

EMC Software and the Sarbanes-Oxley Act

What is Sarbanes-Oxley and what does it mean to be compliant to this standard?

How can EMC software help keep you in compliance?

Our opportunity to serve publicly traded companies is multifold. EMC software:

- Provides validatable document and e-mail management for public firms of all sizes
- Provides long-term data retention to protect accounting and financial data and ensure its ready retrieval throughout its lifecycle
- Provides enterprise backup, replication, and restore capabilities to protect accounting and other financial data
- Ensures availability of applications and business-critical data
- Enables full auditing and reporting to ensure appropriate rules of evidence are adhered to
- Provides a complete information lifecycle management approach for compliance with technical controls outlined in the Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) of 2002, overseen by the U.S. Securities and Exchange Commission (SEC), implements safeguards against accounting errors and fraudulent management practices. This legislation was drafted and passed in direct response to corporate accounting scandals in 2001 and 2002, and it is intended to protect the public from unscrupulous actions by public companies and their accounting firms.

SOX applies to publicly traded firms that are listed on any U.S.-based financial exchange, as well as private companies planning on going public or being acquired by a public company. The first phase calls for significant checkpoints to ensure independence of board members and audit committees, and requires senior management certification of financial results. This effectively holds CEOs and CFOs personally responsible for misrepresentation of company performance.

At first glance, SOX looks like a finance or accounting issue. While it is financial legislation, the rules are all about ensuring internal controls to manage creation of information in financial statements. This changes the nature of what is considered financial information, since many aspects of a company's business operations might influence the financial outcome. IT systems are used to create, house, and transport financial data, and CIOs have to ensure that information can hold up to audit scrutiny. A solution must provide an audit trail that shows where data came from, to whom it went, and who approves its accuracy. Thus SOX impacts many systems and processes, such as finance, sales, and order management, as well as the documents that support them. A SOX solution must help manage both documents and data. In addition, since e-mail is the number one method of business communication, it is critical to efficiently capture, retain, and ensure authenticity of e-mail communications according to rules of evidence.

Document and information preservation takes center stage during the compliance process. Ensuring that documents and reports that support financial information and accounting processes are readily accessible is critical. E-mail and instant messages (IM) are more difficult to manage in terms of internal recordkeeping controls, complicating compliance. To combat this, companies are creating records management plans that require e-mail and document retention by value and relevancy of information, not format.

Industry experts remind companies that SOX compliance is not just an event, but rather a process. The SEC is expected to continue interpreting the Act and issuing new rules defining what will be required. Recently, SOX was amended to make records-based obstruction of justice and tampering provisions applicable to both private and public companies. Many experts also expect private companies to follow the spirit and letter of the law.

Potential IT implications of Sarbanes-Oxley

Unless noted, the following requirements are currently in effect.

Section 103	You and/or your auditor must maintain all audit-related records, including electronic ones, for up to seven years.
Section 201	Firms that audit a company's books can no longer also provide IT-related services.
Section 301	Systems or procedures must be provided for whistleblowers to communicate confidentially with the audit committee. (No effective date set.)
Section 302	The CEO and CFO are required to sign statements which verify the accuracy and completeness of financial reports.
Section 404	CEOs, CFOs, and outside auditors need to attest to the effectiveness of internal controls for financial reporting and that the information contained in any SEC filing is accurate. (Effective June 15, 2004 for most large U.S. businesses; smaller businesses have until April 15, 2005.)
Section 409	Companies will need to report material changes in their financial conditions "on a current basis." The act calls for realtime reporting of events, though it doesn't define this. (No effective date set.)

This is not a complete listing of all requirements under the Act, but is provided to illustrate the scope and nature of the regulation. Organizations should consult with their own legal and compliance experts to determine what they must do to comply. Non-compliance presents a significant risk, with fines ranging into the millions of dollars, as well as potential criminal penalties.

EMC's approach helps organizations address compliance with these regulations in a framework of information protection, automated availability, and content and messaging management solutions.

How does EMC software address compliance from a business requirements perspective?

EMC offers software products that address multiple aspects of SOX. Our content and messaging management solutions primarily address those sections related to collecting and accessing electronic records, as well as securing them from unauthorized access and providing audit trails of all system activity. Types of records that can be managed include:

- Reports and computer output
 - Account records and maintenance
 - E-mail, including attachments and instant messages
 - Statements
 - Notices
 - Communications
 - Interoffice memos
 - Customer correspondence
-

Our information protection solutions provide long-term archiving of records, along with backup and rapid recovery to ensure the highest-degrees of information protection. Our automated availability products ensure that the various systems on which the organization depends continue to operate at peak performance, while ensuring virtually instantaneous recovery in the event of disaster for critical systems.

The EMC® Documentum® ApplicationXtender® suite helps you comply with SOX with respect to maintaining required documents and reports, as well as controlling and tracking authorized access to business content. ApplicationXtender can be easily integrated with virtually any business application, including your ERP or accounting system, to provide access to supporting documents and reports directly from your line-of-business applications. ApplicationXtender can also be used to automate business procedures and processes, providing a greater level of control over transactions, as well as improving workplace productivity and operational efficiency.

