EDP AUDITING

Sarbanes–Oxley Act of 2002 (PL 107-204) and Impact on the IT Auditor

Frederick Gallegos, CISA, CGFM, CDE

INSIDE

Major Points from the Sarbanes–Oxley Act of 2002; Criminal Intent; Legal Implications for External Auditors; The Sarbanes–Oxley Act Forces Organizations to Implement Strong Internal Controls; Potential Impact on the IT Audit Profession; The Potential Costs of Such Implementations

INTRODUCTION

The world of financial auditing has changed dramatically during the past decade and will continue to change rapidly as more and more companies rely on information technology to achieve their business objectives. Certainly, the passage of the Sarbanes–Oxley Act of 2002 (Public Law 107-204) will have a major impact on the internal and external auditor. Also, the IT auditor will play an integral role in assuring compliance with this act.

It is no longer acceptable for auditors to audit around the computer, as was once the case. With the increase in fraud and ceaseless corporate scandals over the past two years, it is now even more imperative than ever before that auditors have a full understanding of both manual and automated internal control processes. The assessment of both the manual and automated internal controls of any system can provide the needed assurance auditors can use to base their professional judgment on as far as the quality of the information derived from the system. This judgment is a key element in the risk analysis process that the auditor must perform during the planning stages of any audit.

External financial auditors are relying more on the process approach today

PAYOFF IDEA

The Sarbanes–Oxley Act of 2002 (Public Law 107-204) is probably one of the most influential federal acts on preventing financial fraud of this decade. For the internal auditor, it has preserved their careers from being outsourced. For the remaining Big 4 accounting firms, it has served due notice that they must not cross the line of independence in their role as financial auditors and must practice due professional care at all times. This act has provided a much-needed lift to the importance of internal auditors and their policies, procedures, and practices for the organizations they serve. This article provides a summary overview of Sarbanes–Oxley Act and its impact on the IT audit professional.

Auerbach Publications
© 2003 CRC Press LLC

rather than the traditional transaction approach. The results of an evaluation of an organization's manual and automated internal controls can either increase or reduce the amount of transaction testing needed to render an opinion on financial statements.

For internal auditors, internal controls are also very important. One of the primary functions of an internal auditor is to provide assurances to management that their approved internal controls are in place and are working effectively and efficiently; and if in fact there are problems, they are being addressed and corrected.

It is important for both the manual and automated internal controls to be operational and effective because management will base its business decisions on the financial results generated from the information system.

It is also important to external auditors that manual and automated internal controls are operational and effective because this will provide assurance to external auditors that information generated from the system is valid, accurate, and complete. Based on this assurance from the system, auditors can then place the appropriate level of reliance on the internal controls of the information system.

If the necessary controls are not in place, or if they are in place but not being applied effectively and as management intended, then the integrity of the data and the information generated from the system should be called into question by both external and internal auditors.

Although it is essential that manual controls are in place and are working effectively and efficiently to produce accurate data output, due to the broadness of the subject matter, this article focuses on auditors' reliance on automated internal controls and the effects of this reliance on the auditors' judgment in assessing business risk related to the integrity of information generated from the system.

As mentioned in an earlier article on the subject of due professional care, the Sarbanes–Oxley Act has provided the needed muscle of internal auditors to do their job better and has added accountability to management to take action on whatever auditors might identify.

Once again, financial fraud came to the forefront of the audit community at the beginning of this decade as a result of the financial scandals of Enron, Global Crossing, and others. The Equity Funding scandal of 1973 gave rise to the development of strong state and federal regulation of the insurance industries and corporate creative accounting of oil companies and the aerospace industry, and provided support for the development and enactment of the Foreign Corrupt Practices Act of 1977.

Now, perhaps, the Sarbanes–Oxley Act of 2002 will be a vivid reminder of the importance of due professional care and financial integrity. This act is a major reform package mandating the most far-reaching changes Congress has imposed on the business world since the Foreign Corrupt Practices Act of 1977 and the SEC Act of the 1930s. It seeks to thwart future scandals and restore investor confidence by, among other things, creating a Public Company Accounting Oversight Board (the Board) revising auditor independence rules, revising corporate governance standards, and significantly increasing the criminal penalties for violations of securities laws.

