be managed through a range of control activities. Management implements approaches to capture, process and communicate information needed for financial reporting and other components of the internal control system. All this is done in context of the company's control environment, which is shaped and refined as necessary to provide the appropriate tone at the top of the organization and related attributes. These components all are monitored to help ensure that controls continue to operate properly over time"*

The reason for the widespread use of the COSO-framework could be explained by the somewhat vague guidance in terms of minimal expectation in a number of key areas offered by the SEC (IMA, 2007) Furthermore, the auditors' task with regard to SOX section 404 is to determine whether management has conducted an adequate evaluation of the internal control over financial reporting, but the SEC's guidance does not provide any detailed instruction on how to approach its evaluation (Palmrose, 2007). However, and to some extent similar to the COSO-framework, the SEC's guidance allows management the flexibility to exercise judgment, which is not necessarily simple, that is appropriate to their company's individual circumstances in order to plan and evaluate their internal control over financial reporting. Furthermore, the intention with this guidance is to mitigate anxieties related to the fears of a costly and burdensome implementation of SOX procedures and so that also smaller, less complex companies easier can adjust their procedures to the framework (Ibid).

A simplified illustration of the SEC's guidance for compliance to the requirements of the SOX section 404, could be described as including three phases:

> *"Phase 1 involves identifying the financial reporting risks and then the controls that adequately address these risks.*
> *Phase 2 involves evaluating the operating effectiveness of the controls identified in phase 1, and determining the evidence needed to support the assessment, using evaluation procedures tailored to the risk assessment.*
> *Phase 3 involves reporting on the effectiveness of ICFR, including disclosing any material weaknesses identified during the evaluation process."*

2.8.2 PCAOB Guidance

Devonish-Mills (2007) says that initially the PCAOB guidance was designed for auditors to conduct the evaluation of compliance to SOX. However, because limited guidance has been issued specifically for management to assess the effectiveness over internal control over financial reporting, the costly and complex audit standard has become the standard for management as well (Ibid). The PCAOB standard is very granular, prescriptive and control focused making it very detailed and complex to utilize as guidance for SOX implementation (IMA, 2007). SEC (2006) points out that feedback has indicated that a number of implementation issues arose from an overly conservative application of the PCAOB auditing standard. According to Ernst&Young (2006), it is not sufficient with the PCAOB guidance in terms of practical - how to implement as guidance for management.

2.8.3 Project Management

One way of managing change is through projects (Turner, 1999). Turner defines a project as

> *—A project is an endeavor in which human, financial and material resources are organized in a novel way to undertake a unique scope of work, of given specification, within constraints of cost and time, so as to achieve beneficial change defined by quantitative and qualitative objectives.*

Due to that the implementation of SOX is a unique occurrence, a way to implement SOX is through a project. The approach taken by companies has been project-orientated (Beaumier and DeLoach, 2005). According to Surveys made by Ernst&Young (2004), various companies in the US appointed project leaders and established Project Management Offices (PMO) in order to ensure the implementation of SOX. Beaumier and DeLoach reinforce this statement and discusses lessons learned from year one. Furthermore, a PMO is required when implementing SOX successfully. A PMO is a solution of managing several projects at the same time through an organized and efficient way. The performance objective for the SOX implementation was time due to the time deadline companies had to meet (Beaumier and DeLoach, 2005). Through a PMO it is possible to utilize the best practices which have an impact on time, cost and quality of a project.

The lifecycle of a project have four different phases; conception, development, realization and termination (Lockyer and Gordon, 2005). The first phase conception can be described as where the vision and objectives are set. The second phase is development. In this phase the project objectives is set and the project is designed. The third phase, called realization is when the objectives are converted into tasks for teams and individuals to undertake and to realize. Phase four is termination, which include completion of the project and analysis to ensure that valuable information is documented. It has been difficult for companies to complete and terminate the SOX implementation project since - the rules of the game were not always clear and many companies were forced to modify their approaches as more information became available. (Beaumier and DeLoach, 2006, p. 27).

Furthermore, Ernst&Young's (2004) findings demonstrated that the PMO often reported to a 404 Steering Committee with the function of comprising different sections within the organization's SOX-processes.

2.9 Risk Assessment

2.9.1 Identify Risk

To reach a high level of internal control, the identification of risks is of high importance and risk assessment is included in COSO's five components on internal control (COSO, 2006b). The SOX act indicates that management should identify risks concerning occurrences that could bring a misstatement in the corporate disclosure. Thereafter, management should implement controls to prevent or identify errors or fraud that could result in a financial misstatement (SEC, 2002).

As part of the risk assessment process, management should determine and consider the implications of relevant risks that could hinder the achievement of the organization's objectives. Management must then provide a basis for managing the risks. An example provided is that management should assess how it considers the possibility of unrecorded transactions or identifies and analyses significant estimates recorded in the financial statements. The process of identifying and analyzing risks is an ongoing repeating process as risks may change as the environment or organization changes (PriceWaterhouseCoopers, 2004).

The sub-components for the risk assessment include:

- Business Risk Assessment
- Entity-wide objectives - Does the entity have approved entity-wide objectives that are aligned with the strategic plan?
- Activity-level objectives - Are activity-level objectives consistent with entity-wide objectives and are they relevant?

- Risk analysis - Are there mechanisms to identify risks and to prevent the entity from achieving its objectives from both internal and external sources? Is the process thorough and relevant?
- Mechanisms for change - Are there adequate mechanisms to identify change for routine events and for events that may have a pervasive impact on the entity?
- Inherent Risks
- Fraud Risks

Management may address risk in a combination of the following ways:

- Having the internal audit department perform annual risk assessments
- Having business units perform risk assessments in a self assessment format, which are then consolidated for review by a senior executive who is responsible for risk management or compliance with Section 404
- Making a senior executive responsible for performing independent risk assessments
- Creating a risk council that is charged with overseeing risk assessment
- Having the internal audit department lead the assessment of fraud risk
- Holding weekly/monthly meetings of executive management to discuss key business risks

2.9.2 Control Activities

Control activities are the policies and procedures that help to ensure that management's directives are implemented, thus, control activities are there to eliminate any risks that could bring a financial misstatement or fraud. Control activities occur throughout the organization, at all levels, and in all functions. The activities involve approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties (PriceWaterhouseCoopers, 2004).

COSO (2006b) discusses many different types of control activities, including preventive controls, detective controls, manual controls and computer controls. Control activities address specified information processing objectives, such as ensuring completeness and accuracy of data processing.

Preventive: Preventive controls are designed to avert problems rather than identify them. Some examples include the use of passwords to gain access to computer application systems, or required approval for all purchase orders over a certain dollar threshold.

Detective: Detective controls are meant to identify errors or irregularities after the fact. These may take the form of reviews, reconciliations, and analyses.

Manual: Manual controls are carried out by people, as opposed to automated controls that take place without direct human intervention. An employee manually reconciling a bank statement or a manager reviewing sales based on budgeted amounts are examples of manual controls.

Information Technology: Information technology (IT) controls are controls over computer processing of information, consisting of general controls (including controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance) and application controls (designed to ensure completeness, accuracy, authorization, and validity of data input and transaction processing).

Another control activity brought on to companies by SOX is Segregation of duties (SoD).

> *"Segregation of Duties means that duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For instance, responsibilities for authorizing transactions, recording transactions, and handling the related assets are divided. A manager authorizing credit sales would not be responsible for maintaining accounts receivable records or handling cash receipts (each of which is a basic business sub-process)."*

This means that a multi-skilled worker that could have been seen as an asset before, due to the fact that he could perform multiple or different duties, is now seen as a risk since he could defraud the firm. However, the Association for Financial Professionals (AFP, 2006) argues that the SoD will be too expensive for smaller and mid-sized companies since they do not have the resources to segregate duties to an extent that would be compatible with the SOX-requirements, only large firms will have the resources to implement SoD to a satisfying degree.

