

Sarbanes-Oxley: Implications for Document and Message Storage

Sarbanes-Oxley has had a dramatic and continuing effect upon organizations, particularly in the area of data storage. Use this guide to help strengthen procedures and ensure that data storage is sufficiently robust to meet external auditing standards.

Inside this report:

<u>General Impact on IT</u>	3
<u>Document Storage Requirements</u>	9
<u>Compliance Frameworks and Controls</u>	13
<u>Technology Solutions</u>	23
<u>Developing a Compliance Plan</u>	25

Info-Tech Research Group is a professional services firm dedicated to providing premium research and objective advice to IT managers of mid-sized enterprises, serving more than 25,000 clients worldwide. Our purpose is to provide practical and thorough solutions that enable IT managers to bridge the gap between technology and business.

www.infotech.com

888-670-8889 (North America)
519-432-3550 (International)

© Info-Tech Research Group, 2005

INTRODUCTION

As a result of the corporate management and accounting scandals of 2000 to 2002, the corporate accountability bill sponsored by Senator Paul Sarbanes and Representative Michael Oxley was passed into law in 2002. In general it contains a number of provisions that impose obligations on public corporations designed to ensure transparency of operations and accountability. These provisions are designed to address specific business processes, and ensure that auditable records are retained. Because records and transactions today are heavily digitized, the result is a considerable impact upon the IT environment, particularly in storage processes. Although the principal targets are financial documents and financial reporting, it is clear that the overflow effect will be to include an ever-increasing variety of materials that may be used to support those materials.

The Securities Exchange Commission (SEC) required publicly traded companies with market capitalization over \$75 million to meet major Sarbanes-Oxley compliance directives by November 15th of 2004, with smaller companies having until July 15th 2005 to comply. One study has suggested that large and medium-sized companies will spend upwards of \$2 billion through 2005 to become Sarbanes-Oxley compliant. Other estimates put the figure at \$6 billion by 2007 on storage infrastructure alone.

The immediate impact of the Act within the storage area is in its Title VII, Section 802, which provides penalties for destruction, alteration or falsification of records, and prohibits destruction of corporate audit records. The records covered are as broadly defined as any that may be required in a federal investigation or bankruptcy proceeding. While financial records are the principle interest, other records such as communications regarding transactions and documents relating to projects may also fall within the Act's purview.

The effect upon storage processes is that all documents must now be protected against wilful deletion, alteration or destruction, with the burden of proof on the corporation to prove that alterations have not taken place. Documents that are relevant to an audit or review need to be retained for a period of seven years; because the scope of a review cannot be determined

in advance, this could potentially include communications, project documents, memos, plans, specifications, and pronouncements.

While traditional data backup and storage processes have been targeted toward speed, efficiency, and disaster recovery, the new provisions require an additional level of archival management, including capability to search through vast numbers of records for relevant data as well as insuring the integrity of data storage. Saving e-mail correspondence also becomes critical, though this has often been previously overlooked. As with other documents, e-mail must be stored in a way that is accessible, in this case, including attachments. Storage must be unalterable, and it must include all relevant e-mail, while at the same time excluding the millions of spam messages and viruses whose addition would create an impossible burden.

In addition to the specific impact areas, Title IV, Section 404 of Sarbanes-Oxley – Management Assessment of Internal Controls – requires verification that appropriate infrastructure is in place. This imposes a requirement to audit IT systems, including storage, to ensure data security and integrity. The audit procedures are generally based on formalized frameworks, the most common of which are COSO (The Committee of Sponsoring Organizations of the Treadway Commission) for financial reporting and COBIT (Control Objectives for Information and Related Technology) for IT management. As companies move from the “quick fix” solutions required to meet immediate compliance requirements, Section 404 is becoming increasingly important. In addition to imposing a burden, however, this can be used as an opportunity for strengthening procedures and ensuring that data storage is sufficiently robust to meet external auditing standards.

GENERAL IMPACT ON IT

In general, IT managers need to develop a better understanding of internal controls, understand their company's Sarbanes-Oxley compliance plan, develop a plan to address IT control elements in the overall plan, and integrate the IT plan into the overall compliance strategy.

Sarbanes-Oxley and other regulatory legislation place a requirement on storage that it should be robust, unalterable, searchable, and exist over a

lengthy period of time. This results in a host of consequent considerations affecting every area of storage technology as well as related business processes. Some of these areas are:

- **Reliability.** Data must be able to be brought online at any time during a period of seven years or more. Reliability must be high enough to satisfy legal requirements of availability and to ensure that large penalties will not be incurred due to data not being obtainable.
- **Heightened performance.** Requirements for storage are dramatically increased due to the need to store a large amount of data, in accessible form, for long periods of time. Automated capture and storage of financial data is of particular importance. E-mail adds to this burden, as messages and message threads are likely to include thousands of items each, with the number of items to account for reaching, potentially, hundreds of millions.
- **Increased security requirements.** Security measures must not only prevent data destruction and ensure recovery is possible, but also preclude interference with stored data. This not only affects the backup software, but also the mechanism and media used. Backup data needs to be secured against access just as though it were data in use.
- **Scalability.** The amount of managed data required to meet these demands is likely to increase exponentially, particularly for large enterprises with high financial transaction volumes. More data will have to be stored for a longer time each year. To this will also be added a new range of content, such as multimedia, particularly in the form of presentations and recorded videoconferences.
- **Migration options and open standards.** These need to be considered to ensure that data stored today will be accessible tomorrow as the organization's data storage infrastructure evolves. This is particularly important with the growing trend toward software "activation" and limited installation options. For document management products, if the vendor goes out of business and the original application has been removed, stored documents may no longer be accessible.

