IDEA GROUP PUBLISHING **ITB12227**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter V

The Impact of Sarbanes-Oxley (SOX) Act on Information Security Governance

Gurpreet Dhillon, Virginia Commonwealth University, USA

Sushma Mishra, Virginia Commonwealth University, USA

Abstract

This chapter discusses the impact 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 assess the nature and scope of its compliance with the law. This chapter reviews the organizational implications emerging from the mandatory compliance with SOX. Industry internal control assessment frameworks, such as COSO and COBIT, are reviewed and their usefulness in ensuring compliance evaluated. Other emergent issues related to IT governance and the general integrity of the enterprise are identified and discussed.

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. In the case of Enron, an accounting loophole allowed the company to use gross instead of net value to calculate profits from energy contracts (Ackerman, 2002). Many shareholders lost their confidence in corporate reporting of company financial statements and generally in the integrity of the auditors. Issues such as lack of independence of auditors providing higher margin consulting services to audit clients, limited independence by corporate directors, increased use of stock options as a means of compensation, and inadequacy of the *generally accepted accounting principles* (GAAP) came to the fore.

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 (Agarwal & Chadha, 2004). Investor protection needed radical changes in the legal system as form of assurance. Thus, the U.S. government intervened by passing the Sarbanes-Oxley Act in 2002.

This chapter reviews the impact of legal controls on *information technology* (IT) governance practices, especially in the case of the SOX Act. The chapter is organized into four sections. The first section describes the concepts of corporate governance, IT governance, and internal controls. A review of the definitions is followed by a rationale for good corporate governance practices. The next section discusses specific titles of SOX Act that impact IT governance practices. Interpretations of those areas of SOX that relate to increased importance of IT Governance are then presented and emerging issues associated with compliance with this law are identified and addressed. The concluding section presents a discussion of the future challenges and implications.

Corporate Governance and IT Management

Corporate governance, as defined by the *Certified Information Systems Auditor* (CISA) Review Manual (2004), is ethical corporate behavior by directors or others charged with governance in the creation and presentation of wealth for all stakeholders. The ethical issues of an organization are fostered through corporate governance practices. The practice of corporate governance is further defined by the *Organization for Economic Cooperation and Development* (OECD, 2004) as: