Sarbanes-Oxley Act

From Wikipedia, the free encyclopedia.

The **Sarbanes-Oxley Act of 2002**, Pub. L. No. 107-204, 116 Stat. 745 (July 30, 2002), is a United States federal law also known as the **Public Company Accounting Reform and Investor Protection Act of 2002** (and commonly called **SOX** or **SarbOx**).

The Act covers issues such as establishing a public company accounting oversight board, auditor independence, corporate responsibility and enhanced financial disclosure. It was designed to review the dated legislative audit requirements, and is considered one of the most significant changes to United States securities laws since the New Deal in the 1930s. The Act gives additional powers and responsibilities to the U.S. Securities and Exchange Commission.

The Act came in the wake of a series of corporate financial scandals, including those affecting Enron, Tyco International, and WorldCom (now MCI). Named after sponsors Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OH), the Act was approved by the House by a vote of 423-3 and by the Senate 99-0.

History

A brief outline of the history of the law is as follows:

The House passed Representative Oxley's bill (H.R. 3763) on April 25, 2002, by a vote of 334 to 90. The House then referred the "Corporate and Auditing Accountability, Responsibility, and Transparency Act" or "CAARTA" to the Senate Banking Committee with the support of President Bush and the SEC. At the time, however, the Chairman of that Committee, Senator Paul Sarbanes (D-MD), was preparing his own proposal: Senate Bill 2673.

Senator Sarbanes's bill passed the Senate Banking Committee on June 18, 2002, by a vote of seventeen to four. On June 25, 2002, WorldCom revealed that it had overstated its earnings by more than $3.8 billion during the past five quarters, primarily by improperly accounting for its operating costs. Senator Sarbanes introduced Senate Bill 2673 to the full Senate that very same day and it passed ninety-seven to zero less than three weeks later on July 15, 2002.

The House and the Senate formed a Conference Committee to reconcile the differences between Senator Sarbanes's bill (S. 2673) and Representative Oxley's bill (H.R. 3763). The conference committee relied heavily on Senate Bill 2673 and "most changes made by the conference committee strengthened the prescriptions of S. 2673 or added new prescriptions." (John T. Bostelman, The Sarbanes-Oxley Deskbook § 2-31.)

The Committee approved the final conference bill on July 24, 2002 and gave it the name "the Sarbanes-Oxley Act of 2002." The next day, both houses of Congress voted on it without change, producing an overwhelming margin of victory: 423 to 3 in the House and 99 to 0 in the Senate. On July 30, 2002, President George W. Bush signed it into law, stating that it included "the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt." (Elisabeth Bumiller, Bush Signs Bill Aimed at Fraud in Corporations, N.Y. Times, July 31, 2002, at A1.)

Three years after the passing of this law, according to a poll conducted by The Wall Street Journal and Harris Interactive, "55 % of U.S. investors believe that financial and accounting regulations governing publicly held companies are too lenient. That figure rises to 77 % for male investors ages 45 to 54." The results are based on an online survey of 2,061 U.S. adults conducted in early October 2005. According to the survey, only one-quarter of investors feel that SarbOx has made the communication of financial information by companies "much more" or "somewhat more" transparent. What's more, 11 % believe the legislation has actually made communication less transparent.

"41 % say they are not sure about the effect Sarbanes-Oxley has had on communication transparency. This suggests that many investors don't understand the legislation and its impact on businesses."

Provisions

The Sarbanes-Oxley Act's major provisions include:

- Certification of financial reports by chief executive officers and chief financial officers
- Ban on personal loans to any Executive Officer and Director
- Accelerated reporting of trades by insiders
- Prohibition on insider trades during pension fund blackout periods
- Public reporting of CEO and CFO compensation and profits
- Additional disclosure
- Auditor independence, including outright bans on certain types of work and pre-certification by the company's Audit Committee of all other non-audit work
- Criminal and civil penalties for violations of securities law
- Significantly longer jail sentences and larger fines for corporate executives who knowingly and willfully misstate financial statements.
- Prohibition on audit firms providing extra "value-added" services to their clients including actuarial services, legal and extra services (such as consulting) unrelated to their audit work.
- A requirement that publicly traded companies furnish independent annual audit reports on the existence and condition (i.e., reliability) of internal controls as they relate to financial reporting.