EMC EmailXtender® provides realtime collection of e-mail messages and attachments including IM. These messages are then fully indexed and secured in the e-mail archive system. The solution delivers comprehensive search and retrieval and audit functionality for messaging systems such as Microsoft Exchange, Lotus Notes/Domino, Bloomberg Mail, and UNIX Sendmail, as well as instant messaging.

Both ApplicationXtender and EmailXtender are seamlessly integrated with EMC DiskXtender® to ensure that relevant information is retained for as long as is required by SOX. DiskXtender provides long-term archiving for database information, so that specific financial transactions can be easily located should the need arise—even if those transactions are several years old.

How does EMC software address SOX from a technical requirements perspective?

EMC software can address requirements of Sarbanes-Oxley through:

- **Capturing information:** ApplicationXtender works hand-in-hand with virtually all business applications to capture a full complement of electronic business content, including documents, reports, images, video, audio, and much more. EmailXtender automatically collects and organizes e-mails, including attachments and instant messages.
 - **Search and retrieval:** Both ApplicationXtender and EmailXtender offer flexible search and retrieval as part of their core functionality. In both cases, users can (according to their security privileges) search the repository for relevant information using simple or complex terms. This capability ensures rapid retrieval of relevant information, which can be displayed on screen, printed, e-mailed, or otherwise collected for review by an internal or outside party. Both systems also offer secure, browser-based access, which could enable an authorized user from an outside party to search and retrieve information for review.
 - **Regulatory review:** Both ApplicationXtender and EmailXtender offer functionality to distribute content to third parties on CD or other forms of removable media. The results of a search within ApplicationXtender or EmailXtender can be output, along with a search and viewing utility. Should a regulator want to review a set of documents or other materials related to a particular topic, the company could quickly produce a CD-ROM containing all the relevant information and make it available to the regulator for review at his or her convenience.
 - **Integration with financial systems:** ApplicationXtender provides access to your financial systems and data through application bridges. This integrates data generation, management, and access into a single comprehensive solution to improve productivity.
-

-
- **Long-term data retention:** SOX requirements for retention of electronic records or other data are specific. For example, accounting firms must retain audit records and work product for a minimum of five years. Standard DiskXtender functionality, implemented as the storage and archival component for ApplicationXtender and EmailXtender, meets these requirements fully. DiskXtender on its own can provide long-term archival of virtually any type of data file for a wide variety of applications. DiskXtender works by migrating data off primary servers onto alternate storage media. In addition, DiskXtender provides quick, transparent access to archived data for users and applications—without intervention from IT personnel. DiskXtender enables the company to use a wide variety of storage media for archiving, depending on their budget constraints, retrieval time objectives, data volume, etc.
 - **Security:** The ApplicationXtender suite offers multiple levels of security, including encrypted connections for both network and web-based user session initiations. Where appropriate, the use of secure sockets and other industry standard technologies are implemented. ApplicationXtender provides for the granting of system access to users and to define user groups. Also, administrators or “super users” can also be defined. In addition to system-level access security, EMC offers application-level, functional, and document-level security.

EmailXtender creates a single repository for e-mail messages and their attachments, much as ApplicationXtender does for documents. Secure access to the EmailXtender repository is controlled through e-mail system security such as Exchange-based or Notes-based security roles and permissions. An individual typically can only access e-mail messages that he or she either sent or received. However, there are two additional levels of access: supervisory and administrative. Supervisors or other authorized personnel can be granted access to the messages of multiple individuals, such as all people on their team. Administrators have access to the entire repository of messages. Supervisory privileges can be granted to others, such as compliance officers or corporate legal counsel, who might need access to a set of messages for monitoring or discovery purposes.

- **Audit trails:** The ApplicationXtender suite is ODMA-compliant, a software industry standard, and enables comprehensive audit trails to be established that track user management, access management, and system monitoring functions for content capture and modification. Audit trails keep information and parameters in logs that can then be used to create compliance reports for Section 404. In order to generate these reports, an industry-standard reporting package (such as Crystal Reports) can be used to generate reports based on the data tracked through ApplicationXtender audit trails. Audit trails are maintained as part of the overall system, and are retained as long as the underlying records.

The EmailXtender suite also provides full audit trails of user and supervisory access and other functions performed on the message archive, as well as a variety of standard reports against the audit trail. Additionally, these auditing records cannot be altered in order to ensure the appropriate rules of evidence are enforced. Once again, the audit trails are maintained as part of the overall system and are retained as long as the underlying records.

The Sarbanes-Oxley Act is intended to ensure internal controls for managing information in financial statements. It is the job of the CIO to guarantee that data created and housed by IT can hold up to audit scrutiny. In addition, the data that supports financial information and accounting processes should be readily available. The solution you choose should manage both documents and data as well as e-mail.



EMC Corporation
Hopkinton
Massachusetts
01748-9103

1-508-435-1000
In North America 1-866-464-7381

EMC², EMC, and where information lives are trademarks of EMC Corporation. ApplicationXtender, DiskXtender, Documentum, and EmailXtender are registered trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

© Copyright 2006 EMC Corporation.
All rights reserved. Published in the USA. 9/06

Data Sheet
S11590906V2