Iron Mountain
The Leader in Records & Information Management

THE FOUR PILLARS OF RESPONSIBLE RECORDS MANAGEMENT UNDER THE SARBANES-OXLEY ACT

Stringent Mandates and Penalties Present Challenges and Opportunities

"THE PERFECT STORM"

In the past 18-24 months, a storm of issues and events has created a crisis in corporate credibility. For virtually all business stakeholders — executives, auditors, attorneys, and especially, shareholders — it has been "the perfect storm" unfolding in the media in a high-profile manner. Improper accounting practices. Off-balance-sheet transactions. Conflicts of interest. Insider trading. The business world has witnessed billion-dollar bankruptcies and the erosion of confidence among investors, who now cast a wary eye on the results and disclosures of even the largest companies in the world.

Now, more than ever before, the corporate world is placing a resounding and proper emphasis on ethical practices as businesses endure greater scrutiny.

SARBANES-OXLEY: THE NEW ENVIRONMENT FOR RESTORING CORPORATE CONFIDENCE

One of the most significant and recent initiatives to reform corporate governance and accounting since the Securities Act of 1933 and the Securities and Exchange Act of 1934 is the Sarbanes-Oxley Act of 2002. Signed by President Bush in July 2002, this law prescribes a sweeping system of additional federal oversight covering corporate governance and financial practices for U.S. and non-U.S. companies that have issued securities in U.S. public markets and that file periodic reports with the Securities and Exchange Commission, as well as their auditors, boards of directors, and lawyers.

As a result, records management is expanding from an important business process into a critical compliance issue as well.

The Act implements a new set of auditor independence rules, new top officer certification requirements, and new disclosure requirements for companies and their insiders, coupled with harsh civil and criminal penalties for people responsible for accounting or reporting violations. Not surprisingly, given the many high-profile incidents of records mismanagement, one of the major areas receiving attention from lawmakers creating the Act is how companies manage, retain, and destroy their business records. And for good reason. Operating in consistent accordance with a proper records management program minimizes the possibility that companies' record-keeping practices will be portrayed as arbitrary or capricious.

The implications of Sarbanes-Oxley for records management are expected to be enormous. As a result, records management is expanding from an important business process into a critical compliance issue as well. Although the regulations have yet to be fully implemented, the clear intent is to hold companies accountable, and will most likely underscore the need for comprehensive retention and destruction policies for all types of documents and records generated by all participants in the corporate governance and auditing process. Regulations are being issued at a rapid pace and will continue to take shape as they emerge from a lengthy regulatory process. Some of the important precepts of Sarbanes-Oxley are listed below.

- Public Company Accounting Oversight Board: This Board will provide the SEC with the authority to issue rules and to set standards. Public accounting firms must register with the Board, which will perform quality inspections, investigations, and disciplinary proceedings. This Board can suspend or bar individuals from a firm or suspend or revoke a firm's registration.
- Auditor Independence: Sarbanes-Oxley prohibits a firm from providing both auditing and many non-auditing services to the same client. Certain audit partners must rotate after a five-year period. A mandatory rotation of auditing firms is also being studied.
- Corporate Responsibility: Under Sarbanes-Oxley, audit committee members of publicly traded companies cannot accept consulting or advisory fees. Audit committees must establish whistleblower procedures for accounting matters and confidential, anonymous submission of concerns. CEOs and CFOs must certify quarterly and annual reports and implement/evaluate internal controls. In addition, personal loans to executives are prohibited.

- **Enhanced Disclosures:** Public companies must disclose off-balance-sheet transactions. They must also include in annual reports an "internal control report" that documents its internal control structures and procedures for financial reporting and assesses the effectiveness of these measures.

Sarbanes-Oxley does not specify the exact internal control processes necessary to address records management. In fact, many specific provisions regarding records management compliance are still being developed. However, we believe that management will be held accountable for records management as part of their overall internal control process. Public accounting firms are preparing to begin formally auditing records management controls, which will lead to a mandate for a comprehensive approach to managing paper and electronic records.

OTHER REGULATIONS AFFECTING RECORDS MANAGEMENT

Gramm-Leach-Bliley Act of 1999

This law establishes federal rules on the disclosure of personal financial information by financial institutions. This carries enormous implications for records management disciplines with respect to retention and destruction of customer records and files.