2.9.3 Documentation

Not only does SOX 404 require that the CEO and CFO attest accuracy of the data and confidence in accounting procedures and controls, but it is also essential with confidence in the IT system that house, move and transform data (SOX-online, 2003-2006a). Data has to move between different business groups and IT systems from the first transaction to the financial reports that have to be attested by the CEO and the CFO. According to Ernst&Young (2004), IT systems should be seen as an opportunity for companies in control monitoring. IT systems can be used to monitor SoD and application of manual controls to provide alerts when a control fails and direct to the person responsible. The IT Governance Institute and the Information Systems Audit and Control Association (ISACA) have published an open standard called COBIT (Control Objectives for information and related Technologies (SOXonline, 2003-2006b). This framework is partly built upon the COSO framework and was created to deal with IT issues. According to ISACA it is important for organizations to use information technology to drive their shareholders' value. COBIT aid companies in identifying the significant dependence of several business processes on IT, rising regulatory compliance that organizations need to comply with and benefits that come with managing risk successfully. This IT governance framework aids managers to overcome the gap between control requirements, technical issues and business risks. Additionally COBIT facilitates a clear policy development and good practice for IT control within the company.

2.10 Monitoring and Evaluation

2.10.1 Testing

To demonstrate whether an organization has an effective internal control over their financial reporting, there is a need to test the implemented control activities. SOX require managers to assess whether the implemented control activities are sufficient to achieve effective internal control over financial reporting, the only way to do this is by testing. The company must save evidence of this testing to support management's assessment of internal control over financial reporting (Deloitte, 2004).

The testing phase can be divided into four steps:

1. Identify the controls that are to be tested
2. Identify who will perform the testing
3. Develop and execute the test plans
4. Evaluate the test results

Any controls that fall under the following categories should be evaluated according to SEC regulation:

- Controls related to the initiation, recording, processing and reconciling of account balances, classes of transactions, disclosures, and related assertions included in the financial statements
- Controls related to the initiation and processing of non-routine and non-systematic transactions
- Controls related to the selection and application of accounting policies
- Controls related to the prevention, identification, and detection of fraud

In addition to the controls listed above, the PCAOB has identified, in its auditing standard No. 2, additional controls that are important.

- Controls, including information technology general controls, on which other controls are dependent.
- Controls over significant non-routine and non-systematic transactions, such as accounts involving judgments and estimates Company-level controls, including the control environment and controls over the period

end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, authorize, record and process journal entries in the general ledger and to record recurring and nonrecurring adjustments to the financial statements (such as, consolidating adjustments, report combinations, and reclassifications)

The PCAOB standard indicates that there are different approaches to testing and different people or departments may perform the testing and monitoring of controls. The corporate internal audit may perform the tests, the firm might use consultants to test or it can be done by self-assessment - the person that performs the control assesses the design and operating effectiveness of the control. In all cases, management must take responsibility for determining whether the personnel who perform the testing have the necessary competence and objectivity, and that the procedures provide evidence sufficient to support management's assessment (PCAOB, 2004b). Managers should recognize that by conducting testing by self-assessment the result will always lack objectivity to some extent. Therefore, independent verification may be required for management to obtain the necessary level of assurance from the self-assessment process. When management believes more objectivity is needed in testing, a quality assurance role may be introduced. The logical and typically most objective candidate for the quality assurance role is the internal audit department, which could both review the test plans and assess the test results (PriceWaterhouseCoopers, 2004).

There are different kinds of tests that can be conducted to assure the operating effectiveness of a control. They are classified into four categories: inquiry, observation, examination and re-performance. Combining two or more of these tests can provide greater assurance than using only one technique. The nature of the control also influences the nature of the tests of controls that should be performed (Ibid).

Inquiry of a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively. Observation of the control provides a higher degree of assurance and may be an acceptable technique for assessing automated controls. Examination of evidence often is used to determine whether manual controls (e.g., the follow-up of exception reports) are being performed. Re-performance of the specific application of the control provides the highest degree of assurance. (PriceWaterhouseCoopers, 2004).

2.10.2 Deficiencies

When testing the control activities implemented to reduce the risk of financial misstatements one might find that there are deficiencies; which can be explained as when a control might be inadequate or incomplete to fulfill its purpose.

PCAOB, (2004a) has identified three different categories of deficiencies when a control fails to meet the objective. Those are:

1. **A control deficiency** exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A deficiency in design exists when a control necessary to meet the control objective is missing or an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.
2. **A significant deficiency** is a control deficiency, or combination of control deficiencies, that seriously affects the company's ability to initiate, authorize, record, process, or report external financial data, hence when there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.
3. **A material weakness** is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

Deficiencies may be identified through many sources, the most common being either by the external auditors or by the firm during the follow-up tests to ensure the operational effectiveness of the controls (PWC, 2004). It is of high importance to identify which category a deficiency belongs to, since if a company's internal control contains one or more material weaknesses then the management is not allowed to certify that the company's internal control is effective (Deloitte, 2004)

When the classification of internal control deficiencies is complete, management should develop a remediation plan. If a material weakness or a significant deficiency exists there is a need for immediate actions and efforts that are initiated to ensure that the operating efficiency is restored in time for the internal control audit (Ibid).

Corrective actions may for instance be the redesign of controls or re-retraining of individuals that are performing the control.

2.11 Communication throughout the Organization

The widespread opinion is that when implementing SOX, communication is a crucial part. Of particular importance is an open flow of information which facilitates communication. All stakeholders affected in the SOX implementation process needs to be updated with the progress of the project to improve the smoothness of the implementation (Campbell et al., 2006).

According to Lawson and Price (2003) the way to a successful implementation is to manage change. The people in the organization have to change the way they work and this is only possible if people are persuaded to think differently about their jobs. There are three different levels of change:

> *"acting to achieve outcomes without changing the way people work (e.g., divesting non-core assets to focus on core business)*
> *requiring employees to adjust new practices or adopt new ones in line with existing mindsets in order to reach new targets (e.g., looking for new ways to reduce waste at an already lean company)*
> *changing the way people behave across the board, essentially by changing its culture fundamentally. Such a transformation entails changing the mindsets of hundreds or thousands of people to achieve a change in the collective culture of the organization. "*

Murray (2003) states that to achieve compliance with SOX the change level that is required is complexity level three. The organization must change the organization culture to become more focused on internal control of financial reporting (ICFR). This includes more than identifying, documenting, remediating and testing key controls. The employees have to be authorized and enabled to improve ICFR on an ongoing basis and therefore be aware of the importance of ICFR. Organizations that have underestimated the level of change have been faced with high costs and reluctance from staff when implementing SOX.

There are four conditions to changing mindsets according to Lawson and Price (2003). These are:

1. Employees must see the point of the change and agree with it. In other words, the purpose of the change must be adequately defined, communicated and reinforced to ensure that it is internalized. Employees need to find personal meaning in the change being proposed.
2. Surrounding structures such as setting targets, measuring performance and granting financial and non financial rewards must be in tune with the new behavior. New behaviors must be monitored and reinforced over time through different methods to ensure employees remain committed to them.
3. Employees must have the capability to do what is required, meaning it may be necessary to add staff with the requisite skills to the employee mix and provide education and training tailor made where required.
4. Role models at all levels of the organization and across all functional areas must walk the talk. This tie in with the first two conditions, in that employees need to see their role models, persons within the organization whom they look up to, are committed to the purpose of the initiative.

