Information Security Journal: A Global Perspective, 17:75–79, 2008

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393550801953372

Taylor & Francis
Taylor & Francis Group

Information Security Implications of Sarbanes-Oxley

Sanjay Anand
SOX (GRC) Institute, Clifton, NJ, USA

ABSTRACT The purpose of this article is to inform and educate the Information Security (IS) professional about some of the key/fundamental tenets of Sarbanes-Oxley (SOX), especially in the context of Confidentiality, Integrity and Availability of information, the three cornerstones of every security initiative. The focus is on such Sections of the Act as 404 (Internal Controls), 302 (Management Certifications), 806 (Whistleblower Protections), 409 (Real Time Disclosures), 802 (Alteration of Documents), amongst others. The purpose is to develop an appreciation and understanding of IS requirements and implications of SOX, and likewise to better understand how SOX can provide a basic roadmap for IS that every professional, department and organization may be able to use.

KEYWORDS segregation of duties, internal controls, records retention, records destruction, transparency, access control, COSO

INTRODUCTION

The purpose of this article is to explore the relationship between Sarbanes-Oxley (SOX[1]) and information security and to illustrate, through specific examples, how this relationship is a natural fit and how the two leverage off of each other. We will look at:

(a) What is SOX – a brief overview of the Act and specifically the famous/infamous Section 404,
(b) Segregation of Duties (SoD) from a Section 404 Internal Controls perspective,
(c) Other relevant sections of the Act as they apply to information security professionals and departments,
(d) Special cases and examples of how this interrelationship between SOX and information security has been played out in the real world, and finally
(e) Recommendations for how you as an information security professional can continue to leverage what you do in the context of SOX and other/similar regulations.

Address correspondence to Professor Sanjay Anand, Chairman, SOX (GRC) Institute, 1360 Clifton Avenue, Clifton, NJ 07012. E-mail: sanjay@anands.com

While it is difficult, if not impossible, to cover all the aspects of the interrelationship between SOX and information security, this article will attempt