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act (HIPAA) was enacted into law on August 21, 1996. Among other things, it contains many requirements related to the privacy and security of patients' health information. The Privacy Rules became effective on April 14, 2001. Most "covered entities" must comply with the rules by April 14, 2003. The Security Rules have not yet been published in final format. HIPAA creates significant compliance challenges for all participants in the healthcare industry, governing the way records are stored, for how long, and the manner and timeframe in which they are destroyed.

SEC Rule 17a-4

In 1997, the SEC amended paragraph (f) of Rule 17a-4 to enable broker-dealers to store records electronically (e.g., on optical disk or magnetic tape). The rule change carries significant requirements for companies choosing this option, covering everything from the media used to store records, how the media is stored, and how records are indexed and retrieved.

RECORDS MANAGEMENT IMPLICATIONS

Sarbanes-Oxley also sets forth specific regulations for managing business records, particularly those that pertain to the auditing process.

One important aspect concerns "audit work papers." The Act requires public accounting firms to retain for seven years all audit work papers and information related to any audit report that support those conclusions and reports. This is a very broad definition that encompasses paper and electronic records that are created in connection with an audit and that contain conclusions, opinions, analyses, or financial data. Even documents that contain information related to a significant matter but are inconsistent with the audit conclusions must be retained. The implication of this requirement is that public accounting firms will require rigorous records management programs with legally credible retention schedules. More broadly, corporations will also need these same records management programs to manage their paper and electronic records.

The Act requires that audit reports contain an evaluation of whether or not proper internal controls are in place, including "maintenance of records that in reasonable detail accurately reflect the transactions." As a result, public accounting firms, internal auditors, and company executives will be extending their auditing processes beyond opinions of financial statements to actually auditing a public company's records management programs to assess their effectiveness and controls.

Perhaps most important are the penalties prescribed by Sarbanes-Oxley in the event of innapropriate destruction of business records. For willful destruction of corporate audit records, the punishment can include imprisonment of up to 10 years. Destroying or altering records to impede a federal investigation or bankruptcy case, tampering with records, or impeding an investigation are all punishable by prison terms of up to 20 years. The likely outcome of these new penalties is that companies will formalize their procedures to appropriately suspend records destruction in anticipation of litigation as a protective measure, therefore raising the bar on the scope of records management procedures and controls.

For willful destruction of corporate audit records, the punishment can include imprisonment of up to 10 years.

THE FOUR PILLARS OF SARBANES-OXLEY RECORDS MANAGEMENT

Faced with these daunting requirements for records management and compliance with Sarbanes-Oxley, many companies are struggling to define the precise characteristics of an appropriate records management program. The following records management "pillars" are Iron Mountain's recommended best practices for complying with the records management provisions of Sarbanes-Oxley. The pillars provide the demonstration of good faith, prudence, and care in retaining records that courts and regulators look for in judicial or other proceedings. It is also important to remember that courts are not seeking a standard of perfection. Rather, they want companies to demonstrate good-faith efforts to properly care for and preserve records in a consistent and fair manner.

Pillar One: Consistency

The most prominent and important hallmark of a legally credible records management program is consistency. However, most companies' records management programs are fragmented, with various business units operating under their own separate policies, archiving rules, and processes. Digital records and paper records are usually treated differently within companies, though legally considered the same. Stand-alone digital record-keeping systems (managed as ordinary data, but really containing business records), and multiple records management vendors combine to make it nearly impossible to implement a consistent program. The external image portrayed is internal inconsistency and randomness.

Companies seeking to comply with Sarbanes-Oxley need consistency because it gives context to recordkeeping actions as ordinary practices, evidencing good-faith efforts.

Companies seeking to comply with Sarbanes-Oxley need consistency because it gives context to recordkeeping actions as ordinary practices, evidencing good-faith efforts. Consistency can take many forms, but primarily it relates to the design and implementation of records retention and destruction policies across media types, geography and business units. Consistency also matters in areas of information privacy, policies, and procedures.

Companies that wish to demonstrate good-faith compliance with Sarbanes-Oxley should be prepared to produce a single set of documented policies and procedures governing the retention and destruction of their business records. And they should implement common systems to govern the chain of custody for those records and to execute those policies.

One of the best ways to achieve consistency is to establish standard, company-wide policies to govern records management efforts. This helps ensure that similar records are treated in a similar manner, which is one of the important tests of a legally credible records management program.

Consistency in records management also means performing the same sets of processes and procedures repeatedly and without exception. For example, your company will want to have a systematic way to issue, review, and release so-called "litigation holds" for records needed in pending legal actions or administrative proceedings. This provides an audit trail of the chain of custody for any and all records in contention and avoids indefensible "he-said/she-said" scenarios.