In 1995 the Canadian Institute of Chartered Accountants (CICA) published the Criteria of Control framework (COCO). This framework has similar components to Lawson and Price's conditions for changing mindsets, any organization of people, the essence of control is purpose, commitment, capability and monitoring and learning (Murray, 2006). The COCO model is based on the concept of repeatedly manner and a feedback loop. According to the model and the element of purpose and commitment, it is important to ensure that employees understand why the SOX project is carried out and that they are committed to the success of the project (Dittmar and Heffe, 2004). In an effective organization, guidelines about authority and responsibility are of great importance (Lock, 1998). The leader must communicate the organizational goals to the employees and how the unit or department can achieve them. A leadership culture like this aids the organization to stay focused on the organizational objectives and is one step towards successful change of the organization culture (Campbell et al., 2006). This requires communication from the management throughout the organization via information channels such as e-mail and an easily accessible intranet (Murray, 2006). The second element of the COCO model necessitate that employees are trained to be able to carry out new controls. The third and fourth element monitoring and learning, calls for that step are taken to ensure that the approach is altered over the life of the project as required and that sustainable compliance is achieved.

COCO and COSO aims to provide guidance on internal control. The difference between the models is that COSO see to what an internal framework is and COCO, on the other hand, provide guidance on how to implement an internal framework. The best approach for companies should be a combination of the two models to achieve SOX compliance (Murray, 2006). According to the COCO model it is important that executives and senior management in the SOX project realizes that the cultural change that is necessary requires significant resources. Furthermore, the project requires dedicated, constant and regular support. These aspects are the most overlooked but are crucial if the project implementation is to be successful. Therefore it is important that the organization realize the amount of effort that is needed to for key persons and senior management to stay dedicated.

2.12 Sustainable Compliance

After the actual implementation phase, Ernst&Young (2004) advocates that the PMO function, discussed in section 2.8.3, instead should become a process management function with the aim of maintaining SOX-compliance. Notwithstanding, striving towards process management within the organization should not disregard the valuable skills and knowledge from the project team. In other words, before ending the implementation, companies must ensure that the transition from project managers to future process managers takes place as smooth as possible.

Furthermore, in the article Sustaining SOX compliance (Beaumier and DeLoach, 2005) there is an example on how to achieve sustainable compliance to SOX after the end of year one and the implementation. It is suggested that companies should become more proactive than reactive in their work with SOX.

SOX Year One ⟶	**Beyond Year-One Goal**
ORGANIZATIONAL INFRASTURCTURE	
Project mentality	**Process mentality**
***Ad hoc* undefined process**	**Managed processes**
ACCOUNTABILITY AND RESPONSIBILITY	
Project team driven	**Process owner driven**
Reactto external auditor	**Managed audit relationship**
CHANGE RECOGNITION PROCESS	
Initial documentation	**Document management**
ADDITIONAL OPPORTUNITIES FOR IMPROVEMENT	
Manual controls	Automated controls
Detective controls	Preventive controls
Comprehensive testing	Targeted testing
Unpredictable costs	Managed costs
Reactive ⟶	**Proactive**

Figures 2.2: Achieve Sustainable Compliance.

Source: Beaumier and DeLoach (2005) p. 29

CHAPTER 3
ORGANIZATION OVERVIEW

3.1 Company A

Company A manufactures construction and mining equipment. Its product line includes hydraulic excavators, bulldozers, motor graders, off-highway dump trucks as well as frames and related components and steel cast products. Company ABC is the main shareholder of the company and it is listed in New York Stock Exchange, therefore Company ABC had requested Company A to apply Sarbanes Oxley Act ("SOX") Section 302 and 906 since 2006.

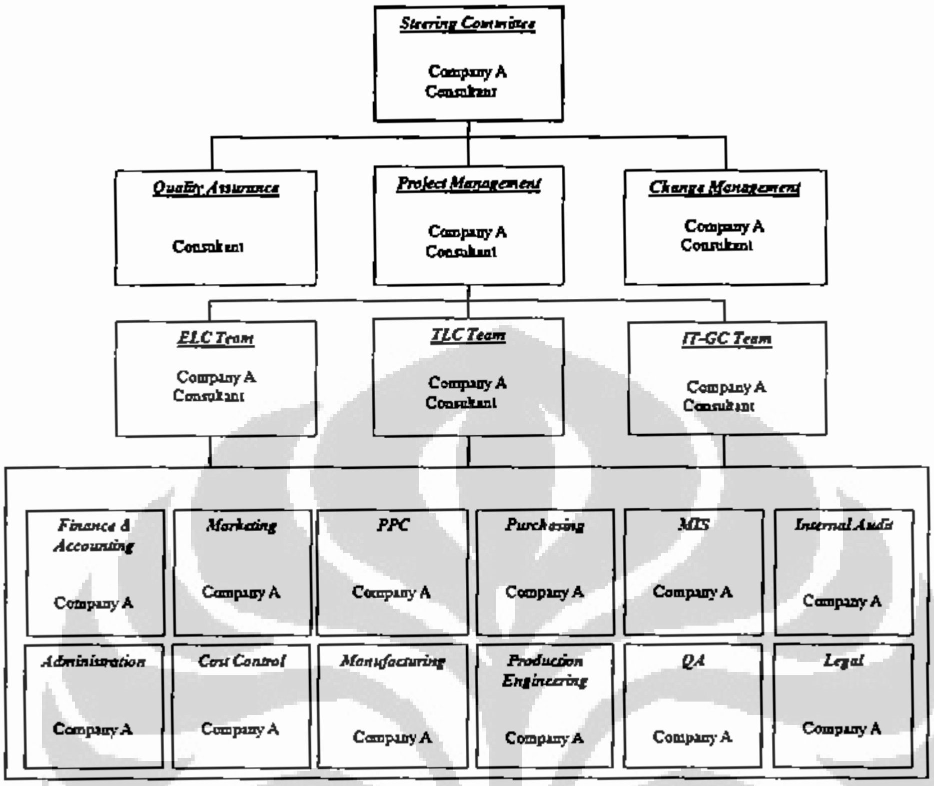
3.1.1 Organization for SOX-Compliance

Based on a letter from the Chief Financial Officer of Company ABC in 2006, Company A was instructed to be complied also with SOX Section 404 for the year ended on March 31, 2008.

Public Accounting Firm X has been requested to assist Company A in SOX Section 404 implementation program. As understand during TV conference meeting with Company ABC on September, 2006, for the purpose of audit in year ended on March 31, 2008, the scope of SOX Section 404 of Company A will be limited to Entity Level Controls. However, for internal purpose, the Company A decided to implement full scope of SOX Section 404 implementation, which also covers Transactional Level Controls and IT-General Controls.

Company A and Public Accounting Firm X then develop a Project Organization which defines the project participants and staffing requirements based on the project roles and responsibilities and the business requirements. It outlines the project structure including the project management and control structure, the Project Team organization, and the project support organization.

The following chart details the Project Organization for the project.



Project Organization Structure

Figure 3.1: Company A's central SOX organization.
Source: Project Charter Company A

The Steering Committee from Public Accounting Firm X will actively participate in monitoring the work progress and provide immediate and proper answers and comments to significant issues that are brought up to the Steering Committee or the Project Manager. Meanwhile Steering Committee from Company A will provide sufficient tone at the top to ensure that internal control culture is embraced by the Company's personnel.

Quality Assurance & Advisory team will conduct an independent and objective management review of the project to identify and manage risks to the project goals; Conduct documentation reviews at the end of each work activity of the project; and Resolves quality issues.

Public Accounting Firm X appoints a Project Manager (PM) who will plan, organize, and control the development as well as quality of project work products. PM will develop and track work plan task and activities; track and resolve project issues, escalating unresolved ones to the Steering Committee; contribute to the external and internal communications of the project; and contribute to the sharing of knowledge across project and to all team members. Meanwhile Project Manager from Company A will work closely with Project Manager from Public Accounting Firm X to ensure smooth and timely completion of the project.

