CEOs Survival: SOX Strategies Over the Long Term

Parviz Partow-Navid, California State University, Los Angeles, USA; E-mail: ppartow@calstatela.edu
Brad Cikra, California State University, Los Angeles, USA; E-mail: bcikra@nexgate.net

INTRODUCTION

The Sarbanes Oxley (SOX) Act has renewed business attention to details and financial reporting. Its intent is information protection and securing information, not just from outside intruders but also from hackers informing traders prior to public announcements. Securing all information within a company is an improbable task, although many steps are specified and suggested in the Act itself and supporting committees (Coe, 2005). Ways of benefiting from the SOX Act exist. Build a better company with a controlled environment (Deloitte, 2004).

Strategic goals and guidelines are described in this paper to assist the CEO in benefiting from the SOX Act. Although this paper is broad based, it is neither a comprehensive nor exhaustive coverage of the compliance issues of the Act. The Act is open ended with Section 404. Each company has areas of uniqueness that open new avenues of compliance interpretation. Embracing the Act completely is like sailing the great oceans. In this paper remedies for the CEO are offered to sail this ocean.

INTENDED AUDIENCE AND SCOPE

The audience for the SOX Act is public companies. Companies that are private are not affected by the SOX Act, which excludes many small companies. The scope of the Act is to make certain that the company's financial health is clearly reported for fair-trading of company stocks. Scope of the Act embraces security of information, which can have both legal and SEC violation implications. Non-profit corporations and other non-profit organizations are also free from compliance; however much pressure is put on these companies and organizations to be compliant to receive both private and federal funds.

AFFECTS CEO AND BOARD OF DIRECTORS

The Board of Directors is now in charge of overseeing the internal audit of the company. The CEO who wants to make good on his corporate promises is no longer the reporting officer for the internal audit. It now is the board of directors' responsibility to the stockholders to audit the company internally. The SOX Act ensures independent auditing by forbidding any officer or employee of a public accounting firm from being on a board of directors for which an external audit is performed. The board of directors cannot hold interest in a public accounting firm, that is utilized in auditing the corporation or company where the board member sits.

AUDIT COMMITTEE

The nature of the SOX Act is so expansive it requires an audit committee to manage. The internal audit committee works with the external-auditing firms and any outsourced internal auditing teams and reports directly to the board of directors. This committee is also an audited issue. It must be in place and operational with agenda and people (Deloitte, 2004). The large volume of issues within the SOX Act requires the audit committee to manage and protect the company from compliance failure.

CONTROLS FOR AUDITING PROCEDURES

The important concern is to have all the security requirements of rotation and cross interest checked and to have methods and procedures in place. A security check on entrance to the building and security auditing of all audit participants is a must. Checklists are available for spreadsheets to track and document procedures involved with spurious business activities such as waste control and unused asset removal (Burnett & Friedman, 2005). Five steps in preparing environmental cost estimates (ECE) are according to Berlin and Goldstein as follows (Berlin & Goldstein, 2005):

1. Evaluate any existing ECE, including any notes, reports, or correspondence.
2. Gather data regarding environmental status.
3. Develop/update ECE.
4. Assess the ECE relative to materiality.
5. Provide assessment to CFO/auditors.

Seven common risks that are difficult to account and measure with environmental issues according to Berlin and Goldstein are as follows (Berlin & Goldstein, 2005):

1. New management's lack of knowledge
2. Liabilities hidden in multiple accounts
3. Partial estimates that incorrectly appear immaterial
4. Increasing state enforcement
5. Masking liabilities with minimally effective treatment systems
6. Changing ownership to hide the cleanup problem

USE OR ABUSE THE AUDITOR? PERFECTING THE COMPANY AS A CORPORATE GOAL

The auditor has a job to perform and that job appears negative. Nothing is going to alter this relationship between auditor and company person, more than the SOX Act (Millman, 2005). "Perfecting the company" as a corporate goal is paramount in making the audit process a positive contribution. Protection for whistleblowers was implanted in SOX Act to protect the very nature of auditing, revealing something amiss. Lawyers are also to report to the board when presenting evidence of material violation. They are also protected from losing employment similar to the whistleblowers (Noorishad, 2005).

BUILD AN ETHICS PROGRAM AS CORPORATE GOAL

The SOX Act probes into whether the senior executives, the CEO and CFO, have a code of ethics (Green, 2004). Section 406 requires posting in the financial reports a disclosure of the company's code of ethics (Anand & Sarbanes Oxley Group, 2004). After ethics, behavioral boundaries can be developed and documented within the company (Green, 2004).

POLICIES FOR LEGAL PROTECTION AS PART AND PARCEL TO ETHICS PROGRAM

An appropriate response in legal terms is necessary for the protection of the CEO when a material violation occurs (Noorishad, 2005). It is clear, that preventive actions are appropriate remedial measures. To protect the company in court it is paramount to pile high a set of policy and procedures for ways and means of behavior. A procedure and policy needs to include education, training and policy signature attachment for the employee, who involves assessing material value that effects the financial statement. If the employee is non-compliant, the court will find the company less liable than if no such policy and procedure documented with policy signature, education and training attachments were in place.