Best practices call for companies to make a significant organizational commitment to records management.

Pillar Two: Accountability

Accountability is an essential, but often missing, characteristic of most companies' records management initiatives. Studies from ARMA International, a leading information management industry organization, show that records management typically reports to a business service or administrative area where it is treated as a non-strategic support function. Senior stakeholders for records management, namely legal, IT and compliance, tend to be underrepresented in determining policies and controls. Internal audit processes often ignore records management. Local accountability for policy implementation at the business unit or department level is not formalized or does not exist.

The standard of reasonableness also requires companies to carefully oversee the ongoing execution of their records management program. Accountability is measured in several ways:

- Organization: Best practices call for companies to make a significant organizational commitment to records management. Leadership should take the form of a steering committee with a compliance officer and risk-management stakeholders from legal, IT, and finance. There must be a designated corporate records manager to administer the program. Program liaisons between the corporate program and the end user in business units and/or departments should be established. This multi-level approach facilitates accountability throughout the organization.
- Certification: An important demonstration of good faith in records management requires that employees acknowledge receipt and review of the records management policies. Administering and documenting a certification program demonstrates a company's diligence in managing its records management program.
- Appropriate Metrics: It is best to carefully track key measures and performance indicators relating to the consistent retention and destruction of paper and electronic records. Records destruction should be timely, consistent, and performed in the ordinary course of business. From a management perspective, accountability means regular periodic reviews of policies and procedures and complete audits and reports.

It is incumbent upon the organization to bring its records management policy to life, to "operationalize" it and ensure it is adopted as an ongoing element of standard business processes, as a compliance program.

Pillar Three: Adoption

Unfortunately, for many companies, records management is a discipline that starts — and ends — with little more than a carefully worded memo from the legal department. Many employees are oblivious to their company's records management expectations of them. Employees do not understand the significance of records management, nor are they trained in basic procedures. Self-help information and tools are neither current nor readily available. In short, records management is not a recognized company program.

It is incumbent upon the organization to bring it records management policy to life, to "operationalize" it, and ensure it is adopted as an ongoing element of standard business processes, as a compliance program. A company must sufficiently demonstrate that it continually makes a diligent effort to identify the type of records that it creates in the normal course of business. It must show a good-faith effort to identify all statutory and regulatory requirements for records retention in all of the jurisdictions in which it conducts business. And a company must be able to document the process by which the retention schedule was approved and implemented. Finally, the company must be able to demonstrate efforts to periodically review the retention policy, update it to reflect changes in the law, and roll it out to all personnel.

Simply creating a records management policy is not sufficient to shield a company from accusations of neglect or fraud. Instead, the company must create a true multi-faceted records management program that involves:

- Rollout and Training: Proper records management program deployment requires a formal program with meetings, training, and reference materials. These initiatives educate all participants about the policies and tools, and provide well-defined, formalized responsibilities throughout the organization.
- Communication: This might include incorporating records management topics in new-employee orientations, creating a records management section on the company intranet, or publishing a periodic internal newsletter on records management topics.
- Reporting and Review: To ensure compliance and foster continuous improvement, the program must have comprehensive reports that can be audited.

Implemented properly, the records management process is inculcated throughout the organization and becomes second nature for users, like filling out an expense report.

Pillar Four: Accessibility

Companies struggle to access information from the organizational and technology silos they have amassed over time and through acquisitions. Their archiving systems tend to feature person-specific filing methods and inadequate searching tools that impede information access. In legal settings, information is requested by content, regardless of the media format or system issues; yet companies don't maintain information in that fashion. Electronic records are often stored in the system creating the information, resulting in a sea of archives. Responsible companies need to demonstrate good faith by efficiently responding to information requests during an audit or litigation.

A company can improve its access to archived information by focusing on two important areas: consolidating the records management systems and establishing standard identification conventions.

The best approach to achieve optimal records management accessibility lies in creating a single, consolidated, easily accessible system for all records in all media. Unfortunately, it is neither feasible nor economical to create a universally accessible single archive for all media. However, it is feasible — and desirable — to create a universal view of multiple mixed-media archives or create a universal archive of all paper records.

With electronic records volumes growing upwards of 100% per year, companies must focus on those electronic records with evidentiary or compliance importance. These records can be more effectively managed in a single archive using policies similar to those applied to paper records. They might include, for example, e-mail, customer statements, and communications.