Change Management team from Public Accounting Firm X will facilitate the identification of stakeholders whom will be impacted by the changes; Assist in conducting change readiness assessment and stakeholders analysis; Assist in conducting SOX 404 communication audit; and Assist in developing SOX 404 communication strategy. Meanwhile Change Management team from Company A will act as the counterpart to be fully dedicated during the project and collaborate together.

3.1.2 Risk Assessment

Public Accounting Firm X initiated Financial Reporting Risk Assessment by identifying inherent financial reporting risks and evaluating whether the control management has implemented adequately address those risks. This process provides the project team with a foundation for implementing top-down, risk management based approach for SOX Section 404 compliance purposes. The output of the Financial Reporting Risk Assessment is a Documented Risk Assessment Criteria Matrix that can provides information about the magnitude/impact, likelihood and control effectiveness criteria. In cooperation with Company A, Public Accounting Firm X is prioritizing list of significant inherent financial reporting risks into High, Moderate and Low level.

The Public Accounting Firm X is then responsible to perform a walkthrough within significant processes. Each significant process in the organization was investigated to have an understanding of the processing procedures; ensure the correctness of the information obtained about the relevant prevent and/or detect controls in the process; and ensure that these controls have, in fact, been placed in operation. The output of this process is walkthrough documentations, updated process maps, preliminary list of identified control weaknesses and other matters for improvement, and risk points and corresponding controls, including the consideration of segregation of duties. Then all outputs will be used to develop a Risk Control Matrices (RCM) for both Transaction Level Controls and IT-General Controls.

The company has 500 controls and is striving to that a majority of these should be automatic since this is better than manual controls due to that they are more reliable. However, sometimes it has not been possible to implement an automatic control to be compliant. The automatic controls are preferred due to that they are more cost effective, provide high-quality control and do not generate the same number of testing as manual controls. Several of the automatic controls are built in to SAP, a financial accounting system utilized within Company A.

As a result of SOX, user access to systems had to be cleaned up so that one person is not allowed to perform several steps in the financial flow. This is a basic step to good internal control, but was now more obvious due to SOX. Before SOX, the firm already had SoD, but according to SOX this now had to be written down and be more official.

3.1.3 Monitoring and Evaluation

Internal testing is conducted in same ways on the different departments. All departments have used Public Accounting Firm X to carry out the tests. Company A is striving for only using internal personnel when testing in the future.

Public Accounting Firm X develops a testing plan which considers the nature, extent, and timing of evaluating procedures. During an internal testing, tester from Public Accounting Firm X tests a sample of the controls that have been carried out. Based on the existing Risk Control Matrices (RCM), testers do a walkthrough to follow the flow and decide which control to test.

If a controls fails in the testing, a template will be filled in defining which unit, process group, process, control and which accounts that are involved. Tester from Public Accounting Firm X will also propose recommended for remediation plan and deliver report of testing result. The report consists of information why the controls fails, an action plan to correct it and a date when this is to be fulfilled.

Reasonable assurance is decided through discussions and argumentations between the tester from Public Accounting Firm X and staff from Company A. Reasonable assurance is used in the areas assessment, testing and efficiency evaluation. For example, if a control is carried out every day and there is one fail, then a new sample will be taken, is this one satisfactory, it is considered to reach reasonable assurance. However, if a quarterly control fails, the control will be considered to have failed.

3.1.4 Communication throughout the Organization

Information about the SOX project comes from the Change Management team and is spread through a SOX newspaper that everyone within the Company Group can read to. The newspaper contains information about SOX and presentations for 'champions' in selected department. Champions are employees from Company A that are selected by Project Management to be involved more closely and directly with the implementation process. Each significant department has its own champions and they have to socialize the knowledge they have to its subordinate or fellow employees.

Employees have the opportunity to give feedback through a mail box and conferences with 'champions' in selected department involved in the SOX implementation. Within this network, it is possible for the 'champions' to cooperate and discuss difficulties. Although it is useful with this cooperation, there is a problem since there are different requirements on the different units.

Although it has been hard work and much effort has been required, it is the opinion of the interviewees that the response to the SOX implementation has been positive throughout the organization. Additionally, they think that the company Group has been successful in implementing SOX. This is owing to strong focus from management and good support, the CFOs has been especially driving and the resources required have been allocated to the project.

3.1.5 Sustainable Compliance

In terms of good internal control within the firm, the difference between before and after the SOX implementation is that it is now measured and documented more thoroughly. In addition, the controls are followed up. This structure will be maintained in the future but there is still a question about the volume necessary and resources required.

SOX is meant to be adapted into the daily assignments and not something extra that has to be carried out. Currently, the most time consuming is the testing and is believed to require the most resources in the future as well. The documentation is already created therefore this will not demand much resources, unless the company acquires new organizations which will have to comply with SOX.

The work with SOX will in the future most likely be based on identifying risks and focusing on them. Those units that do not have to comply with SOX have a larger scope, including operational risks and these units will also benefit from SOX. As long as the SOX requirements does not change dramatically, the firm will continue evaluate and work with SOX the same way as now.

3.2 Company B

Company B is the leading operator of cellular telecommunications services in Indonesia by market share and revenue share. As a consolidated subsidiary of PT XYZ which is listed in the New York Stock Exchange, Company B is also required to comply with the Sarbanes Oxley Act (SOA) sect 404 and sect 302.

3.2.1 Organization for SOX-Compliance

The firm started to have their risks and control activities documented in 2003. The number of control activities in the Head Office and all regions is around 1,200 controls. The next major activities to be undertaken are assessment of the internal control system implementation, ongoing updates of the internal control matrices and proper communication and socialization of the internal control system to ensure effective implementation by all related personnel.

Public Accounting Firm Y has been requested to assist Company B with the assessment of the internal control implementation in certain areas, updates of the internal control matrices, improvement in selected entity level controls and development of internal control scorecard to monitor the effectiveness of the internal control system implementation. Public Accounting Firm Y is responsible for the quality of the work and deliverables produced by the project team.

Company B and Public Accounting Firm Y then develop a Project Organization which defines the project participants and staffing requirements based on the project roles and responsibilities and the business requirements. It outlines the project structure including the project management and control structure, the Project Team organization, and the project support organization.

The following chart details the Project Organization for the project.

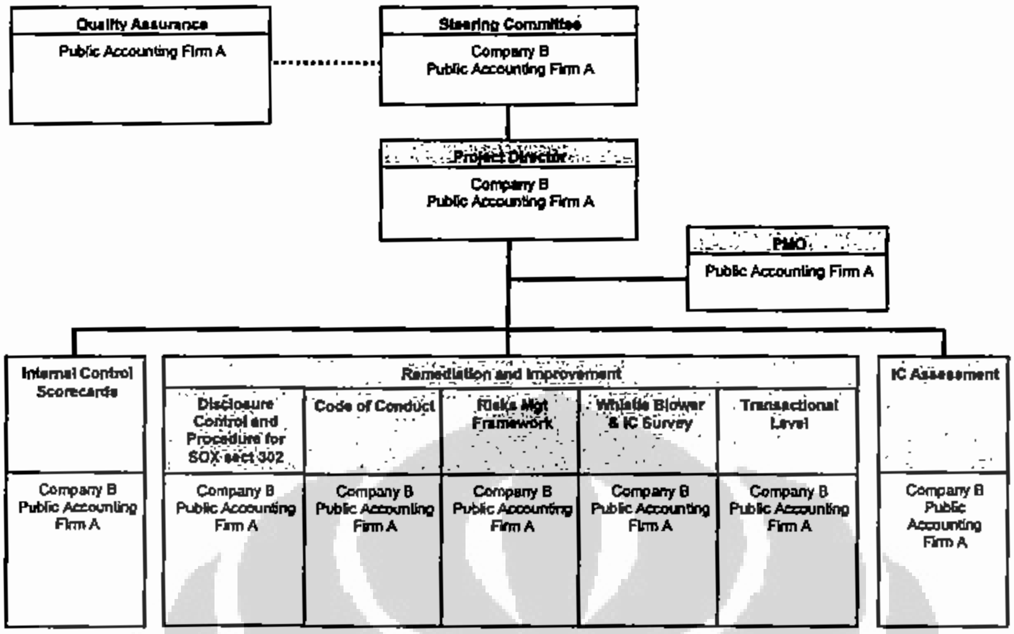


Figure 3.2: Company B's central SOX organization

Source: Project Charter Company B

The Steering Committee is the owner of the project and primarily responsible for setting priorities, approving scope, and settling enterprise-wide issues. It aids in promoting the section 404 projects throughout Company B and ensures that appropriate resources are available.

