# INFORMATION TECHNOLOGY AND THE SARBANES-OXLEY ACT

*David Olsen, Utah State University, David Luthy, Utah State University*

## ABSTRACT

A series of spectacular failures in corporate governance at several companies that resulted in tremendous losses gave rise to the U.S. Public Company Accounting Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act (SOX). Certain issues concerning corporate governance and internal control are addressed by SOX in an attempt to improve the overall controls associated with financial reporting. Among other things, senior management is required to provide an annual certification concerning internal controls where, in today's organizations, information technology (IT) is inherently a key component. External auditors are then required to audit and report on management's certification.

Even though the trend has been evident for some time, SOX is moving IT from being mostly a technical management issue to being a concern about governance and control across the organization. It is clear that in modern organizations IT is so important that there is a critical codependency between corporate governance and IT where one cannot be considered without the other. This changing environment calls for an expanded understanding and appreciation for the interaction effects between IT and corporate governance in general. Specifically, it appears that a collateral effect of SOX is that an underlying tension between IT professionals and auditors is magnified. For example, the following appears under the heading "Sarbanes-Oxley: Accountants Setting IT Policy."

"We were just wrung through the Sarbanes-Oxley wringer here. And in my opinion, the effort was a total waste of time. The auditors didn't know what they were supposed to do, and they missed a lot of things that would have benefited from closer audit scrutiny. Important concerns were either given a cursory look or totally ignored, while auditors focused on 'important' financial bottom-line stuff like "How often do you change passwords?" and "Where do you store your backup drives?" Those are certainly valid IT audit concerns, but I kept asking them "How does this affect our corporate financial statements?" It seems to me that auditors with lots of axes to grind went way overboard in using Sarbanes-Oxley as a big stick to get their way on certain things."

The sentiment expressed above may be an isolated opinion. However, it may indicate that there is a need for IT professionals and accountants/auditors to better understand the increasingly overlapping domains in which they each operate. The purpose of this paper is to outline the theoretical and practical overlap or bridge between IT and accounting/auditing to help clarify the current environment within which companies must operate as required by SOX. The discussion begins with an overview of SOX requirements as promulgated by the Public Company Accounting Oversight Board (PCAOB), the organization that is responsible under SOX for auditing standards. Then, the accounting and audit process is outlined, including generally accepted auditing standards, as they relate to financial statement disclosures. Next, the pervasive role of IT in the generation of financial statements starts to be evident with a discussion of the "Enterprise Risk Management Framework" of the Committee of Sponsoring Organizations of the Treadway Commission (COSO-ERM). The more specific audit and internal control aspects related to IT are then outlined in light of the "Internal Control – Integrated Framework" that is also authored by COSO. Finally, the very specific aspects of "Control Objectives for Information and Related Technology" (COBIT) are presented. Several other very specific control frameworks are mentioned including ISO 17799 and Information Technology Infrastructure Library (ITIL).