MAJOR POINTS FROM THE SARBANES–OXLEY ACT OF 2002

The act discusses requirements for the Board, including composition and duties. The Board must:

1. Register public accounting firms.
2. Establish, or adopt, by rule, auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers.
3. Conduct inspections of accounting firms.
4. Conduct investigations and disciplinary proceedings, and impose appropriate sanctions.
5. Perform such other duties or functions as necessary or appropriate.
6. Enforce compliance with the act, the rules of the Board, professional standards, and the securities laws relating to the preparation and issuance of audit reports and the obligations and liabilities of accountants with respect thereto.
7. Set the budget and manage the operations of the Board and the staff of the Board.

The Sarbanes–Oxley Act of 2002 focuses on the importance of due professional care. This act prohibits all registered public accounting firms from providing audit clients, contemporaneously with the audit, certain non-audit services, including internal audit outsourcing, financial-information-system design, and implementation and expert services. These scope-of-service restrictions go beyond existing Securities and Exchange Commission (SEC) independence regulations. All other services, including tax services, are permissible only if preapproved by the issuer's audit committee and all such preapprovals must be disclosed in the issuer's periodic reports to the SEC.

The act requires auditor (not audit firm) rotation. Therefore, the lead audit partner or the concurring review partner must rotate off the engagement if he or she has performed audit services for the issuer in each of the five previous fiscal years. The act provides no distinction regarding the capacity in which the audit or concurring partner provided such audit services. Any services provided as a manager or in some other capacity appear to count toward the five-year period. The provision starts as soon as the firm is registered; so, absent guidance to the contrary, the audit and concurring partner must count back five years, starting with the date in which Public Company Accounting Oversight Board (the Board) registration occurs. This provision has a definite impact on small accounting firms. The SEC is currently considering whether or not to accommodate small firms in this area; currently, there is no small-firm exemption from this provision.

As previously discussed, the Sarbanes–Oxley Act of 2002 is a major reform package mandating the most far-reaching changes Congress has imposed on the business world since the Foreign Corrupt Practices Act of 1977 and the SEC Act of the 1930s. It seeks to thwart future scandals and restore investor confidence by, among other things, creating a Public Company Accounting Oversight Board, revising auditor independence rules, revising corporate governance standards, and significantly increasing the criminal penalties for violations of securities laws.

To audit a public company, a public accounting firm must register with the Board. The Board will collect a registration fee and an annual fee from each registered public accounting firm, in amounts that are sufficient to recover the costs of processing and reviewing applications and annual reports. The Board will also establish a reasonable annual accounting support fee to maintain the Board.

Annual quality reviews must be conducted for firms that audit more than 100 issuers; all others must be conducted every three years. The SEC and/or the Board can order a special inspection of any firm at any time. The Board of a firm can impose sanctions if the firm fails to reasonably supervise any associated person with regard to auditing or quality control standards. The act also includes foreign accounting firms that audit a U.S. company to registrations with the Board. This would include foreign firms that perform some audit work, such as in a foreign subsidiary of a U.S. company that is relied upon by the primary auditor.

It is unlawful for a registered public accounting firm to provide any non-audit service to an issuer during the same time as the audit, including:

1. Bookkeeping or other services related to the accounting records or financial statements of the audit client
2. Financial information systems design and implementation
3. Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
4. Actuarial services
5. Internal audit outsourcing services
6. Management functions or human resources
7. Broker or dealer, investment adviser, or investment banking services
8. Legal services and expert services unrelated to the audit
9. Any other service that the Board determines, by regulation, is impermissible.

The Board may, on a case-by-case basis, exempt from these prohibitions any person, issuer, public accounting firm, or transaction, subject to review by the Commission. However, the SEC has oversight and enforcement authority over the Board. The Board, in its rule-making process, is to be treated as if it is a registered securities association. A registered securities association is defined in Section 15A Registered Securities Associations of the Securities & Exchange Act of 1934.

It will not be unlawful to provide other non-audit services if they are preapproved by the audit committee in the following manner. The Sarbanes–Oxley Act allows an accounting firm to engage in any non-audit service, including tax services that are not listed above, only if the activity is preapproved by the audit committee of the issuer. The audit committee will disclose to investors in periodic reports its decision to preapprove non-audit services. Statutory insurance company regulatory audits are treated as an audit service, and thus do not require preapproval.