The Project Directors from Company B are from Finance Directorate and IA Sub Directorate. The project director from Finance Directorate is responsible for work stream related to Internal Control Scorecard, Code of Conduct, Risks Management Framework, Disclosure procedures and transactional level. While the project director from IA Sub Directorate is responsible for work stream Internal Control Assessment and Whistle Blower Program. The Project Directors have accountability for project results, deliverables and second level decision making for the entire project. The project director can resolve moderate levels of judgmental questions. The project director also resolves moderate levels of conflict with the project teams. The Project Director is responsible for escalating judgmental issues to the Steering Committee as necessary and reports on the project status to other executives and committees.

Quality Assurance and Advisor team will be responsible to perform quality assurance reviews of the documentation produced by the project team and also communicate findings to the steering committee. PMO team will be responsible to assist the Project Director to manage the overall project from the administration side.

3.2.2 Risk Assessment

The development of the risk management framework concerning risks and control activities has been done with great support from Public Accounting Firm A, which acted as internal auditors and advisors for Company B due to their professional experience in this area. The establishments of this framework will enable management to continuously identify, measure, manage and monitor key risks that occur from both external and internal sources. The output of this activity is Company B's Risk Management Framework, Enterprise-wide Risk maps, and risk-mitigation action plan.

In August 2003, the management of Company B has issued a Directors Decree about *Internal Control for Financial Reporting Improvement* which is to establish an effective internal control system and to comply with the SOA s.404 and s.302 requirements. The implementation of the Directors Decree ("KD") was developed in line with the COSO framework. Based on this KD, Company B has identified and documented all risks and control activities related to the internal control over financial reporting. The number of control activities in the Head Office and all regions is around 1,200 controls which need to be continuously monitored, validated and improved.

Based on Risk Management Framework, standardized process maps and activity descriptions, Public Accounting Firm Y has on a centralized basis identified risks in the processes and consequently developed key controls in terms of who, when and how to manage and mitigate these risks throughout the company group to reinforce the internal control environment within the company. Adherence to these control activities is mandatory to all entities within the group, and a deviation is considered as a control deficiency unless the entity can demonstrate that the deviation is justified in terms of not being able to execute the controls in line with the existing framework, yet still eliminating the risk.

The vast majority of the control activities are manual whereas automated controls constitute for 10 % of all control activities. However, the utilization of automated controls is intended to increase in the years to come. The responsibility for the control activities in terms of control execution lies with the entities. Thus, delegation of who to perform the controls is based on judgment, yet due to documentation of the different roles in the processes, the responsibility for the control activities becomes somewhat clear. Furthermore, to ensure the internal control over financial reporting, the concept of SoD is central within the company. Consequently, one person is not allowed to perform more than one thing in the same flow. However, the conflict of duties is being assessed by low, medium and high risks. In addition, the company has established a SoD checklist with all activities and how they are in conflict to achieve formalization for identifying if and when accesses are in conflict with the SOX work.

3.2.3 Monitoring and Evaluation

Public Accounting Firm Y develops Internal Control Scorecard that establishes linkages between internal control implementation and performance evaluation. The output of this activity is a Control Self Assessment (CSA) which is a tool for monitoring SOX compliance and contains the controls from the existing framework. The entities are supposed to report their performance and to quarterly sign off the key controls. The tool is used to secure the operating effectiveness of the controls and to monitor the execution of the controls.

Furthermore, each person that executes controls must report via the CSA documentation if they have performed the control according to the control descriptions, but also if the control was conducted with or without problems. If there has been a problem in the control execution, it is logged as an issue in the CSA documentation for monitoring SOX compliance with an appropriate action plan, which means that the SOA Division and Public Accounting Firm Y can perceive all issues throughout Company B's group and evaluate the significance of the logged issues in a SOX perspective.

Beside CSA that was performed by employee in each entity, formal audit testing is firstly conducted through the use of the corporate internal audit within the company in terms of management testing in order to secure and review the overall internal control environment within the company. Additionally, the external audits are performed by Public Accounting Firm C and conducted on various occasions over the year in order for the auditors to give a statement over the company's internal control environment. Although the scope of the testing in terms of units and processes is up to the external auditors to decide, the procedure involves testing of processes, done by so-called walkthroughs, or of key controls.

If the corporate internal audit detects internal control deficiencies, due to deviation from the predetermined control descriptions or flaws in the design of the control for instance, these deficiencies are reported to the FSO Division. The FSO Division is responsible for remediation if the deviation is due to an insufficient design. However, control executors could also be responsible for the remediation if a deficiency is detected, yet the formal approval that the deficiency has been solved does not lie with the same person responsible for the remediation but it is instead another person in the organization, often the Unit Lead or Head of Department. In addition, corporate internal audit demand that the name of the person responsible for remediation as well as the date for correction is evident, so that they can follow up on the remediation.

3.2.4 Communication throughout the Organization

Public Accounting Firm Y develops an effective communication strategy and plan during the implementation process. The objective is to address the communication aspect of the internal control and to positively influencing attitude and motivating people to take action towards improving the internal control system. And to increase the awareness level of all people involved on the importance of strong internal control system.

During the implementation, an intranet web page is used where all information about SOX was uploaded and weekly newsletters were e-mailed to employees. Furthermore, a helpdesk was established and people could e-mail questions about the implementation. Templates, information about directives and a list of approved deviations will be accessible. There were also local conferences and workshops. Each entity had one SOX champion that attended these workshops. In addition, this information will bring the opportunity to compare between the entities within the company.

Furthermore, during the project, department have had the opportunity to identify problems with controls and then make a proposal for changing the control. However, these proposals had to be approved by, first the Unit Lead or Head of Department, and then by the FSO Division.

3.2.5 Sustainable Compliance

Public Accounting Firm Y establish of proper internal control documentations and ensure the operational personnel responsible for performing the control activities aware and understand their roles and responsibilities in relation to internal controls. And it also transfers technical knowledge on the development and maintenance of internal control documentation to relevant Company's personnel. The objective is to ensure continuation of compliance and ongoing updates of the internal control documents.

Company B is striving towards that SOX will become a non issue and the vision is that it is going to be fully integrated with the normal financial reporting. People will be obliged to report in the CSA Documentation. This report are supposed to be integrated with people's daily assignments.

According to the interviewees, SOX is merely an extension of what they were doing before the implementation of SOX. The major difference is that now everything has to be documented and signed off in the CSA Documentation, hence more time consuming but high quality and enhanced internal control is achieved.

CHAPTER 4
ANALYSIS

The approach taken by companies towards SOX compliance has been project oriented. All organizations in this study established a project organization to achieve SOX compliance. However, there are variations in the different approaches in terms of that Company A delegated more responsibility to the entities level, whereas Company B centralized the responsibility to the project organization. Company A argued that large differences between the entities made it impossible to apply a centralized project organization, while the respondent at Company B would have preferred a centralized project organization and argued that this would have been less expensive.

