CHAPTER II. COMPLIANCE REVIEW

2.1. Compliance Definition

From the Merriam Webster Dictionary, the word “Compliance” means :

1. the act or process of complying to a desire, demand, proposal or regimen or to coercion
2. conformity in fulfilling official requirements
3. a disposition to yield to others
4. the ability of an object to yield elastically when force is applied.[4]

From Wikipedia, the Compliance (regulation) is defined as the act of adhering to, and demonstrating adherence to, a standard or regulation. In this thesis, the word “compliance” is associated with regulation or standard.

In summary, compliance can be defined as the act of adhering to and demonstrating adherence to a standard or regulation. In IS or IT, compliance can be defined as the act of adhering to and demonstrating adherence to industry standard or external regulation, frameworks, and internal corporate policies in all IT activities. And IT compliance can be defined as IT internal control function to the company’s management around creation, retention, disclosure, protection and integrity of information in the company that is related to financial activities.

[4] http://www.merriam-webster.com/dictionary/compliance

2.2. IT Compliance category

According to Financial Insights (an International Data Company specializing in the Financial Services sector), IT compliance can generally be categorized into the following three distinct areas (as described in Figure 2.1) :

1. Information Security
2. Content Management
3. Policies and Procedures

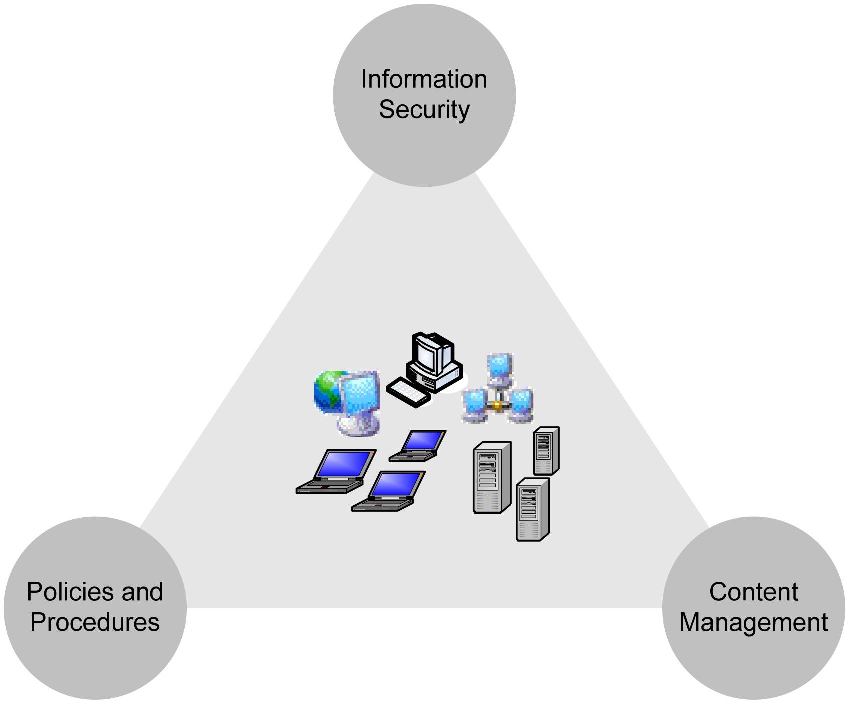

Figure 2.1. Key Components of IT Compliance

2.2.1. Information Security

Information security is the backbone of any compliance infrastructure. Without an effective security controls, financial institution risk exposing proprietary information and personal customer information to theft or unauthorized access. Theft on customer information can lead to fraud, money laundering, or even financing of illicit activities.

Achieving a secure IS environment is a dynamic and continuous process. The company must continually assess the possible Security risk and continually improve the security controls to manage the security risk.

2.2.2. Content Management

Content Management is about managing the company's data or information. A good content management should make: the data to be available every time it is needed, the data can be easily retrieved, the data can be accessed only by the authorized person.

A good content management should cover 3 things[5] :

1. Availability: Will the information systems on which the business is heavily dependent be available for the business at all times when required? Are the systems well protected against all types of losses and disasters?
2. Confidentiality: Will the information in the systems be disclosed only to those who have a need to see and use it and not to anyone else?

[5] http://www.isaca.org/Template.cfm?Section=IT_Audit_Basics&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11223

3. Integrity: Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?

Bad content management can lead data/information leakage in the company. That may lead also to fraud, money laundering, even financing of illicit activities.

To achieve a good content management, the company must identify all the data information in the company. Then, company should have a control for each data or information. This will reduce the risk of leakage data or information.