The success of a records management program often hinges on the ability to retrieve information for either business support, litigation response or compliance reasons. Courts are generally unsympathetic to a company's excuses about the difficulties of obtaining information because of technology problems or excessive workload. Federal Rule 26 of Civil Procedure explicitly requires that defendants affirmatively turnover "relevant" discovery information early in the litigation process.

Implementing a common identification approach will ensure that records are described well enough to be retrieved, even years later. Companies should consider their retrieval needs and create common and logical indexing procedures with an eye towards accessibility.

A company can improve its access to archived information by focusing on two important areas: consolidating the records management systems and establishing standard identification conventions.

Summary

Sarbanes-Oxley has called attention to what companies should have been doing all along as prudent business practices. CEOs and boards of directors now have no practical choice but to implement compliance-grade records management programs. Management will find that investing in the four pillars of records management (Consistency, Accountability, Adoption and Accessibility) will not only support their compliance obligations, but will also help them better manage their information assets. In the end, companies will reduce their costs and risks, and have more control over their information.

For more information on best-practices records management programs and Sarbanes-Oxley compliance, contact Iron Mountain.

SARBANES-OXLEY AT A GlANCE

The Sarbanes-Oxley Act, signed into law on July 30, 2002, implements changes in federal securities regulation, corporate governance, and the regulation of auditors.

Who it directly affects:

- Registered public accounting firms
- Publicly traded companies
- Companies in the process of registering securities under the Securities Act of 1933

Who it indirectly affects:

- Private companies that may go public in the future
- Private companies that may be acquired by public companies
- Private companies in states considering adopting parallel legislation

Key Provisions:

- Establishment of Oversight Board: Establishes a Public Company Accounting Oversight Board and provides the SEC with the authority to issue rules, set standards, and provide oversight and enforcement over the Board.
- Registration of Public Accounting Firms: Requires all public accounting firms that wish to perform auditing functions for publicly traded companies to register with the Board. The Act also defines the scope of audit practice and reports, details investigations and disciplinary proceedings provisions, and defines conflict-of-interest prohibitions.
- Restrictions for Publicly Traded Companies: Prohibits or restricts numerous behaviors regarding insider trades, loans to officers and directors, disclosure of information, and/or improper influence on audits. It also requires a reporting company to disclose whether it has at least one financial expert on its audit committee and whether it has adopted a code of ethics for the CEO, CFO, and principal accounting officer. Companies must disclose off-balance-sheet transactions, stock transactions, finance-related procedures, and other matters in a timely manner.
- Auditing: All Audit Committee members must be independent and free of consulting, advisory, or other compensatory engagements with the company. Auditors report directly to an Audit Committee and are restricted in the non-auditing services they can provide. Audit whistleblowers receive added protection. Auditing firms must retain work papers for seven years and lead and concurring audit partners must rotate every five years.
- Certification by Officers: Imposes increased responsibility for financial reports on the CEO and CFO, requiring that they certify as to the fair presentation of results of operations and financial condition and other matters. Public companies must include certifications by the CEO and CFO that disclosure controls and procedures and internal control systems are functioning properly to provide accurate results of operations and statements of financial condition. Officers must certify any significant changes in internal controls that were adopted or other factors that could significantly affect internal controls, and that they have reported to the Audit Committee and the company's outsider auditors any fraud committed by management or other personnel who have a significant role in the company's internal controls.
- Crimes and Penalties: Establishes new crimes and increases the maximum penalties for certain existing crimes.
  - It is a crime, punishable by imprisonment of up to 10 years, to knowingly and willfully violate new provisions regarding retention of corporate audit records. Requires accountants to maintain all audit and review work papers for five years from the end of the applicable fiscal period. The SEC increased the retention period to seven years.
  - It is a crime, punishable by imprisonment of up to 20 years, to knowingly alter, destroy, or conceal records or documents with the intent to impede, obstruct, or influence a federal government investigation or case filed in bankruptcy, or in relation to or contemplation of any such matter or case; to impair their integrity or availability in an official proceeding; or to otherwise obstruct, influence, or impede a proceeding.
  - Maximum penalties are increased for wire and mail fraud (from five to 20 years), violating ERISA (from one to 10 years), and violating the Securities Exchange Act of 1934 (from 10 to 20 years). The same maximum penalties are now available for an attempt or conspiracy to commit any of the crimes addressed in the Act as for the completed offense.