To ensure that the decentralized project organization was adhered to, Company A appointed several support functions and roles since lack of strict obedience throughout the organization would diminish the usefulness of having a decentralized project organization. To some extent, these functions deviates Company A from Company B where the entities have more responsibility in the implementation of SOX.

The PCAOB and SEC proposed guidance are somewhat vague. However, due to limited implementation guidance from other institutions this points to that a majority of companies have utilized the guidance from SEC and PCAOB. In terms of guidance from SEC and PCAOB the respondents have had limited information from these institutions, hence the knowledge mainly derived from Public Accounting Firms. The Public Accounting Firms have aided all companies in this study in developing a framework and guidelines. The interviewees expressed the opinion that the guidance from SEC and PCAOB are somewhat insufficient. The empirical findings confirm that the COSO framework is a widespread tool for developing a framework for internal control.

Common for two companies is that time has been the most crucial objective in implementing SOX. As a respondent from Company A expressed - Time has been an important factor, money is always important but time was the most important factor. This demonstrates the importance of compliance on time.

4.1 Risk Assessment

Deloitte (2005) has declared that risk assessment is the first and a necessary step towards SOX compliance. The companies have not neglected this fact. Company A used top – down, risk management approach in developing its risk assessment which provides information about the magnitude/impact, likelihood and control effectiveness criteria. Company B developed a risk management framework concerning risks and control activities which enable management to continuously identify, measure, manage and monitor key risks that occur from both external and internal sources. In other words, despite different approaches, all respondents underscored that risk assessment is a central and significant part of the development of a SOX framework.

The respondent from Company B suggest that the initial scope of risk assessment was excessively extensive in terms of identifying risk and control objectives that had insignificant effect on the financial reporting since many of the risks was more of an operational nature.

Both companies stated that they are striving to have as many automated controls as possible, since it is more reliable and cost effective, than manual. In addition, both companies are working towards preventive controls rather than detective controls. However, it is sometimes impossible to implement automated controls on certain activities. Furthermore, the respondent from both Company argue that it is sometimes not possible to apply a preventive control, hence a detective control is their single option.

The critical issue of SoD has demanded much effort in terms of resources and time, mainly in identifying conflicts, within the researched organizations. The opinions about SoD vary between the companies, for example, Company B had not experienced much difficulty with the user access, although the documentation was time consuming. In comparison, Company A has experienced difficulties when implementing SoD, since they were also in the process of implementing SAP Application.

4.1.1 Top - Down Risk Management Approach

In a top down approach, Company A identifies the controls to test in a sequential manner, starting with company-level controls, then drilling down to significant accounts at the financial statement level and then to relevant individual controls at the process, transaction or application levels. This top down approach enables management of Company A to focus early in the process on matters that may have an effect on later decisions about scope and testing strategy, such as company-level controls.

The top down approach comprises the following sequence of actions:

- Company-level controls. Identify, understand and evaluate the design effectiveness of company-level controls.
- Accounts. Identify significant accounts, beginning at the financial statement or disclosure level. Identify the assertions relevant to each significant account.
- Processes. Identify significant processes and major classes of transactions that are related to these accounts and disclosures; link the accounts to the processes.
- Risks. Identify the points in each process at which errors or fraud could occur. This occurs during the identification of significant accounts, relevant assertions and related processes, and is confirmed by performing self-assessments.
- Controls. Identify controls that are designed to prevent or detect errors or fraud on a timely basis; clearly link individual controls with the significant accounts and assertions to which they relate.

The top down approach is both effective and efficient. The identification of significant accounts at the financial statement level is driving the process "down" to the individual controls level. In this manner, management of Company A is more likely to identify the controls to be tested that address relevant assertions for significant accounts. The process prevents an auditor or tester from spending unnecessary time and effort understanding a process or control that ultimately is not relevant to whether the financial statements could be materially misstated.

The top down risk-based approach allows management of Company A to reduce the scope of the internal control audit and the amount of testing being performed, thus improving the focus and efficiency of the audit and, over time, the amount of hours and cost associated with SOX compliance.

4.1.2 Risk Management Framework Approach

Company B implement Enterprise Risk Management Framework to manage overall corporate risk effectively. It is a fundamental business process that allows owners of assets to balance the operational and economic costs of protecting Company B assets. It also allows the balancing of the benefits derived from an informational asset, against the cost of protection of the confidentiality, integrity, and availability of the asset. The owners of assets must determine the security capabilities of that their systems must have, in order to meet business needs in the face of real world threats.

The process of risk management is not unique to the specific environment; it impacts the decision making process throughout Company B, mainly in Enterprises Risk Management (ERM) Sub Directorate. However, a well structured ERM process when implemented effectively can help management identify appropriate security controls, matching security capabilities to those assets which required most protection.

The following chart details the Risk Management Process of Company B.

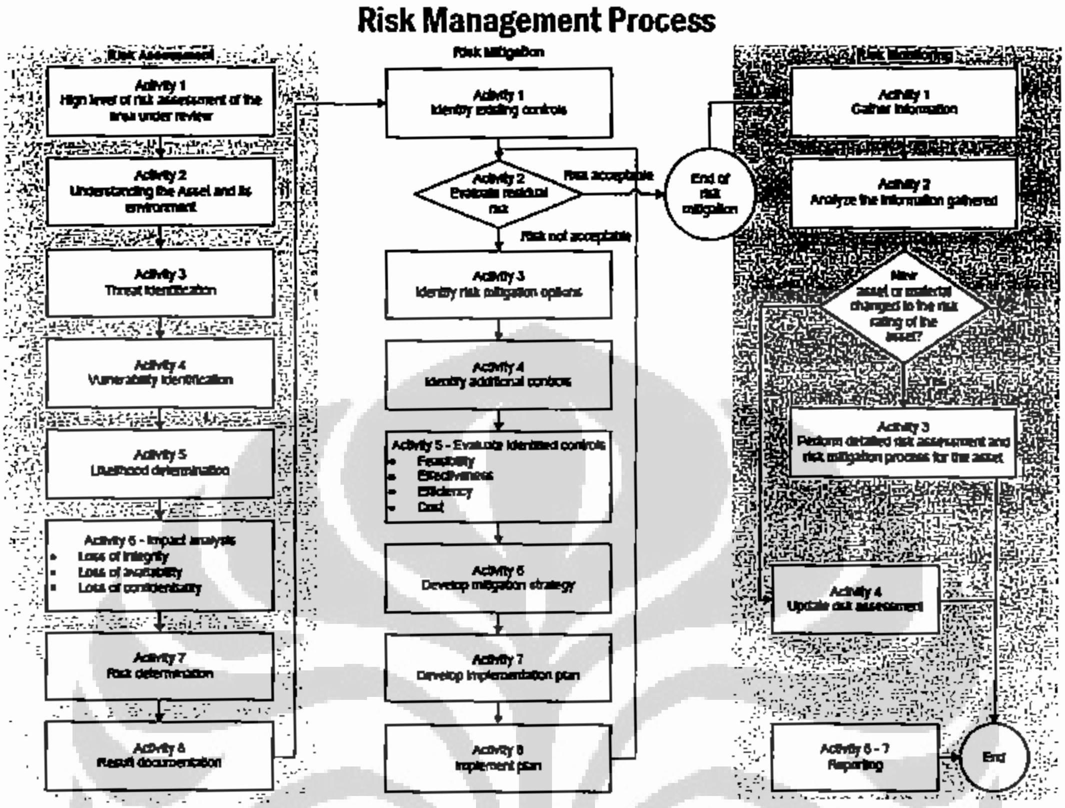


Figure 4.1: Company B's Risk Management Process
Source: Company B's ERM Framework Documentation

Company B divided its Risk Management Process into 3 cycles, they are:

1. Risk Assessment Cycle
2. Risk Mitigation Cycle
3. Risk Monitoring Cycle

Risk Assessment is the process of understanding the value to Company B of the asset being evaluated, identifying the threats and vulnerabilities that relate to the asset, evaluating the likelihood and impact of these threats and vulnerabilities, and based on the likelihood and impact of various threat / vulnerability combination identifying the overall level of risk which the asset has placed upon it.