Overview of the PCAOB's requirements

(Source: KPMG report)

'Auditing Standard No. 2' of the Public Company Accounting Oversight Board (PCAOB) has the following key requirements:

- The design of controls over relevant assertions related to all significant accounts and disclosures in the financial statements
- Information about how significant transactions are initiated, authorized, supported, processed, and reported
- Enough information about the flow of transactions to identify where material misstatements due to error or fraud could occur
- Controls designed to prevent or detect fraud, including who performs the controls and the regulated segregation of duties
- Controls over the period-end financial reporting process
- Controls over safeguarding of assets
- The results of management's testing and evaluation

Internal controls

Under Sarbanes-Oxley, two separate certification sections came into effect – one civil and the other criminal. *See* 15 U.S.C. § 7241 (Section 302) (civil provision); 18 U.S.C. § 1350 (Section 906) (criminal provision).

Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the [company] and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared." 15 U.S.C. § 7241(a)(4). The officers must "have evaluated the effectiveness of the [company's] internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date." *Id.*

Moreover, under Section 404 of the Act, management is required to produce an "internal control report" as part of each annual Exchange Act report. *See* 15 U.S.C. § 7262. The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." 15 U.S.C. § 7262)a). The report must also "contain an assessment, as of the end of the most recent fiscal year of the [Company], of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." Id. Finally, under both Section 302 and Section 404, Congress directed the SEC to promulgate regulations enforcing these provisions. (See Final Rule: Management's Report on Internal Control

Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Release No. 33-8238 (June 5,2003), available at http://www.sec.gov/rules/final/33-8238.htm.)

"SOX 404 Compliance" has had serious effects on those found to have material weaknesses in internal control. Under the Act companies must, for the first time, provide attestation of internal control assessment. This presents new challenges to businesses, specifically, documentation of control procedures related to information technology.

Additionally, PCAOB has issued guidelines on how management should render their opinion. The main point of these guidelines is that management should use an internal control framework such as COSO (which describes how to assess the control environment, determine control objectives, perform risk assesments, and identify controls and monitor compliance). Companies have almost uniformly elected COSO as the standard when choosing an internal control framework.

Information technology and SOX 404

The PCAOB suggests considering the COSO framework in management/auditor assessment of controls. Auditors have also looked to the IT Governance Institute's "COBIT: Control Objectives of Information and Related Technology" for more appropriate standards of measure. This framework focuses on IT processes while keeping in mind the big picture of COSO's "control activities" and "information and communication". However, certain aspects of COBIT are outside the boundaries of Sarbanes-Oxley regulation.

IT controls, IT audit, and SOX

In today's business environment, the financial reporting processes of most organizations are driven by Information Technology (IT) systems. Few companies manage their data manually and most companies have moved to electronic management of data, documents, and key operational processes. Therefore, it is apparent that IT plays a vital role in internal control. As PCAOB's "Auditing Standard 2" states:

> *"The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."*

Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. Systems such as ERP (Enterprise Resource Planning) are deeply integrated in the initiating, authorizing, processing, and reporting of financial data. As such, they are inextricably linked to the overall financial reporting process and need to be assessed, along with other important process for compliance with Sarbanes-Oxley Act. So, although the Act signals a fundamental change in business operations and financial reporting, and places responsibility in corporate financial reporting on the chief executive officer (CEO) and chief financial officer (CFO),

the chief information officer (CIO) plays a significant role in the signoff of financial statements.

For a detailed discussion on the impact of SOX on IT audit and controls, see Information Technology Controls.

Cost of implementation

There is some debate over the specific requirements of the Sarbanes-Oxley act, as written. The business community has generally acknowledged that, as John A. Thain, CEO of the New York Stock Exchange states, "There is no question that, broadly speaking, Sarbanes-Oxley was necessary" [1]. However, the cost of implementing the new requirements has led some to question how effective or necessary the specific provisions of the law truly are.

One key area of cost is the updating of information systems to comply with the control and reporting requirements. Systems which provide document management, access to financial data, or long-term storage of information must now provide auditing capabilities. In most cases this requires significant changes, or even complete replacement, of existing systems which were designed without the needed level of auditing details.

Costs associated with SOX 404 compliance have proven to be higher than first anticipated. According to the Financial Executives International (FEI), in a survey of 217 companies with average revenue above $5 billion, the cost of compliance was an average of $4.36 million. The survey also indicated actual costs of to be approximately 39% higher than companies expected to spend.[2] The high cost of compliance throughout the first year can be attributed to the sharp increase in hours charged per audit engagement. However, non-compliance comes with an even higher cost in terms of stiffer penalties and jail sentences.