2.2.3. Policies and Procedures

All processes and activities have to have a standard procedure or in a company level, a policy. This is very important in order to achieve a compliant environment. Policies and procedures should be created by the related person. Input and endorsement are critical to achieve a compliant procedures and policies that best suit the organization.

The organizations must properly train and inform their employees of any policies changed. Participation across organization is also important and should include IT organizations, legal departments and business stakeholders.

2.3. The IT Compliance challenges

A research sponsored by the Security Compliance council (www.securitycompliance.com) indicates that the key challenges that organizations face in meeting the requirements for IT Compliance are, as follow :

- Growing complexity of managing compliance with multiple regulations
- Increasing costs of compliance
- Risks posed by noncompliance

2.3.1. Growing complexity of managing compliance with multiple regulations

From the survey of 400 respondents represented enterprise-level companies across a wide range of industries. More than half of them were from companies with 10,000 or more employees. About half held IT management or executive positions. The remainder included consultants/systems integrators or held other IT titles.

Ranking of IT objectives in terms of the most critical priority [6]

1. Reducing IT costs
2. Regulatory compliance
3. Improving availability and performance of business services
4. Incident and problem management
5. Change management
6. Virtualization

[6] http://www.ebizq.net/topics/business_service_management/features/12276.html?page=2

7. Capacity planning
8. IT budgeting and chargeback
9. Data center consolidation
10. IT risk management
11. Improving internal user satisfaction
12. Service desk consolidation
13. IT-enabled process improvement (ITIL, COBIT, ISO/IEC 20000, etc.)
14. Asset and vendor management
15. Cloud computing (may also be part of a virtualization initiative)

It is completely obvious that IT compliance is holding a significant rank of IT objectives (2 out of 15). And according to Ernst & Young, the most pressing challenges that companies face today:[7]

- Internal control,
- Corporate governance,
- Risk management, and
- Regulatory compliance

With so many organizations struggling to run IT compliance by meeting the internal and external auditors, hat must satisfy multiple regulatory mandates. On average more than one third (34 percent) of IT resources are being spent to meet multiple regulatory demands, according to research sponsored by the Security Compliance council.

[7] https://eyo-iis-pd.ey.com/drivinggrowth/unprotected/downloads/Risk_Post_IPO.pdf Ernst & Young, The Essential Guide to: Risk Post – IPO, 2006

The analyst firm AMR research for example, estimates that compliance spending will exceed $80 billion over the next five years and $15.5 billion this year. For 2005, AMR research says companies spent $5.8 billion on meeting the SOX requirements alone.[8]

2.3.2. Increasing Cost of Compliance

Compliance is an issue with which all financial institutions must grapple. According to financial insights, US Financial institutions (including banks, capital market firms and insurance companies) spent almost $3.7 billion on compliance solutions in 2005. This figure is expected to grow at a five-percent compounded annual rate through 2010.[9]

There are several factors that contribute to the increasing costs of compliance in term of IT budget and resources. Manual and ad hoc processes in IT compliance process creating labor-intensive activities that are expensive, error-prone and not easily repeatable.

Beside, inconsistent process among business units and geographies also create more time used to prepare an audit, more time spend by external auditors to evaluate control environment. Longer audit is mean higher audit fees. Inconsistent process also may create duplication or redundant work, which requires multiple efforts to test, measure and report on the same IT control.

[8] Copyright Association of Records Managers and Administrators Jan/Feb 2006, Provided by ProQuest Information and Learning Company. All rights Reserved.
http://findarticles.com/p/articles/mi_qa3937/is_200601/ai_n17188931/

[9] http://eval.symantec.com/mktginfo/enterprise/yellowbooks/it_compliance_03_2006.en-us.pdf

2.4. Sarbanes-Oxley

Sarbanes-Oxley is the most common standard used in Compliance. The rule was started on 2002. Enron, Arthur Andersen, WorldCom, Tyco, Adelphia. These companies have become household names mostly because of their past display of corporate greed, fraud and accounting improprieties. The offenses of these few organizations are not representative of the majority of more than 15,000 public companies in the United States, yet the results of their abuses are far reaching. Thus, on July 30th, the U.S. Congress declared the Sarbanes-Oxley Act of 2002. [10]

Sarbanes-Oxley is named after two person, Senator Paul Sarbanes (D-Md) and Congressman Michael Oxley (R-Oh). Sarbanes-Oxley Act is also known by several names, including :

- Public Company Accounting Reform and Investor Protection act of 2002
- SOA
- SOX
- SarbOx.[11]

