

SARBANES OXLEY AND HOW IT AFFECTS INFORMATION TECHNOLOGY

Susan Orr

Susan Orr Consulting

President Bush signed the Sarbanes Oxley Act into law on July 30, 2002. The Act targets improving corporate governance and includes numerous provisions addressing financial disclosures and auditing relationships of public companies, including public banking organizations. However, banking organizations are only directly subject to Sarbanes-Oxley if the company has a class of securities registered or the company is required to file reports under the Securities Exchange Act of 1934, or if the financial institution has registered its securities with the appropriate federal banking agency under Section 12 of the Securities Exchange Act of 1934. All financial institutions that have assets of \$500 million or more, whether or not they are publicly traded, are subject to the provisions of Section 36 of the FDI Act and the FDIC's implementing regulations and guidelines, 12 CFR Part 363. Section 36 and Part 363 require an annual management report, and impose annual auditing and attestation, and audit committee requirements on covered depository institutions. Financial institutions with assets less than \$500 million do not fall under the requirements of Sarbanes Oxley; however, certain provisions of Sarbanes Oxley mirror regulatory guidance and policy relating to corporate governance.

Sarbanes Oxley has significantly increased accountability of directors, auditors, and legal council. Corporate officers who sign false financial statements, knowingly, can be fined up to \$1 million and face up to 10 years in prison. The Securities and Exchange Commission, the New York Stock Exchange, and NASDAQ are the primary regulatory agencies for Sarbanes Oxley. The Public Company Accounting Oversight Board (PCAOB) has oversight responsibilities.

While Sarbanes Oxley does not directly regulate technology it does regulate business practices, which include manual and electronic (IT) processes and the implementation of internal controls. The SEC defines internal control over financial reporting as a process designed by, or under the supervision of the company's principal executive and financial officers, or persons performing similar functions, and implemented by the board of directors, management, and other personnel to provide a reasonable assurance regarding the reliability of financial reporting and the preparation of the financial statements for external use in accordance with generally accepted accounting principles and includes policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer,
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting

principles, and that receipts and expenditures of the issuer are being made only in accordance with authorization of management and directors of the issuer, and

- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.

There is also a direct correlation between Sarbanes Oxley and the Gramm-Leach-Bliley Act of 1999 requirement of a written comprehensive security program. Sarbanes Oxley addresses the requirement of an appropriate awareness of security policies and procedures and management's commitment to designing, implementing, and monitoring security controls. In addition, security policies are to be documented and audited.

Sections 302 and 304 of Sarbanes Oxley specifically require businesses to design, implement, and monitor internal controls. Section 404 mandates that organizations file an assessment of its internal controls on an annual basis. IT plays a very important role in supporting the financial systems and data as well as in protecting the systems and data from unauthorized access and fraudulent abuse. "Strong internal controls provide better opportunities to detect and deter fraud. For example, many frauds resulting in financial statement restatement relied on the ability of management to exploit weaknesses in internal control. Part of management's responsibility when designing a company's internal control over financial reporting is to design and implement programs and controls to prevent, deter, and detect fraud."¹ IT security controls are a key element of overall internal controls.

Preventing and deterring fraud directly relate to the IT controls the organization has implemented. The first step in developing and implementing these controls is performing a risk assessment including an assessment of data security, data and system availability and performance. Once the risks are identified, policies, procedures, and controls must be put into place to prevent and deter unauthorized access to and misuse of internal systems and information. Unauthorized access can occur from inside the network as well as externally. Connecting to the Internet exposes financial data and systems to unauthorized access and potential misuse, therefore it is imperative that organizations implement the appropriate security controls to prevent and deter access, i.e. firewalls, vulnerability monitoring. In addition, if the organization itself or its customers conduct ecommerce transaction online, financial data is at risk due the lack of proper authentication, which can lead to Domain Name Server (DNS) poisoning and Border Gateway Protocol (BGP) hijacking making transaction monitoring and authentication a priority. However, you don't have to be connected to the Internet for threats to the data and systems to exist. Security threats also originate from inside the network, making it necessary to monitor the internal environment to prevent and deter unauthorized access and potential misuse. Organizations should be monitoring the internal network for rogue network devices that have connected to the network, as well as rogue wireless devices. It is not uncommon for contractors and or auditors to connect to an organizations network; however, in doing so the network becomes susceptible to the outside and to viruses and vulnerabilities. There is also a growing threat from unauthorized and undetected wireless networks connecting to the organizations internal network.

¹ Public Company Accounting Oversight Board draft audit standard, October 7, 2003.

Once the appropriate controls have been implemented, to ensure continuous effectiveness and performance of those controls, the next step is to institute a process to monitor and test (validate) the controls. There are several methods for monitoring and testing controls. Conducting port scans on firewalls, monitoring for vulnerabilities, penetration testing, firewall logging, and network monitoring are all examples of monitoring and testing that are performed electronically using technology. Controls can also be tested manually through auditing, which includes inquiries into the processes, inspection of documentation, observation of the controls in use, and or an analysis using selected transactions. The most complete method would be a combination of both electronic methods and internal/external auditing.

The responsibility for appropriate security and internal controls is not limited to internally administered systems. Outsourcing data processing or security does not relieve management of its responsibility of ensuring that the controls in place with the service provider are effective and adequate, and that the controls are monitored and tested. Therefore, management should implement an ongoing oversight program over the service provider's activities. Management should not overly rely on assertions and representations from the service provider, but review the controls and testing that is performed by the service provider. ■

Susan Orr is a leading financial services expert with vast regulatory, risk management, and security best practice knowledge and expertise . During her 14 year tenure as a bank examiner, Susan held numerous lead positions including Regional IT Examination Specialist, Special Assistant to the Regional Director, Special Assistant to the Director of DSC, and Special Assistant to the Vice Chairman of the FDIC. Susan was also a lead instructor for the FDIC's technology school and was instrumental in key industry initiatives such as the FDIC E-Risk Strategic Initiatives Risk Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites. Prior to launching her consulting practice, Susan was Vice President of Regulatory Compliance at for an Internet security company where she advised staff, customers, and partners on regulation, security, and risk management. Susan retains close relationships within the FFIEC agencies as well as industry trade groups to stay abreast on new technologies, best practices, and regulatory issues.

Susan currently consults for several security providers and vendors as well as performs IT security and regulatory reviews for financial institutions. She also speaks regularly at risk management and security educational seminars and has authored numerous white papers on emerging information technology and security risk management topics. Susan is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Risk Professional (CRP).