# SOX and its effects on IT Security Governance

Rosslin John Robles[1], Min-kyu Choi[1], Sung-Eon Cho[2],
Yang-seon Lee[2], Tai-hoon Kim
[1]*School of Multimedia, Hannam University, Daejeon, Korea*
[2]*Dept of Information Communication, Sunchon Univerity, Sunchon, Korea*
[3]*Fumate Inc., Daejeon, Korea*
*rosslin_john@yahoo.com, secho@sunchon.ac.kr,*
*yslee@fumate.com, taihoonn@empal.com*

***Abstract***

*The Sarbanes-Oxley (SOX) Act is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. This paper discusses the effects of Sarbanes-Oxley (SOX) Act on corporate information security governance practices. The resultant regulatory intervention forces a company to revisit its internal control structures and asses the nature and scope of its compliance with the law. This paper reviews the implications emerging from the mandatory compliance with Sarbanes-Oxley (SOX) Act. Issues related to IT governance and the general integrity of the enterprise are also identified and discussed. Industry internal control assessment frameworks, such as COSO and COBIT, are reviewed and their usefulness in ensuring compliance evaluated.*

## 1. Introduction

Accounting scandals at some of the big corporations like Enron, HealthSouth, Tyco and WorldCom had a devastating impact on investor confidence. Clearly, it was possible to engage in frauds of such magnitude because of the inability of auditors to detect early signs of such possibilities. This paper reviews the impact of legal controls on Information Technology (IT) governance practices, especially in the case of SOX Act. The resultant crisis in the financial markets and massive media coverage of the frauds created a situation where government's interference was inevitable. The main reason cited, leading to such a situation, was a lack of accountability of top management to government and shareholders. Measures like assessment of internal controls on the part of corporations to restore investor confidence did not seem enough. Investor protection needed radical changes in the legal system as form of assurance.

## 2. Corporate & IT Management

Corporate Governance "is ethical corporate behavior by directors or others charged with governance in the creation and presentation of wealth of all stakeholders. The distribution of rights and responsibilities among different participants in the corporation, such as board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set and the means of attaining those objectives and monitoring performance.

### 2.1 IT Governance

Information Technology Governance, IT Governance or ICT (Information & Communications Technology) Governance, is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. The rising interest in IT governance is partly due to compliance initiatives, for instance Sarbanes-Oxley in the USA and Basel II in Europe, as well as the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization.

A characteristic theme of IT governance discussions is that the IT capability can no longer be a black box. The traditional involvement of board-level executives in IT issues was to defer all key decisions to the company's IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers, and in particular departments such as finance, have the necessary input into the decision making process. This prevents IT from independently making and later being held solely responsible for poor decisions. It also prevents critical users from later complaining that the system does not behave or perform as expected.

### 2.2 Role of Internal Controls

The Importance of identifying, establishing, and maintaining the integrity of internal controls has been felt by organizations for a rather long period of time. It was the Committee of Sponsoring Organizations of the Treadway Commission (COSO) that first introduced the framework for assessing internal controls in 1992. Subsequently, other frameworks, such as Control Objectives for Information and related Technology (COBIT), were developed and are now being extensively used by businesses.

### 2.3 Internal Control Objectives

Internal controls are a means to provide reasonable assurance that an organization will achieve its business objectives while avoiding undesired risks. Internal controls are policies, procedures, practices, and organizational structures put in place to reduce risks. At the heart of internal controls lies routinization of organizational processes. Any problem in the company ought to be corrected based on compliance or management initiated concerns. Internal control activities and supporting processes are either manual or supported by computers. They operate at all levels in an organization and help in reducing risks involved at various stages of the operation, thus helping the organization reach its business objectives.

### 2.4 The COSO framework

The COSO framework describes a unified approach for evaluation of the internal control system that a management designs to provide reasonable assurance of achieving the fundamental business objectives. The original COSO framework contains five control components that assure sound business objectives such as Control environment, Risk assessment, Control activities, Information and communication and Monitoring. These

components work to establish the foundation for sound internal control within the company through directed leadership, shared values and a culture that emphasizes accountability for control. The various risks facing the company are identified and assessed routinely at all levels and within all functions in the organization. Control activities and other mechanisms are proactively designed to address and mitigate the significant risks. Information critical to identifying risks and meeting business objectives is communicated through established channels up, down and across the company. The entire system of internal control is monitored continuously and problems are addressed timely.

### 2.5 COBIT

COBIT was developed to align IT resources and processes with business objectives, quality standards, monetary controls, and security needs. COBIT is composed of four domains: Planning and organization, Acquisition and implementation, Delivery and support and Monitoring.

The idea behind the COBIT framework is that information is needed to support business objectives and requirements. Companies should be able to assess the nature and extent of IT controls required to integrate their internal control objectives. Basically, it is important for a company to demonstrate how its IT controls support COSO and whether IT controls are appropriately documented in all COSO components. In COBIT, control objectives are defined in a manner consistent with COSO. It is a process-oriented framework following the concept of business reengineering. COBIT is comprised of four domains, 34 IT processes or high-level control objectives, and 318 detailed control objectives. A control objective has been identified and the rationale to link the document to business objectives has been provided at all identified processes and domains. It is a comprehensive framework for managing risk and control of information and related technology. COBIT 3rd edition, released in 1996, is the latest version available.

## 3. The Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 (Pub.L. 107-204, 116 Stat. 745, enacted 2002-07-30), also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox; is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These scandals, which cost investors billions of dollars when the share prices of the affected companies collapsed, shook public confidence in the nation's securities markets. Named after sponsors Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OH), the Act was approved by the House by a vote of 423-3 and by the Senate 99-0. President George W. Bush signed it into law, stating it included "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt."

The legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. It does not apply to privately held companies. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. Debate continues over the perceived benefits and costs of SOX. Supporters contend that the legislation was necessary and has

played a useful role in restoring public confidence in the nation's capital markets by, among other things, strengthening corporate accounting controls. Opponents of the bill claim that it has reduced America's international competitive edge against foreign financial service providers, claiming that SOX has introduced an overly complex and regulatory environment into U.S. financial markets. Sarbanes-Oxley contains 11 titles that describe specific mandates and requirements for financial reporting. Each title consists of several sections which are summarized as follows:

### 3.1 SOX Titles

**3.1.1 Title I: Public Company Accounting Oversight Board (PCAOB).** This title consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors").

**3.1.2 Title II: Auditor Independence.** Consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest.

**3.1.3 Title III: Corporate Responsibility.** Consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

**3.1.4 Title IV: Enhanced Financial Disclosures.** 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.

**3.1.5 Title V: Analyst Conflicts of Interest.** Consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

**3.1.6 Title VI: Commission Resources and Authority.** Consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC’s authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, adviser or dealer.

**3.1.7 Title VII: Studies and Reports.** Consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions.

**3.1.8 Title VIII: Corporate and Criminal Fraud Accountability.** Title VIII consists of seven sections and is also referred to as the “Corporate and Criminal Fraud Act of 2002”. It describes specific criminal penalties for fraud by manipulation, destruction or alteration of

financial records or other interference with investigations, while providing certain protections for whistle-blowers.

**3.1.9 Title IX: White Collar Crime Penalty Enhancement.** Consists of two sections. This section is also called the “White Collar Crime Penalty Enhancement Act of 2002.” This section increases the criminal penalties associated with white-collar crimes and conspiracies.

**3.1.10 Title X: Corporate Tax Returns.** Consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.

**3.1.11 Title XI: Corporate Fraud Accountability.** Title XI consists of seven sections. Section 1101 recommends a name for this title as “Corporate Fraud Accountability Act of 2002”. It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments.

### 3.2 The impact of Sarbanes-Oxley Sections on IT

**3.2.1 Corporate Responsibility.** Section 302 (CorporateResponsibility for Financial Reports) Applies to financial statements and related financial information. Requiring CEOs and CFOs to certify the following in each annual and quarterly report filed with the SEC: that the report has been reviewed and that, to the best of their knowledge, the report does not contain an untrue statement or omit any material fact.

**3.2.2 Enhanced Financial Disclosures.** Section 401. Disclosures in Periodic Reports requires the company to disclose "all material off-balance sheet transactions, arrangements, obligations (including contingent obligations) and other relationships" that might have a "material current or future effect"on the financial health of the company.

**3.2.3 White Collar Crime Penalty Enhancements.** Section 906. Corporate Responsibility for Financial Reports holds CEOs, CFOs, and corporate directors both accountable and liable for the accuracy of financial disclosures. In contrast to Section 302, Section 906 penalties apply only if the officer knows of the problem or error when certifying a report.

**3.2.4 Corporate and Criminal Fraud Accountability.** Section 802. Criminal Penalties for Altering Documents applies to the retention and protection of corporate audit documents and related records, including e-records. This section establishes new criminal penalties for document alteration and destruction.

## 4. IT controls and the Sarbanes-Oxley Act (SOX)

SOX requires the chief executive and chief financial officers of public companies to attest to the accuracy of financial reports (Section 302) and require public companies to establish adequate internal controls over financial reporting (Section 404). Passage of SOX resulted in an increased focus on IT controls, as these support financial processing and therefore fall into the scope of management's assessment of internal control under Section 404 of SOX.

The COBIT framework may be used to assist with SOX compliance, although COBIT is considerably wider in scope. The 2007 SOX guidance from the PCAOB and SEC state that IT

controls should only be part of the SOX 404 assessment to the extent that specific financial risks are addressed, which significantly reduces the scope of IT controls required in the assessment. This scoping decision is part of the entity's SOX 404 top-down risk assessment. In addition, Statements on Auditing Standards No. 109 (SAS109) discusses the IT risks and control objectives pertinent to a financial audit and is referenced by the SOX guidance.