The act was signed into law to improve the accuracy and transparency of financial reports and corporate disclosures, as well to reinforce the importance of corporate ethical standards. As a result, the SEC (Securities and Exchange Commission) issued rules outlining the provisions of the Act. In addition, the NYSE (New York Stock Exchange), Amex (American Stock Exchange) and the Nasdaq

[10] Marchetti, Anne M, 2005, Beyond Sarbanes-Oxley compliance : effective enterprise risk management, John Wiley & Sons, Inc

[11] Anand, Sanjay, 2007, Essentials of sarbanes-oxley, John Wiley & Sons, Inc

Stock Market, have all significantly modified the standards for listing stocks on their exchanges. [12]

SOA is the most significant legislation impacting the accounting profession. It addresses a wide range of matters range relevant to publicly held issuers and their auditors, including the auditor oversight and independence, corporate responsibility for financial reports, and enhanced financial disclosures. SOA is composed 11 titles :

I. Public Company Accounting Oversight Board

II. Auditor Independence

III. Corporate Responsibility

IV. Enhanced Financial Disclosures

V. Analyst Conflicts of Interest

VI. Commission Resources and Authority

VII. Studies and Reports

VIII. Corporate and Criminal Fraud Accountability

IX. White Collar Crime Penalty Enhancement

X. Corporate Tax Return

XI. Corporate Fraud and Accountability

[12] Solomon, Jill, 2007, Corporate governance and accountability, 2nd Edition, Wiley.

SOA is designed to reassure shareholders that their investments are being protected from scandal and deception. Thus SOA was written in the spirit of three key principles (figure 2.2) : integrity, accuracy and accountability.

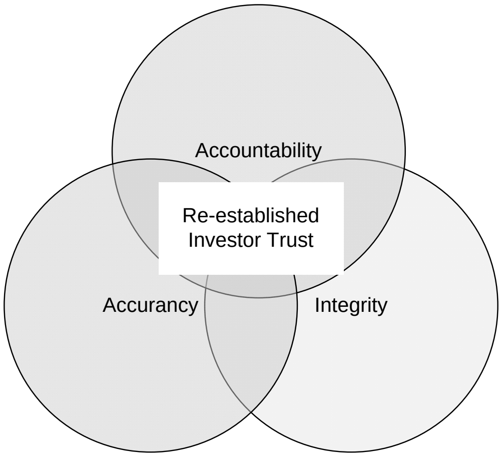

Figure 2.2. SOA Key Principles

These three principles are the main points that should have to be fulfilled in implementing SOA compliance in a company.

The most important section from SOX to Financial services company is the SOX 302, SOX 906 and SOX 404. SOX 302 stated about the Corporate Responsibility for Financial Report, "The CEO and CFO of each issuer shall prepare a statement to accompany the audit report to certify the 'appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respects, the operations and financial condition of the issuer.' A violation of this section must be knowing and intentional to give rise to liability".

SOX 906 also stated about Corporate responsibility for financial reports and also mention that the white collar that commit crime will get the penalty.

SOX 404 is specifically stated about the Management Assessment of Internal control. The internal control stated here is the internal control that have influenced to the company's annual financial report (stated in SOX 302 and SOX 906).

2.4.1. Sarbanes-Oxley – Section 404 Overview

SOA Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports. The sections of title IV are:

Section 401.	Disclosures in periodic reports
Section 402.	Enhanced conflict of interest provisions
Section 403.	Disclosures of transactions involving management and principal stockholders
Section 404.	Management assessment of internal control
Section 405.	Exemption
Section 406.	Code of Ethics for senior financial officers
Section 407.	Disclosure of audit committee financial expert
Section 408.	Enhanced review of periodic disclosures by issuers
Section 409.	Real time issuer disclosures

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.[13]

(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 engagement.

Section 404 requires the Management to have an assessment of internal control, main concern is to the financial reform. It also requires that all annual financial reports include an Internal Control report to certify and explain those efforts

[13] http://news.findlaw.com/hdocs/docs/ gwbush/sarbanesoxley072302.pdf

that have been made to ensure the integrity and accuracy of the financial information. This rule (b) is purposely mention that a Compliance section is needed as the key of internal control. It also can be concluded the same for IT Compliance in IT systems.

Section 404 doesn’t directly relate to IT Compliance implementation in the company explicitly. But by having an independent IT compliance section and implement IT compliance in the IT Systems, management can sure that the internal control on financial transaction done by IT systems is in place.

