★ CLOSING CASE ONE

Sarbanes-Oxley: Where Information Technology, Finance, and Ethics Meet

The Sarbanes-Oxley Act (SOX) of 2002 was enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices by organizations. One primary component of the Sarbanes-Oxley Act is the definition of which records are to be stored and for how long. For this reason, the legislation not only affects financial departments, but also IT departments whose job it is to store electronic records. The Sarbanes-Oxley Act states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." The consequences for noncompliance are fines, imprisonment, or both. The following are the three rules of Sarbanes-Oxley that affect the management of electronic records.

1. The first rule deals with destruction, alteration, or falsification of records and states that persons who knowingly alter, destroy, mutilate, conceal, or falsify documents shall be fined or imprisoned for not more than 20 years or both.
2. The second rule defines the retention period for records storage. Best practices indicate that corporations securely store all business records using the same guidelines set for public accountants, which state that organizations shall maintain all audit or review workpapers for a period of five years from the end of the fiscal period in which the audit or review was concluded.
3. The third rule specifies all business records and communications that need to be stored, including electronic communications. IT departments are facing the challenge of creating and maintaining a corporate records archive in a cost-effective fashion that satisfies the requirements put forth by the legislation.

Essentially, any public organization that uses IT as part of its financial business processes will find that it must put in place IT controls in order to be compliant with the Sarbanes-Oxley Act. The following are a few practices you can follow to begin to ensure organizational compliance with the Sarbanes-Oxley Act.

- Overhaul or upgrade your financial systems in order to meet regulatory requirements for more accurate, detailed, and speedy filings.
- Examine the control processes within your IT department and apply best practices to comply with the act's goals. For example, segregation of duties within the systems development staff is a widely recognized best practice that helps prevent errors and outright fraud. The people who code program changes should be different from the people who test them, and a separate team should be responsible for changes in production environments.
- Homegrown financial systems are fraught with potential information-integrity issues. Although leading ERP systems offer audit-trail functionality, customizations of these systems often bypass those controls. You must work with internal and external auditors to ensure that customizations are not overriding controls.
- Work with your CIO, CEO, CFO, and corporate attorneys to create a document-retention-and-destruction policy that addresses what types of electronic documents should be saved, and for how long.

Ultimately, Sarbanes-Oxley compliance will require a great deal of work among all of your departments. Compliance starts with running IT as a business and strengthening IT internal controls.[6]