FAQ SERIES #3

THE SARBANES-OXLEY ACT AND RECORD RETENTION

William Saffady

INTRODUCTION

Since its passage in 2002, the Sarbanes-Oxley Act (SOX) and its associated rules and regulations have been the subject of many presentations and publications that emphasize its importance for information governance, records management, and allied disciplines. SOX recordkeeping requirements have been widely discussed, but they are not always accurately presented. In particular, SOX record retention requirements are often overstated, and the entities to which they are apply are not clearly articulated.

This report is intended for records managers, information governance specialists, compliance officers, risk managers, legal counsel, information technology specialists, and others who are responsible for SOX compliance. The report answers frequently asked questions about SOX provisions that specify recordkeeping requirements or that have implications for development of a company's record retention policies, procedures, and schedules.

1. Which organizations are subject to SOX recordkeeping requirements?

The Sarbanes-Oxley Act applies to the following entities:

- Public companies—Companies that issue stocks, bonds, notes, or other securities for sale to the public on stock exchanges or in the over the counter market, including foreign companies that are listed on U.S. stock exchanges. The Sarbanes-Oxley Act adopts definitions presented in Section 3 of the Securities Exchange Act of 1934, which refers to public companies as "issuers."

- Registered investment companies—Investment companies that are registered with the Securities and Exchange Commission (SEC) under the Investment Company Act of 1940 and that register its public offerings under the Securities Act of 1933.

- Public accounting firms—Accounting firms that are registered with the Public Company Accounting Oversight Board (PCAOB) to provide accounting and auditing services to public companies and registered investment companies. The Sarbanes-Oxley Act applies to proprietors, partners, shareholders, or other professional employees of public accounting firms as well as to independent contractors or other entities that act as agents of such firms.

2. Do any recordkeeping provisions of the Sarbanes-Oxley Act apply to other organizations?

With one exception, recordkeeping provisions of the Sarbanes-Oxley Act do not apply to privately held companies, to partnerships other than public accounting firms, to

government agencies, or to not-for-profit organizations such as educational institutions, cultural institutions, scientific and research organizations, professional associations, religious groups, and philanthropic organizations. The exception relates to Section 802 of the Act, which amended Title 18, Section 1519 of the U.S. Code 1519 to impose criminal penalties for destroying, concealing, modifying, or falsifying records with the intent to obstruct a government investigation or bankruptcy proceeding. That provision applies to all organizations. Similar provisions are found in Section 1102 of the Act.

3. Which sections of SOX are relevant for record retention?

Recordkeeping requirements are directly addressed in the following section:

- Title III, Section 301(m)(4)(A), which deals with complaint records.
- Title III, Section 302(a), which specifies signing requirements for periodic reports submitted to the SEC by public companies.
- Title IV, Section 403, which deals with certain information that must be posted on a company's web site.
- Title VIII, Section 802, which deals with retention of audit records and prohibits the destruction, alternation, or concealment of records.
- Title XI, Section 1102, which deals with destruction, alteration or concealment of records.

Title IV, Section 404 does not deal with record retention directly, but it has implications for an organization's information governance and records management initiatives.

The following portions of the Sarbanes-Oxley Act do not deal with recordkeeping requirements or issues, either directly or by implication, and are not relevant for the development of record retention policies, procedures, or schedules:

- Title I – All Sections
- Title II – All Sections
- Title III – Sections 303 through 308
- Title IV – Sections 401, 402, 405, 406, 407, 408 409
- Title V – All Sections
- Title VI – All Sections
- Title VII – All Sections
- Title VIII – Sections 801, 803, 804, 805, 806, 807
- Title IX – Sections 901 through 905
- Title X – All Sections
- Title XI – Sections 1101, 1103, 1104, 1005, 1106, 1107

4. What are the SOX retention requirements for complaint records?

According to Title III, Section 301(4) of the Sarbanes-Oxley Act, a public company's audit committee must establish procedures for "(A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." The same requirement is specified in 17 CFR 240.10A-3. Retention periods are not specified for complaint records, but a public company must designate a retention procedure for them. According to the SEC Final Rule on Standards Related to Listed Company Audit Committees (68 FR 18788), self-regulatory organizations are prohibited from listing the securities of a company that fails to comply with this requirement.