The preapproval requirement is waived with respect to the provision of non-audit services for an issuer if the aggregate amount of all such non-audit services

provided to the issuer constitutes less than 5 percent of the total amount of revenues paid by the issuer to its auditor (calculated on the basis of revenues paid by the issuer during the fiscal year when the non-audit services are performed); such services were not recognized by the issuer at the time of the engagement as non-audit services; and such services are promptly brought to the attention of the audit committee and approved prior to completion of the audit. The authority to preapprove services can be delegated to one or more members of the audit committee, but any decision by the delegate must be presented to the full audit committee.

For independence acceptance, the lead audit or coordinating partner and the reviewing partner must rotate off the audit every five years. Also, the accounting firm must report to the audit committee all critical accounting policies and practices to be used, all alternatives methods to generally accepted accounting principles (GAAP) that have been discussed with management, and the ramifications of the use of such alternative disclosures and methods.

Another audit independence compliance issue is that the CEO, Controller, CFO, Chief Accounting Officer, or person in an equivalent position cannot have been employed by the company's audit firm during the one-year period preceding the audit. The CEO and CFO of each issuer will prepare a statement to accompany the audit report to certify the appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly represent, in all material respects, the operations and financial condition of the issuer. A violation of this section must be knowing and intentional to give rise to liability. It will be unlawful for any officer or director of an issuer to take any action to fraudulently influence, coerce, manipulate, or mislead any auditor engaged in the performance of an audit for the purpose of rendering the financial statements materially misleading.

The act penalizes executives for non-performance. If an issuer is required to prepare a restatement due to material noncompliance with financial reporting requirements, the CEO and the CFO must reimburse the issuer for any bonus or other incentive-based or equity-based compensation received during the 12 months following the issuance. It prohibits the purchase or sale of stock by officers, directors, and other insiders during blackout periods. Any profits resulting from sales in violation of this will be recoverable by the issuer.

Each financial report that is required to be prepared in accordance with GAAP will reflect all material correcting adjustments that have been identified by a registered accounting firm. Each annual and quarterly financial report will disclose all material off-balance sheet transactions and other relationships with unconsolidated entities that may have a material current or future effect on the financial condition of the issuer.

The SEC will study off-balance sheet disclosures to determine (1) the extent of off-balance sheet transactions (including assets, liabilities, leases, losses, and the use of special-purpose entities); and (2) whether generally accepted accounting rules result in financial statements of issuers reflecting the economics of such off-balance sheet transactions to investors in a transparent fashion and make a report

containing recommendations to Congress. Generally, it will be unlawful for an issuer to extend credit to any director or executive officer. Consumer credit companies can make home improvement and consumer credit loans and issue credit cards to their directors and executive officers if it is done in the ordinary course of business on the same terms and conditions made to the general public. Also, directors, officers, and 10-percent owners must report designated transactions by the end of the second business day following the day on which the transaction was executed.

The act requires each annual report of an issuer to contain an "internal control report." The SEC will issue rules to require issuers to disclose whether at least one member of its audit committee is a "financial expert." And, the issuers must disclose information on material changes in the financial condition or operations of the issuer on a rapid and current basis.

CRIMINAL INTENT

The Sarbanes–Oxley Act identifies as a crime for any person to corruptly alter, destroy, mutilate, or conceal any document with the intent to impair the object's integrity or availability for use in an official proceeding or to otherwise obstruct, influence, or impede any official proceeding. A convicted violator is subject to a maximum prison sentence of up to 20 years in prison and a fine. Also, the SEC is authorized to freeze the payment of an extraordinary payment to any director, officer, partner, controlling person, agent, or employee of a company during an investigation of possible violations of securities laws. Finally, the SEC can prohibit a person from serving as an officer or director of a public company if the person has committed securities fraud.

- Title VIII:
  - It is a felony to "knowingly" destroy or create documents to "impede, obstruct or influence" any existing or contemplated federal investigation.
  - Auditors are required to maintain "all audit or review work papers" for five years.
  - The statute of limitations on securities fraud claims is extended to the earlier of five years from the fraud, or two years after the fraud was discovered, from three years and one year, respectively.
  - Employees of issuers and accounting firms are extended "whistleblower protection" that would prohibit the employer from taking certain actions against employees who lawfully disclose private employer information to, among others, parties in a judicial proceeding involving a fraud claim. Whistleblowers are also granted a remedy of special damages and attorney fees.
- Title IX:
  - Maximum penalty for mail and wire fraud increased from five to ten years.
  - The CEO and CFO must certify financial statements filed with the SEC. The certification must state that the financial statements and disclosures

fully comply with provisions of the SEC Act and that they fairly present, in all material respects, the operations and financial condition of the issuer. Maximum penalties for willful and knowing violations of this section are a fine of not more than $5,000,000 and/or imprisonment of up to 20 years.