Year One Resources Spent on Section 404 Compliance
Roundtable Survey, December 2004, by Revenue

Company Revenue	**< $5 B**	**$5 B - $10 B**	**$10 B – $50 B**	**> $50 B**
Average Additional Audit Hours	**6,285**	**20,756**	**11,540**	**19,000**
Average Total Compliance Cost (millions)	**$1.9**	**$6.1**	**$20.6**	**$1230.3**

Case studies

Case Studies of Companies with Sarbanes Oxley Certification Delays, Material Weaknesses, Etc. Caused By Information Technology Issues:

- Cray Inc. - numerous material weaknesses in internal control over financial reporting, specifically, inadequate review of third-party contracts and lack of software application controls and documentation

The future of SOX 404 compliance

In a recent article by the accounting and consulting firm of Deloitte Touche Tohmatsu entitled "Under Control", the need for "sustainable compliance" is encouraged. The article suggests leveraging lessons learned to immediately transition into a long-term strategy. The following areas are described as impedances to the process:

1. **"Project mindset:** … many companies understandably treated section 404 compliance as a discrete project with a clearly defined ending point."
2. **"Overextension of internal audit:** If management continues to utilize internal audit for intensive 404 and 302 compliance-related work, then a significant infusion of resources (i.e., budget and headcount) to accommodate the additional workload will be needed."
3. **"Poorly defined roles:** Internal control-related roles and responsibilities, often poorly defined and segregated from the day-to-day routine of employees during the first year, will require greater clarity and integration going forward"
4. **"Improvisational approach:** Another symptom of deadline pressure showed up in the jerrybuilt practices that carried many companies through the first year."
5. **"Underestimation of technology impacts and implications:** …IT is recognized as critical for achieving the goals of the Act, and the impact and implications of technology are widely regarded as significant and pervasive. In many year-one projects, organizations focused heavily on business processes and did not consider the broader role that IT plays in managing financial information and enabling controls… IT will make a huge impact on compliance going forward. At a minimum, technology investments will be necessary to support sustainable compliance in several areas, including repository, work flow, and audit trail functionality. Technology will also be used to enable the integration of financial and internal control monitoring and reporting — a critical requirement at most large and complex enterprises."
6. **"Ignored risks:** Effective internal control is predicated on risk… the controls themselves — exist expressly for the purpose of minimizing the risk of financial reporting errors… In year one, risk assessment was treated as an afterthought — if addressed at all."

The future of SOX 404 will depend on the ability of businesses to respond to the areas noted above by making it a part of every-day business. Deloitte has developed the "Sustained Compliance Solution Framework". Key areas of the framework are also taken from "Under Control":

- Effective and efficient processes for evaluating testing, remediating, monitoring, and reporting on controls
- Integrated financial and internal control processes
- Technology to enable compliance
- Clearly articulated roles and responsibilities and assigned accountability
- Education and training to reinforce the "control environment"
- Adaptability and flexibility to respond to organizational and regulatory change.

Legislative information

- House: 107 H.R. 3763, H. Rept. 107-414, H. Rept. 107-610
- Senate: 107 S. 2673, S. Rept. 107-205
- Law: Pub. L. 107-204, 116 Stat. 745.

Law Review commentaries

"Sarbanes-Oxley §§ 302 & 906: Corporate reform or legislative redundancy? A critical look at the 'new' corporate responsibility for financial reports" by Luke Alverson, 33 Sec. Reg. L.J. 15 (2005)

"Company Liability After the Act Sarbanes-Oxley," by Peri Nielsen & Claudia Main, 18 No. 10 Insights 2 (Oct. 2004)

"Enron--The bankruptcy heard around the world and the international ricochet of Sarbanes-Oxley," by John Paul Lucci, 67 Alb. L. Rev. 211 (2003)

"A Pox on Both Your Houses: Enron, Sarbanes-Oxley and the Debate Concerning the Relative Efficacy of Mandatory Versus Enabling Rules," by Jonathan R. Macey, 81 Wash. U. L.Q. 329, 333 (2003)

"United States v. Simon and the new certification provisions," by Christian J. Mixter, 76 St.John's L.Rev. 699 (2002)