Chapter XIV

Information Disclosure and Regulatory Compliance: Economic Issues

Anindya Ghose, New York University, USA

Abstract

The Sarbanes-Oxley Act (SOX) introduced significant changes to financial practice and corporate governance regulation, including stringent new rules designed to protect investors by improving the accuracy and reliability of corporate disclosures. Briefly speaking, it requires management to submit a report containing an assessment of the effectiveness of the internal control structure, a description of material weaknesses in such internal controls and of any material noncompliance. Such mandatory regulations can have some broader ramifications on firm profitability, market structure, and social welfare, many of which were unintended when policy makers first formulated this act. Moreover, the tight coupling of compliance activities, information disclosure, and information technology (IT) investments can have implications for IT governance because of its potential to change relationships between technology investments and business. This chapter aims to provide some intuitive insights into the trade offs involved for firms in disclosure of such information, and lays the ground for some research questions that would be of interest to academics, industry executives, and policy makers, alike.
Introduction

The SOX was formulated to increase companies’ compliance with Securities and Exchange Commission (SEC) disclosure laws. In the aftermath of Enron, World Com, Tyco, and other high-profile business scandals between December 2001 and June 2002, congress reacted rapidly to introduce the SOX. What prompted lawmakers to create this provision was the concern that there was a lack of sufficient controls at these scandal-ridden firms and that firms’ financial statements needed to be accurate. Thus, SOX required managers to implement controls over the financial reporting process and state whether they were effective.

In particular, SOX introduced significant changes to financial practice and corporate governance regulation, including stringent new rules designed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. Perhaps the part of the act having the most impact was Section 404. This section requires management to submit to the SEC the company’s annually filed financial statements, an internal control report, that states the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It also contains an assessment, as of the end of the fiscal year, of the effectiveness of the internal control structure and procedures for financial reporting. It also requires auditors to attest to and report on the management’s assessment of the internal control systems. Such reports include a description of material weaknesses in such internal controls and of any material noncompliance.

Since modern financial reporting systems are heavily dependent on technology and associated controls, any review of internal controls would not be complete without addressing controls around information security. An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or data manipulation, each of which can compromise data integrity. SOX focuses on management accountability and operating efficiencies in firms. Both of these are tightly coupled with investments in IT and the role played by IT professionals. Indeed, sections 302 and 404 indirectly force the scrutiny of information security controls for SOX compliance. The implication of these new regulations is that organizations, especially those dealing with financial information, must establish the appropriate processes and technologies to evaluate data usage requirements for all users and create a data usage control policy that defines how data may be used by each user. They need to record database activity and report on deviations from the data usage control policy. Further, they need to alert management when a deviation from usage control policy might violate data integrity.

There’s been a lot of debate about the impact of new government and industry regulations on IT departments, especially in the financial services sector. The financial services sector has long been presumed to practice superior information security, largely because of the preciousness of its assets and the fact that its business is carried out almost entirely on IT systems. A study based on interviews with 100 IT managers in UK financial services companies reveals that given the current level of investment in technologies that help companies comply with regulations such as SOX, around 60% of IT managers from financial services companies believe the demand on IT to deal with compliance issues will increase over the coming three years (Carr, 2006). Indeed, the study states that most respondents are not satisfied with their current capabilities to perform tasks necessary for compliance, such as
The Brazilian Case of IFRS Adoption: The Impacts and the New Perspectives
www.igi-global.com/chapter/the-brazilian-case-of-ifrs-adoption/147329?camid=4v1a