AFFECTS MANAGEMENT

In Section 404 of the SOX Act, management must document all policy and procedures for any activities business or related that effect the bottom-line of the financials. This includes any risks or waste removal costing. Vacations that are not taken and airline miles not ticketed create openings for hidden costs to the company that need to be documented. Very few companies realize the extent of this Section 404 impact. The Act is open ended. The rules, such as vacation tracking, are followed haphazardly in many areas around many companies and this documenting activity is part of compliance to the SOX Act. Subsidiaries and other partners or companies with business relationship practices are included in section 404.

Under SOX Act the internal auditors do not report to the CEO; rather, to a board member of the board of directors. Ex-internal auditor specialists are needed to help the CEO comply with Section 404. These auditor specialists are not doing audits, but preparing the company to meet or exceed the internal audit; hence, the external audit.

BEHAVIORAL BOUNDARIES (STEERING) COMMITTEE

The human resource department has handled many difficult situations regarding employee behavior. The process of education, regular training, and employee signing of policy documents falls under the human resource domain. The Behavioral Boundaries Committee is needed to protect the company in its control of management and workers. Issues from sexual harassment, to getting user login permission require a policy and it is to be signed by the employee.

Management in one area of the company joins the Behavioral Boundaries Committee to oversee and enforce another area of the company. A ring of managers can work to oversee each other as committee members with human resource superiors and chairperson. The mixing of management participation, ethics as a company goal promoted by human resource management protects and builds an ethical company. This is the story and plan that goes into the financial statement as a disclosure on an ethics program for the company and SOX Act compliance.

AFFECTS INFORMATION TECHNOLOGY

Corporations are going to have to invest in IT to handle all of the security issues. Projected IT financial spending amounts to 40 billion dollars in 2006 (Swann, 2005). Although mostly for maintenance, SOX Act is putting the IT focus on data security. Securing company information from email to hard disks pregnant with company financial data is paramount to comply with the Act. It refers to the area of managing risks.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission satisfies the SEC criteria for internal audits. A proactive approach is to go with COSO framework as an institutional strategy that would fund IT with appropriate money and support IT with the needed policy and procedures that meet the COSO framework. CobiT also provides a framework to supply proactive compliance (Coe, 2004).

CONTROLS FOR IT NETWORK SECURITY WITH CHECKLIST

IT networks are to be secure to comply with the SOX Act. COSO includes five levels in its internal controls model, which are control environment, risk assessment, control activities, information and communication and monitoring (The Institute of Auditors, 1998). CobiT from the The Information Systems Audit and Control Foundation (ISACA), Trusted Services, once referred to as SysTrust, from the foundations of the American Institute of Certified Public Accountants (AICPA) and the Assurance Services Development Board (ASDB) of the Canadian Institute of Chartered Accountants (CICA) posted the AICPA/CICA Privacy Framework and two other frameworks that are compliant for information technology management and control (Coe, 2004). A checklist for IT network compliance for the SOX Act follows (Gallegos, Senft, Manson, & Gonzalas, 2004):

Firewall: It is a must for a company or corporation at every entry into internal systems.

Access Control: Every entry into any system from outside or inside the company must have access control and policy and procedures for every access is required.

Authentication: Access authentication systems to protect systems, data, and network and to permit access based on policy and procedures are required.

Cryptography: Choosing cryptography methods with at least a 128 bit key length.

Virus Protection: Anti-virus software and regular updates.

Backup: Loss data protection and replacement is part and parcel to business continuity when accidents and disaster recovery occurs.

Intrusion detection and logging: The computer forensics requirements for corrective action when network intrusion or attacks are detected which requires monitoring software.

Operating Systems and Application protection: The need to secure the operating systems and application systems against intrusions and attacks.

Database and file systems: SOX Act addresses this as an area that involves email data and potential trading advantages via intrusion from gathering material information prior to public announcements, which could affect stock price changes.

Vulnerability Management: Using COPS, Crack, Tripwire software, vulnerabilities can be identified prior to intrusion.

Monitoring: A security professional awareness with the computer security industry is required (Gallegos, Senft, Manson, & Gonzalas, 2004).

SECURITY COMMITTEE

The Security Compliance Steering Committee is a way to set priorities and audit all areas of security and provide suggestions and directions to oncoming issues. Security is an ongoing effort and requires legal participation. A lawyer is needed whose focus is security. The members of the team include human resource people, IT people both in systems, applications and telecommunications, a security lawyer, management in all divisions and corporate executives CIO, CFO. Ex-Auditing specialists are best included for help in the processing of procedures.

Other companies determined the need for an executive officer called the Chief Security Officer (CSO) or Chief Compliance Officer (CCO) (Brady, 2005). This chosen person would improve and protect the company's operations and set policy for advancing compliant requirements from outside government agencies. This Security Committee will work with the Behavioral Boundaries Committee and the Audit Committee. The Security Committee will prepare security policy and procedures with regard to management and workers and supply them to the Behavioral Boundaries Committee to enact and enforce. Education, employee training and policy signatures will have security issues along with others for employee processing. The Audit committee will feed security breaches and risks to the Security Committee for remedy. A security committee protects the company's property and its material financial asset value critical to the CEO, the company and SOX Act compliance.

REFERENCES

References are available upon request.