2.5. SOX 404 Internal Control Framework

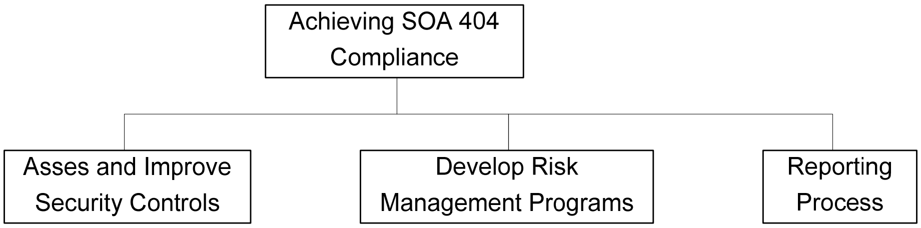
Achieving SOA 404 Compliance
Asses and Improve Security Controls
Develop Risk Management Programs
Reporting Process

Figure 2.3. Processes to Achieve SOA Compliance

Companies generally implement SOA compliance by adopting the internal control framework (figure 2.3). The process are included :[14]

- Assessment and improvement of internal controls
- Development of risk management programs
- Reporting processes

[14] Anand, Sanjay, Essentials of Sarbanes-Oxley, John Wiley & Sons, Inc, 2007

2.5.1. Assessment and Improvement of Internal Controls

To implement SOX 404 compliance, first the IT compliance has to do self assessment. To do the assessment, IT Compliance has to define the internal control areas for the assessment.

In assessing the company's internal control, usually COSO's (Committee of Sponsoring Organizations of the Treadway Commission) framework is used. for financial and IS auditing. COSO's framework (figure 2.4) consists of[15] :

1. Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
2. Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
3. Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

[15] http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

4. Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
5. Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
6. Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
8. Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

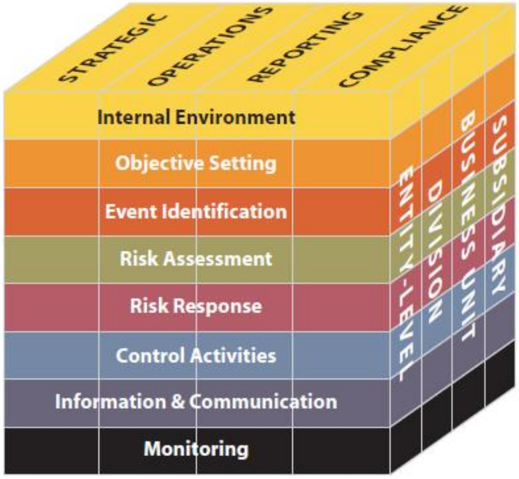

Figure 2.4. COSO Framework 2004

The major elements / internal control area of IS audit can be broadly classified as[16] :

1. In Physical and environmental review - This includes physical security, power supply, air conditioning, humidity control and other environmental factors.
2. System administration review - This includes security review of the operating systems, database management systems, all system administration procedures and compliance.
3. Application software review - The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed.
4. Network security review - Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.
5. Business continuity review - This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.

[16] Sayana,S. Anantha, CISA,CIA, "IT Audit Basics", Information Systems Control Journal, Vol.1, 2002. http://www.isaca.org/Template.cfm?Section=IT_Audit_Basics&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11223

6. Data integrity review - The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software (e.g., computer assisted audit techniques).

2.5.2. Development of risk management programs

After the assessment of internal control in IT systems, IT compliance will have to define risks that may be occurs if the internal control not on place.

The risks if internal control is not on place :[17]

1. Loss of Integrity.

   System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

   Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

2. Loss of Availability.

[17] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30. Risk Management Guide for Information Technology Systems

If a mission-critical IT system is unavailable to its end users, the organization’s mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users’ performance of their functions in supporting the organization’s mission.

3. Loss of Confidentiality.

   System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

After IT risks are defined, IT compliance will treat the risk in order to improve performance or based on the management’s will. Risk treatments are categorized as below[18] :

1. Avoidance – company exit the activities due to the risk. E.g. exiting a product line, declining expansion, or selling a division.
2. Reduction – company try to reduce the frequency and or severity at business activity and decision making.

[18] https://eyo-iis-pd.ey.com/drivinggrowth/unprotected/downloads/Risk_Post_IPO.pdf Ernst & Young, The Essential Guide to: Risk Post – IPO, 2006

3. Sharing – company try to reduce the frequency and or severity by transferring or sharing some or all risk. The common techniques are by buying insurance, hedging the transactions, or outsource the activity.
4. Acceptance – No action regarding the frequency and severity of inherent risk.

2.5.3. Reporting processes

After treating Risk, IT compliance has to create reports of the compliance process. This reporting process is also include collecting all of the reports and evidences on IT operations that are being controlled. These reports will be used for report to the company management. This report makes the management know the condition of its IT internal control and can make better decision to direct the company in the future. The report will also be as a fulfillment of SOS section 404.