LEGAL IMPLICATIONS FOR EXTERNAL AUDITORS

In the pre-Sarbanes–Oxley years, the establishment of "Limited Liability Partnership" came as a result of a Big 5 organization that was taken to court by a client. The client, who selected a support system based on the firm's recommendation, failed to perform in the manner recommended and caused the company financial loss. The courts held the Big 5 firm liable for not exercising "due professional care" in the conduct of its work performed.

Today, we now have a "Big 4" due to the Enron scandal and the demise of Arthur Andersen LLP. The guidance that the courts used to evaluate the issues of this case was the guidance issued by the American Institute of Certified Public Accountants (AICPA). Because the firm held itself and its professionals compliant with AICPA governing standards and guidance, the courts used this guidance as a basis for evaluating the evidence of the case and the firm's professional conduct. Arthur Andersen LLP was the first major international accounting firm taken to court and successfully convicted for a lack of due professional care in the destruction of client documents and obstructing justice. A jury on June 16, 2002, found Arthur Andersen LLP guilty of obstructing justice, all but sealing the fate of this accounting firm.

After a month-and-a-half trial and ten days of deliberations, jurors convicted Andersen of obstructing justice when it destroyed Enron Corp. documents while on notice of a federal investigation. Andersen and its lawyers had claimed that the documents were destroyed as part of its housekeeping duties and not as a ruse to keep Enron documents away from the regulators.

THE SARBANES–OXLEY ACT FORCES ORGANIZATIONS TO IMPLEMENT STRONG INTERNAL CONTROLS

The following reasons are the top four reasons why organizations need to have strong internal controls and the IT auditor role will be to assist in verifying compliance:

1. *The passage of the SEC Sarbanes–Oxley Act of 2002 (Public Law 107-204).* Under this act, companies would be required to include an annual internal control report of management stating the following:
   a. Management's responsibilities for establishing and maintaining adequate internal controls and procedures for financial reporting for the company
   b. Management's conclusions about the effectiveness of the company's internal controls and procedures for financial reporting as of the end of the company's most recent fiscal year

c. That the company's registered public accounting firm has attested to, and reported on, management's evaluation of the company's internal controls and procedures for financial reporting

2. *Inherent security and control risk* issues organizations face within virtual corporate environments and E-commerce business today
3. *Large corporate spending on information technology* has demanded that there be a quantifiable approach to view not only a return on the corporation's investment, but also assurance the products and services the company is paying for are performing and producing as intended. Therefore, it is incumbent upon management to review the effectiveness of these controls. According to IT Almanac.com, information technology spending by commercial organizations is projected to be $831 billion by 2005.
4. The current-day situation of "world terrorism and cyber-crime," and the passage of the Homeland Security Act of 2002 mandates that we as individuals in the corporate sector and in the government arena protect our systems as a sense of national security and pride to ensure the ongoing concern of open and free capital markets within the United States as well as for our allies. Also, the recent release of U.S. "National Strategy for Securing Cyberspace" provides additional guidance and thought to the importance of our information infrastructure. In fact, the supporting report addresses in-depth the critical infrastructures and key assets the United States needs to protect. Both sources are provided in the reference section.

POTENTIAL IMPACT ON THE IT AUDIT PROFESSION

What does this all mean to the IT auditor? Due to the passage of the Sarbanes–Oxley Act, organizations are now required to attest to the effectiveness of their internal controls. With this new regulatory requirement, organizations need the expertise and commitment of IT professional auditors for both internal and external audit functions. To cope with these new legal requirements, IT auditors will, now more than ever before, need to have the appropriate level of expertise and knowledge.

To help companies manage or mitigate business risks against corporate fraud, inefficiencies, ineffectiveness, as well domestic and international cyber-crimes and terrorism, IT auditors with skills, knowledge, and experience will be in high demand to help organizations and government cope with these complexities. One of the better articles on this subject appears in the *Information Systems Control Journal,* which addresses the ramifications of the Sarbanes–Oxley Act authored by my colleague, Professor Tommie Singleton at the University of Northern Alabama (see References).