To comply with Sarbanes-Oxley, organizations must understand how the financial reporting process works and must be able to identify the areas where technology plays a critical part. In considering which controls to include in the program, organizations should recognize that IT controls can have a direct or indirect impact on the financial reporting process. For instance, IT application controls that ensure completeness of transactions can be directly related to financial assertions. Access controls, on the other hand, exist within these applications or within their supporting systems, such as databases, networks and operating systems, are equally important, but do not directly align to a financial assertion. Application controls are generally aligned with a business process that gives rise to financial reports. While there are many IT systems operating within an organization, Sarbanes-Oxley compliance only focuses on those that are associated with a significant account or related business process and mitigate specific material financial risks. This focus on risk enables management to significantly reduce the scope of IT general control testing in 2007 relative to prior years.

## 5. Emergent Issues

The Sarbanes-Oxley Act is exerting tremendous pressure on IT organizations to attest to the control of IT processes related to financial reporting. Only recently has the daunting scope of these requirements become apparent to them, and a majority of IT organizations are struggling to cope with these overwhelming compliance demands. These new responsibilities add significant effort to the already daunting IT business management challenges —pressure on IT to drive more business value, lower costs, and maintain high-service levels.

The Sarbanes-Oxley Act will create new avenues of concern for organizations having to cope with pressures to improve the quality of information for the sake of compliance in the coming years. The tools for automatic control mapping, evaluating online and realtime control functioning will greatly facilitate compliance.

## 6. Key Findings

Companies don’t focusing on technology fixes instead they focus on auditing, procedures, and reporting. Most are not buying new technology to solve, but may upgrade or partially replace to address. Split on whether finance understands technology issues involved in SOX compliance, and whether IT understands the business issues IT will be affected by SOX, more so than all other departments except finance. Most viewSOX compliance more resource intensive than other regulatory compliance projects. Almost 1 in 10 thinks their job is at risk if the firm is non-compliant and 1 in 4 must certify results personally. Vendors are talking about SOX but not delivering much. To comply with the SOX, companies will need to improve information quality and Technology improvements are required to provide cost-efficient, online, real-time reporting. SOX can’t legislate ethics and integrity into the public management process.

## 7. Conclusion

SOX has created challenges and set new standards for IT governance in companies. To fully comply with the law, companies will need to improve information quality to insure transparency and reliability. Investors (individual or institutional) are outsiders for the most part and can only rely on the good faith of corporate insiders for insight into effectiveness of the companies. To protect such investors, SOX attempts to legislate ethics and integrity into the public management process. Sarbanes-Oxley was created to restore investor confidence in public markets. This Act has literally rewritten the rules for accountability, disclosure, and reporting of good corporate governance. Ethical practices are no longer optional. The responsibility of making this Act a success lies with the managers and auditors of each and every firm. Such legislation can act as a watchdog, but morality cannot be legislated.

## References

[1] Dhillon, G., Mishra S. (2006) The Impact of Sarbanes-Oxley (SOX) Act on Information Security Governance

[2] Alles, M., Kogan, A., & Vasarhelyi, M. (2004). The law of unintended consequences? Assessing the costs, benefits and outcomes of the Sarbanes-Oxley Act. Information Systems Control Journal, 1, 17-20.

[3] Anantha, S. (2004). Auditing governance in ERP projects. Information Systems Control Journal, (2),19.

[4] Anderson, P. J., & Black, A. R. (2002, October 23). Accountants'liability after Enron. S&P's: The Review of Securities & Commodities Regulation, 35(18), 227.

[5] Coates, B. E. (2003). Rogue corporations, corporate rogues & ethics compliance: The Sarbanes-Oxley Act, 2002. Public Administration and Management, 8(3), 164-185.

[6] Gallagher, S. (2003, August 1). Gotcha! Complying with financial regulations. Baseline Magazine. Retrieved November 29, 2005, from http://www.baselinemag.com/article2/0,3959,1211224,00.asp

[7] General Masters, Inc. (2004). COSO framework and Sarbanes Oxley [Electronic Version]. Retrieved July 2, 2005, from http://www.gmasterinc.com/coso/cosomain.htm

[8] Hagerty, J., & Scott, F. (2005). SOX spending for 2006 to exceed $6B. AMR Research. Retrieved November 29, 2005, from http://www.amrresearch.com/content/view.asp?pmillid=18967

[9] Hoffman, T. (2003). Users struggle to pinpoint IT costs of Sarbanes-Oxley compliance. Computerworld, December 1. Retrieved November 29, 2005, from http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,87613,00.html

[10] Volonino, L., Kermis, G., & Gessner, G. (2004, August 5-8). Sarbanes-Oxley links IT to corporate compliance. In Proceedings of the Tenth Americas Conference on Information Systems. New York: Association for Information Systems