Risk Mitigation is the process of identifying possible controls that would assist in reducing the overall risk faced by an asset by addressing threats / vulnerabilities identified during risk assessment. The controls identified are evaluated from a cost benefit, practicality and other criteria. Based on the evaluation of the controls, a suitable control is identified and the responsibility for its implementation agreed. In cases where the initially suggested control is not considered suitable, alternative control strategy may be developed or in some cases the risk may be transferred to third party if it could not be accepted by Company B.

Risk Monitoring is the process by which the risks faced by an asset are evaluated on a regular basis, to identify changes in the threat and vulnerability profile of the asset which may change the overall level of risk faced by the asset.

4.2 Monitoring and Evaluation

All companies have implemented systems for testing the internal control to assure the effectiveness of control activities. The approach among the participating organizations is that the internal testing has been conducted mainly by external resources. However, the extent to which external resources have been utilized differs among the participant companies. For example, Company A conducts their internal testing by only using external resources. The main reason was that they either have had a lack of internal resources to conduct the testing and or that they needed support from consultants in carrying certain testing. Hence, it reduces the level of subjectivity, since the utilization of external consultant increases the objectivity in the evaluation.

Company B's approach for internal testing is highly dependent on self-assessment, although the early stages of the SOX-project were characterized by highly comprehensive tests from the Corporate Audit function. For example, one interviewee from Company B stated that the initial tests from the Corporate Audit function were even more thorough than the testing performed by Public Accounting Firms. Subsequently, the personnel within Company B understood the significance of complying right form the start. The corporate audit's function is now monitor the results from the self- assessment testing process and in the same time conduct regular formal audit testing in order to secure and review the overall internal control environment within the company.

All companies in the study address the endeavor of reducing the involvement from Public Accounting Firms in the internal testing. They are striving towards merely using internal personnel within the group for carrying out future testing.

4.3 Communication throughout the Organization

For a smooth implementation of SOX into the organization an open flow of communication and updated information needs to be facilitated within the organization. The participating companies addressed several approaches for communicating information concerning SOX throughout their organizations. Company B utilized e-learning and communication through their intranet to spread information concerning SOX in the early stages of the project. And Company A was spreading information through a SOX newspaper. Consequently, general information about SOX was accessible to all parts of the organization that were affected by SOX.

The researchers' impression is that none of the participating companies have neglected the importance of communicating SOX throughout the organizations. However, Company B has taken one step further in terms of ensuring that employees have understood the implications of SOX through the use local conference and workshops. Templates, information about directives and a list of approved deviations can also be accessible via intranet.

All participating organizations have expressed the essential need of spreading information in order to facilitate a smooth implementation of SOX. One respondent from Company A stated that the communication within the SOX project have been more extensive than within previous projects. Additionally, he considered the communication within the SOX project to have been sufficient, mentioning the established Change Management team as an example. Whereas the use of a central helpdesk in Company B has been effective due to the fact that the local entities have similarity in processes and control activities.

Derived from SOX, the employees, to some extent, had to implement new routines and procedures to ensure compliance, states all respondents. Consequently, the implementation of SOX involved change. In order to change the mindsets within the organizations all participating organizations stressed the importance of management commitment at the local level, but also the tone at the top from the senior management. This is in line with the COSO model, which underscores the importance of dedicated and constant support from top management in order to spread and communicate the purpose of SOX throughout the organization.

4.4 Sustainable Compliance

Both companies to some extent have integrated the SOX work into the daily assignments, they emphasize that SOX should be fully integrated and not be considered as additional work. The respondents at the companies in this study reinforce this suggestion and states that they are working towards more effective and fewer controls. At Company B for instance, there are about 90% manual controls, but this number has decreased since the implementation of SOX, due to that controls that cover many risks have been identified, hence the controls are more cost effective. This respondent reasoned that although automated controls may be desirable, this is not always possible.

Furthermore, the approaches taken by the participating companies suggest that they are striving towards similar goals in terms of achieving sustainable compliance. Within Company B, the use of a self-assessment constitutes a central role in the future work with SOX which aids the endeavor of reducing the number of controls. Nevertheless, by only relying on the self-assessment approach for testing can be somewhat fragile, since there is a potential risk for subjectivity. Therefore both companies will still rely on internal testing through the use of the corporate audit function.

In common for the two organizations is that in the future the level of effort will most likely decrease in terms of documentation and remediation, whereas testing is likely to constitute a vast part of resources for SOX compliance.

4.5 How have two companies implemented the Sarbanes-Oxley Act of 2002 sec. 404?

In order to implement SOX, companies have established a project organization with the responsibility to ensure SOX compliance. Public Accounting Firms have been aiding companies in developing a framework for SOX. Together with Public Accounting Firms, companies have developed control matrices to identify risks and control activities that would eliminate these risks. Initially external resources were used to test the internal control due to lack of resources and knowledge in the subject area. However, companies are in general striving towards only using internal personnel for internal testing and some organizations have already achieved this.

It has been evident that good communication throughout the organization is crucial for a smooth implementation of SOX and the companies have not neglected this fact. The communication has been carried out by intranet, discussion groups and or work shops.

Implementation of SOX has to some extent been considered as a project within organizations. However, internal control should also be considered as a process which requires organizations to integrate SOX into the daily assignments of the employees. To achieve this, companies have utilized internal resources and external resources, and are aiming towards using internal resources to the highest degree possible to achieve sustainability. During the progress of SOX-implementation companies have gradually decreased the number of external resources.

It has been evident during this research that the theory considers only aspects which are important to consider when implementing SOX, not so much practical guidance on how to implement. The different approaches taken by companies towards SOX compliance may suggest that there is no implementation guide that is suitable for all companies in order to achieve compliance.

4.6 Have there been any significant similarities or differences between the organizations when implementing SOX sec. 404?

The implementation of SOX involves a high level of complexity in terms of that it is a novelty project. Therefore the companies have sought advice from Public Accounting Firms. This could explain why they have been so similar in their implementation of SOX, such as developing a SOX framework based on the COSO framework with aid from Public Accounting Firms. This could be due to the lack of implementation guidance.

Similarities could also be derived from an environmental point of view since the studied companies are located in Indonesia. The companies in the same country, in general have shared values and beliefs and the way of working correlates with each others. The fact that SOX originates from the US and in practice is directed towards larger American firms, in addition to the guidance received from American Public Accounting Firms, it might not have been the most suitable for companies in Indonesian environment. Hence, the companies have encountered resembling obstacles during the implementation. However, it has been shown that the approaches taken in addition to the difficulties experienced by Indonesian firms are rather similar to the approaches taken by American companies.

The significant differences in the approach taken to implement SOX between the companies in the study might be derived from how they are organized. SOX involves people at all levels in an organization, hence, if the organization is centralized or decentralized may affect how SOX has been implemented in the different firms. By utilizing a central function for implementing SOX, companies take a centralized approach to implementing SOX. However, by assigning the entities with more responsibility, a more decentralized approach is taken, thus, this is how companies differ in their progress towards SOX compliance. In addition, if the project was driven on a central or local level might also have affected the attitude towards SOX.

When implementing SOX it has shown that companies differ in their approach for testing and assuring the effectiveness of internal control. Companies have used a range of resources for monitoring and evaluation such as the Corporate Internal Audit, Public Accounting Firms or self-assessment. Public Accounting Firms would constitute for a more objective source for monitoring, however, utilizing internal resources might be more cost effective than Public Accounting Firms. The extents to which companies have used Public Accounting Firms and independent testing for assuring the effectiveness of internal control have differed. This might be due to that some entities lack resources to conduct testing independently.