5. What are the SOX retention requirements for signature pages?

According to Title III, Section 302(a) of the Sarbanes-Oxley Act, the company's signing officers must certify that quarterly and annual reports filed with the Securities and Exchange Commission "fairly present" the company's financial condition and results of operations for the indicated period. Further, signing officers must establish and maintain internal controls to ensure that they are aware of "material information" relating to the company and its subsidiaries during the periods covered by the reports. Signing officers must also disclose to the company's auditors and audit committee all significant deficiencies "which could adversely affect the issuer's ability to record, process, summarize and report financial data."

Retention requirements associated with this provision are specified in federal regulations rather than in the Sarbanes-Oxley Act itself. According to 17 CFR 232.302(b), each signing officer must execute a manual signature page for an electronic filing of a periodic report. This manual signature page, which acknowledges the signature that appears in typed form within an electronic filing, must be retained for 5 years. This is a general SEC requirement for signatures associated with electronic filings. It is not unique to the Sarbanes-Oxley Act.

6. What are the SOX retention requirements for web site content?

This requirement has a narrowly defined scope. Title IV, Section 403 of the Sarbanes-Oxley Act modified Section 16 of the Securities Exchange Act to require disclosure of certain ownership changes, which must be posted on a public company's web site by the end of the next business day after the changes occur. As specified in 17 CFR 240.16a-3(k), SEC Form 3—Initial Statement of Beneficial Ownership of Securities, SEC Form 4—Statement of Changes in Beneficial Ownership, and SEC Form 5—Annual Statement of Changes in Beneficial Ownership of Securities must remain accessible on the company's web site for a minimum of 12 months.

7. What are the SOX retention requirements for Audit Records?

Title VIII, Section 802(a) of the Sarbanes-Oxley Act amended Title 18, Section 1519 of the U.S. Code. It specified a retention period of 5 years from the end of the pertinent fiscal year for certain records maintained by public accounting firms that audit or review the financial statements of public companies and registered investment companies. The records to be retained include work papers and other documents that form the basis of the audit, as well as memoranda, correspondence, communications, and other records (including electronic records) that are created sent or received in connection with the audit and that contain conclusions, opinions, analysis, or financial data related to the audit. Section 802(a) further specifies that intentional destruction, alteration, concealment, or falsification of records that are relevant for federal investigations or bankruptcy cases is a crime punishable by a fine and/or imprisonment. Section 1102 contains similar provisions.

17 CFR 210.2-06 increased the retention period for a public accounting firm's audit and review records to 7 years from conclusion of the audit or review. This retention period is consistent with retention requirements specified by the Public Company Accounting Review Board in Auditing Standard No. 3.

As specified in SEC Final Rule on Retention of Records Relevant to Audits and Reviews (68 FR 4862), the 7-year retention requirement applies to records listed in Section 802(a) of the Sarbanes-Oxley Act. The requirement also applies to records that document a consultation or resolution of differences in professional judgment as well as records that do not support the auditor's final conclusions.

The retention requirement does not encompass all financial information, reports, databases, and other records that a public accounting firm received from the public company being audited but that were not made part of the auditor's work papers. The retention requirement does not apply to administrative records or documents that lack significant content, such as superseded drafts, notes that reflect incomplete or preliminary thinking about an audit, previous copies of work papers that have been corrected for typographic errors, or duplicate records. 17 CFR 210.2-06 states that the significance of a record is determined by "objective analysis of the facts and circumstances."

8. Does the 7-year retention requirement apply to financial records maintained by the public company being audited?

No. The 7-year retention requirement only applies to public accounting firms. It does not apply to financial records maintained by the public companies or registered investment companies being audited. Public companies and registered investment companies may retain their financial records for 7 years or longer, but the Sarbanes-Oxley Act does not apply to those records.