THE POTENTIAL COSTS OF SUCH IMPLEMENTATIONS

Having said all the above, what is the potential cost of implementing control infrastructures of this magnitude to safeguard corporate assets from corporate fraud, computer crimes, and terrorist attacks?

One of the more difficult issues facing both internal and external auditors is the issue of costs. Once the audit is completed and the key findings and suggestions have been discussed, the topic immediately switches to money. Everyone wants to know how much it is going to cost to safeguard the system.

Everyone also wants to know if they really do need it, or if they can rely on some other forms of compensating controls already in the system to provide the same or similar assurances.

In the end, it is the judgment of management whether or not they want to take the risk of not implementing the changes recommended once they have been provided all the information. If management should decide not to implement suggestions recommended, the liability is on their shoulders, not the auditors, if they have performed at the levels of the professional standards they are required to adhere to during the performance of the audit work.

The questions of costs are excellent questions to pose to auditors recommending system changes or improvements to reduce the various business risks. Therefore, auditors not only have the responsibility of performing their jobs in compliance with the professional standards but must also act with integrity and ethics as well as exercise due professional care (also part of the professional standards) in the performance of their audits if they want to ensure that they have provided all the facts and information necessary for management to rely on and make the appropriate decision in the end. As far as the costs are concerned, that question is still being deliberated because, in the end, when the determination is finally made it will be the consumers and taxpayers who will have pay.

References

A Comparison of Internal Controls; COBIT, SAC, COSO, and SAS 55/78, Colbert, Janet L., Ph.D, CPA, CIA, and Paul L. Bowen, Ph.D, CPA; [on-line]; *Information Systems Control Journal* available at http://www.isaca.org/bkr_cbt3.htm.

American Institute of Certified Public Accounting, IT and the Audit, George H. Tucker, (online); available from http://www.aicpa.org/pubs/jofa/sept2001/tucker.htm.

Carnegie Mellon University, "Everything You Wanted to Know about Internal Auditing," (online); available at http://www.cmu.edu/internal_audit/Q&A.html#FUNCTION.

COBIT 3RD Edition, July 2002, (online); available at http://www.isaca.org/cobit.htm.

Gallegos, Frederick and Ann Carlin, "Best Practices in Due Professional Care: An IT Audit Perspective," submitted to Auerbach June 2003, publication pending.

Gallegos, Frederick, Daniel P. Manson, and Sandra Allen-Senft, *Information Technology Control and Audit*. Auerbach Publications, 1999.

Information Systems Audit and Control Foundation, (online); standards available from http:/www.isaca.org/.

Institute of Internal Auditors, [on-line]; standards available at http://www.theiia.org/iia/index.

National Institute of Standards and Technology, Role Based Access Control, (online); available at http://csrc.nist.gov/publications/nistbul/csl95-12.txt.

"National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," 2002, http://www.whitehouse.gov/pcipb/physical.html.

Proposed Rule: Disclosure Required by Sections 404, 406, and 407 of the Sarbanes–Oxley Act of 2002, Securities and Exchange Commission,17 CFR PARTS 210, 228, 229, 240, 249, 270, and 274, Release Nos. 33-8138; 34-46701; IC-25775; File No. S7-40-02.

RIN 3235-AI66, Disclosure Required by Sections 404, 406, and 407 of the Sarbanes–Oxley Act of 2002; (online); available at http://www.sec.gov/rules/proposed/33-8138.htm.

Sarbanes–Oxley Web site: www.sarbanes-oxley.com.

Sarbanes–Oxley Act (H.R. 6763), Public Law 107-204, http://www.riahome.com/newlaw/full-text.pdf.

Singleton, Tommie, "The Ramifications of Sarbanes–Oxley," *Information Systems Control Journal,* 3, 11–16, 2003.

The Securities Exchange Act of 1934, Section 15A Registered Securities Association, http://www.law.uc.edu/CCL/34Act/sec15A.html.

"The National Strategy for Securing Cyberspace," 2002, http://www.whitehouse.gov/pcipb/.

Frederick Gallegos, CISA, CGFM, CDE, is an adjunct professor and MSBA–Information Systems Audit Advisor for the Computer Information Systems Department, College of Business Administration, California State Polytechnic University, Pomona, California. He has more than 30 years of experience in the information systems audit, control, and security field. He has taught undergraduate and graduate courses in the IS audit, security, and control field and has published widely. He has been active in the Information System Audit and Control Foundation.