CHAPTER 5
CONCLUSION AND RECOMMENDATION

5.1 Conclusion

It is somewhat difficult to assess whether or not an organization has been truly successful in their implementation. It has shown that it is difficult to identify an approach that is suitable for all companies when implementing SOX due to that all companies diverge from each other to some extent. However, it has been evident that some factors have shown to be of particular importance for a successful implementation. For example, a strong commitment from management at all levels within the organization, accompanied by effective communication channels has shown to be important factors for success. Furthermore, the organizations that successfully engaged employees to the project have been smoother in the implementation. In other words, not only is management commitment important, but also that they can communicate with their personnel so that they understand the implications of SOX in terms of whom, why and how the law is going to be enforced.

Another important factor for companies that are in the process of implementation is to have strong focus on relevant risks and control activities from the beginning, thus focusing on risks that actually have an effect on the internal control over financial reporting. As a result, the costs for the SOX implementation might be reduced and would also lower the level of effort associated with documentation for example. These resources could be allocated to other activities within the SOX process, such as improving testing procedures and training of personnel.

Time has also shown to be a crucial factor for a successful implementation. By thorough time management, companies can prepare themselves for SOX, which could result in a smoother implementation. Consequently, companies are then given the opportunity to improve over time to achieve compliance. However, since SOX was a law that had a strict deadline, it might have affected the smoothness of the implementation.

Another key factor to a successful implementation has shown to be to integrate the work with SOX in the employees' daily assignments, such as clearly defining roles and responsibilities. This is important since SOX will constitute a central role in how companies will ensure internal control over financial reporting in the future. Furthermore, incorporating SOX as early as possible would facilitate the understanding and work towards ensuring internal control.

5.2 Recommendation

5.2.1 Proposal for Companies

In the future, it might be possible for companies that have not yet implemented SOX to seek guidance from companies with experience from SOX. They would not have to go through the same process with trying to interpret the law and can subsequently avoid problems. In addition, Public Accounting Firms will most likely have more knowledge and experience within the subject area, and subsequently it is important that companies that are going to implement SOX do not neglect the importance of utilizing the professional expertise possessed by Public Accounting Firms.

5.2.2 Proposals for Further Research

As the implementation phase just recently was completed the researches could find out how companies are sustaining compliance in the future. Researchers could focus on sustainable compliance as compared to this study where sustainable compliance is merely limited to one section.

What would also be interesting to investigate is how SoD will affect companies in the future. It has been clear that new conflicts are still being identified and it would be interesting to research what future effects SoD will have on organizations, depending on how far organizations have to go to comply with the SoD in the future. Furthermore, it would be interesting to research how employees interpret and perceive SOX and how it changes over time.

Additionally, it would be interesting to carry out an in-depth study on one company to evaluate their implementation on a deeper level. This would give the researcher a deeper understanding which is more difficult to achieve when conducting a comparative study. Furthermore, a study of companies not included in this study could be of interest in order to be able to further identify differences and similarities, and subsequently success factors to a smooth SOX implementation. In addition, it would be interesting to find out if there are any similarities or differences between different geographically located companies.

REFERENCE

Literature

Brown, L., (1993), The New Shorter Oxford - English Dictionary, Oxford University Press Inc.

Lock, D (1998) Project Management 6th Ed. Gower Publishing Limited, Hampshire

Turner, R. (1999) The Handbook of project-based management 2nd Ed. Mc Graw Hill, London

Internet Sources

AFP, (2006), Comments on Concept Release Concerning Management"s Reports on Internal Control over Financial Reporting, [Online], Available from: http://www.sec.gov/comments/s7-11-06/s71106-61.pdf,

COSO, (2006a), Internal Control over Financial Reporting - Guidance For Smaller Public Companies, [Online], Available from: http://www.coso.org/Publications/SB_Executive_Summary.pdf,

COSO, (2006b), Internal Control - Integrated framework, Executive Summary, [Online], Available from: http://www.coso.org/publications/executive_summary_integrated_framework.htm,

Deloitte, (2004), Taking Control - A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002, [Online], Available from: http://www.iasplus.com/dttpubs/0408takingcontrol.pdf,

Deloitte, (2005), Under Control - Sustaining Compliance with Sarbanes-Oxley in Year Two and Beyond, [Online], Available From: http://www.iasplus.com/dttpubs/0503undercontrol.pdf,

Ernst&Young, (2006), Emerging Trends in Internal Control, [Online], Available from: http://www.ey.com/global/download.nsf/US/ETIC_10-May-06_Roundtable.pdf/$file/ETIC_10-May-06%20Roundtable.pdf,

Ernst&Young (2004) Section 404 post- implementation- What you should be thinking about now [online] available from: http://www.ey.com/global/download.nsf/International/S404_PostImp.pdf/$file/S404_Post-Imp.pdf

IMA, (2007), IMA files letter to SEC/PCAOB on Sarbanes-Oxley guidance, [Online], Institute of Management Accountants, Available from: http://www.imanet.org/pdf/SOX%20FCL.pdf,

PCAOB, (2004a), PCAOB Release 2004-001,[Online], Available from: http://www.pcaobus.org/Rules/Docket_008/2004-03-09_Release_2004-001_Appendix_D.pdf,

PCAOB, (2004b), Auditing Standard No. 2 - An Audit of Internal Control over

Financial Reporting Performed in Conjunction with an Audit of financial Statements, [Online], Available from: http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf,

PCAOB, (2007), Our Mission, [Online], Available from: http://www.pcaob.org/,

PriceWaterhouseCoopers, (2004), Sarbanes-Oxley Act: Section 404 - Practical Guidance for Management, [Online], Available from: http://www.pwc.com/images/gx/eng/fs/1004soa.pdf,

SEC, (2002), PUBLIC LAW 107-204, [Online], Available from: http://www.sec.gov/about/laws/soa2002.pdf,

SEC, (2006), Proposed Rule, [Online], Available from: http://www.sec.gov/rules/proposed/2006/33-8762.pdf,

SEC, (2007), The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation, [Online], Available from: http://www.sec.gov/about/whatwedo.shtml,

SOX-Online, (2006), Sarbanes-Oxley Act Basics, [Online], Available from: http://www.sox-online.com/basics.html,

SOX-online (2003-2006a) Accounting and IT Control Frameworks [online] available from: http://www.sox-online.com/coso_cobit_2frameworks.html

SOX-Online (2003-2006b) COSO and COBIT center [online] available from: http://www.sox-online.com/coso_cobit.html

SOX-Online, (2003-2006c), COSO Financial Controls Frameworks, [Online], Available from: http://www.sox-online.com/coso_cobit_coso_framework.html,

Journals

Beaumier C. and DeLoach, J. (2005) Sustaining SOX compliance, Bank Accounting & Finance, Apr/May 2005, Vol. 18 Issue 3, p27-51, 5p

Campbell, D., Campbell, M., and Adams, G. (2006) Adding Significant Value with Internal Controls The CPA Journal, Vol. 76, Iss. 6

Devonish-Mills, L., (2007), Updates on XBRL and SOX, Strategic Finance, Feb., Vol 88, Iss. 8, p. 14

Dittmar, L. and Heffes, E.M. (2004) What will you do in Sarbanes-Oxley"s Second year? Financial Executive, Vol 20, Iss. 8 Nov 2004 p. 17-18

Lawson, E. and Price, C. (2003) The psychology of change management McKinsey Quarterly, 2003 Special Edition, Issue 4, p30-41, 12p

Murray, W (2006) Change of Mindset CA Magazine, Volume 139, Issue 9

Palmrose, Z-V. (2007), MANAGEMENT REPORTING ON INTERNAL CONTROL OVER FINANCIAL REPORTING, States News Service