9. Does Section 404 of SOX specify retention requirements for financial records?

No. Section 404 of the Act and its associated SEC rules and regulations deal with internal controls and financial reporting. According to Section 404(a)(2), a public company's annual reports must include management's assessment of the effectiveness of the company's internal control structure for financial reporting. Management must evaluate whether the company's internal controls provide reasonable assurance that a public company's financial statements accurately and fairly represent the company's financial condition in accordance with generally accepted accounting principles. Section 404(b)of the Act requires the company's public accountants to attest to and report on the assessment.

According to the SEC Final Rule on Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (Release No. 34-47986), a public company "must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the company's internal control over financial reporting," but no specific recordkeeping practices or retention periods are prescribed. In Commission Guidance Regarding Management's Report on Internal Controls Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934 (Release Nos. 33-8810 and 34-55929), the SEC states that management should have "flexibility as to the nature and extent of the documentation it maintains to supports its assessment."

10. How does Section 404(a) relate to record retention?

Reliable recordkeeping systems are a precondition for compliance with Section 404(a). In particular, a company must have policies, procedures, and practices to ensure that information related to its financial condition is retained for as long as necessary and protected from inadvertent damage or destruction during that time. This requirement did not originate with the Sarbanes-Oxley Act. Section 13(B)(2)(A) of the Securities Exchange Act requires public companies to "make and keep books, records and accounts which in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." In Administrative Proceeding File No. 3-10789, the SEC stated that such books and records include memoranda and internal corporate reports as well as accounting records.

While SEC rules and regulations do not define standards for the effectiveness of a company's internal controls over financial reporting, they suggest that the Internal Control—Integrated Framework, which was issued in 1992 and updated in 2013 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, is an acceptable basis for implementing and assessing internal controls. COSO's sponsoring organizations are the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants. Among its objectives, the COSO framework is designed to ensure accurate financial reporting and compliance with laws and

regulations. According to the COSO framework, internal controls consist of five interrelated components: (1) a control environment that sets the tone for an organization, (2) risk assessment to identify and evaluate risks from external and internal sources, (3) policies and procedures to ensure that management directives are carried out, (4) systems to capture and communicate information, and (5) ongoing monitoring for compliance. Assessment of a company's internal controls must consider all five of these criteria.

A systematic record retention program is fully compatible with and supportive of the COSO framework. Systematic record retention is an important internal control activity. By ensuring that recorded information will be controlled by directives rather than discretion, a systematic record retention program supports a control environment. Risk assessment is an integral facet of initiatives for the retention and preservation of recorded information. A systematic record retention program is driven by policies and procedures that specify how long information must be kept to satisfy a company's legal and operational requirements. A systematic record retention program includes procedures for the retrieval and distribution of information needed for specific purposes and for ongoing compliance monitoring.

ABOUT THE AUTHOR

William Saffady is a records and information management consultant and researcher based in New York City. He is the author of over three-dozen books and many articles on records management, record retention, information governance, document storage and retrieval technologies, and other information management topics. He recently completed the third edition of *Records and Information Management: Fundamentals of Professional Practice,* the most widely used textbook on records management. Other recent books include *Legal Requirements for Electronic Records Retention in Western Europe* and *Legal Requirements for Electronic Records Retention in Eastern Europe*, both published by ARMA International in 2014; *Legal Requirements for Electronic Records Retention in Asia*, which was published by ARMA International in 2015; *Email Retention and Archiving: Issues and Guidance for Compliance and Discovery*, which was published by ARMA International in 2013; and *Cost Analysis Concepts and Methods for Records Management Projects, Second Edition*, which was published by ARMA International in 2011.

Since 1976, Dr. Saffady has served as an information management consultant, providing analytical services and training, to companies, government agencies, not- for-profit entities, cultural institutions, and other organizations. These projects have involved the development of strategic plans and governance models for records management programs, needs assessments and gap analysis, the development of record retention policies and schedules, and the preparation of technical specifications for procurement of records management products and services.

For more information, go to www.saffady.com or email wsaffady@saffady.com.