- **Business processes.** All processes relating to storage need to be reviewed and modified to meet the new demands. Auditing procedures for storage must be developed to ensure that it continues to meet reporting requirements, and procedures for access control to stored data need to be put into place. This area, related to Section 404 of Sarbanes-Oxley, is likely to have the largest long-term impact, because it requires business processes involved with storage to be opened to external audit controls.

E-mail storage represents a particularly difficult problem in compliance. It has been estimated that over 50 billion e-mails are sent per year, and this number is climbing. An Osterman Research Survey shows that the average information worker sends and receives over 19,000 e-mail messages each year, and stored messages are growing by 37 percent annually – a percentage established before the more rigorous demands of Sarbanes-Oxley. E-mail has normally been stored online or moved to tape backup in the same manner as ordinary documents. Users are more likely to keep as much as possible online, though over 80 percent is never viewed after 30 days from receipt. This practice grows personal storage requirements, and also makes e-mail more difficult to backup and manage. Even where global backup to tape is possible, The Radicati Group reports that each dollar spent on storage disk space requires an additional \$15 in management.

Specific Impact on IT

Sarbanes-Oxley contains a number of provisions of special relevance to IT. The Act specifies that public accounting firms must “prepare and maintain for a period of not less than 7 years, audit work papers and other information related to any audit report, in sufficient detail to support the conclusion reached in such report.” This will inevitably require public companies to maintain backup records. Another specific provision is that it is 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.” This broader statement will force enterprises to store all data because it cannot be determined in advance just which materials might be required in an investigation.

Sections of specific relevance are:

Title I, Section 103: Auditing, quality control, and independence standards and rules.

The company's auditor must maintain all audit-related records for seven years. While this is specifically targeted at accounting firms, it is also likely to impose similar requirements on public companies whose results are being guaranteed by those accounting firms, which will include all public companies.

Title II, Section 201: Services outside the scope of practice of auditors.

Firms that audit a company's books cannot also provide IT services. This means that IT services used in recordkeeping can no longer be provided by the auditor.

Title III, Section 301: Public company audit committees

Companies must provide systems or procedures that permit whistleblowers to communicate confidentially with the company's audit committee.

Title III, Section 302: Corporate responsibility for financial reports

The CEO and CFO must both sign statements verifying completeness and accuracy of financial reports. This makes them personally responsible, and imposes penalties, thus being more effective than a simple fine.

Title IV, Section 404: Management assessment of internal controls

The CEO, CFO, and auditors must all attest to the effectiveness of internal controls for financial reporting.

Title IV, Section 409: Real time issuer disclosures

Companies are required to report changes in financial conditions on a rapid and current basis, for "real-time disclosure." This makes it necessary to provide facilities for search and retrieval of documents and messages.

Title IV, Section 802: Criminal penalties for altering documents

Companies must ensure that authentic, immutable records are retained, and adequate retention infrastructure is in place.

Similar Recent Legislation

Sarbanes-Oxley represents only the tip of the iceberg when the recent spate of regulations affecting IT procedures is also considered. Sarbanes-Oxley is primarily distinguished from the other regulations by two things. First, it is global, in that it is applied directly to public corporations of all types, and will gradually become a factor to all organizations doing business with them... effectively including most companies of any size. Second, instead of the usual fine, it imposes jail sentences for non-compliance. Many previous regulations have been under-enforced, so companies have grown accustomed to considering whether the rules should be followed on the basis of a compliance cost-versus-risk assessment. Sarbanes-Oxley is different, however, in that executives are unwilling to risk a custodial sentence at any cost.

However, in addition to Sarbanes-Oxley, there are numerous regulations impacting the IT environment, ranging from those focusing upon vertical industries – such as healthcare – to those focusing upon specific corporate activities (generally, finance). Additionally, they exist at all levels of government, from federal down to the municipal level. For this reason, it is important to develop a general compliance strategy, in addition to addressing the requirements of the most prominent regulations.

Among the most important regulations that need to be considered are Sarbanes-Oxley, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and financial services regulations SEC17a and NASD 3010. All of these require organizations to be able to quickly produce e-mail as a part of the discovery process in litigation, audits, and investigations.

HIPAA, which comes into force in April 2005, requires that all patient information, authorizations, policies, procedures, and contracts with business associates be retained for at least six years. This information must also be stored in a data center that provides minimum guaranteed uptime and high

security. The SEC regulation SEC 17 CFR 240, which came into effect in May 2004, requires that all communications between stockbrokers and clients, including e-mail and instant messaging messages, be retained for three years and be easily accessible for the first two years.

The Enterprise Strategy Group (formerly Enterprise Storage Group) has estimated that as many as 15,000 laws and regulations have IT compliance components.

Regulations of this type are now proliferating around the world, as can be seen in Table 1.

Table 1. Recent Regulation Affecting IT

Regulation	Applies to:
European Data Privacy Directive	Companies doing business in Europe handling Personally Identifiable Information
HIPAA	Healthcare Insurance U.S. businesses handling medical records
Gramm-Leach-Bliley	Banks and financial services companies doing business in the U.S.
DoD 5015.2 (Standard)	U.S. Department of Defense U.S Federal Agencies Business dealing with U.S. Federal Agencies
Public Records Office Standards	Companies doing business in public sectors for various countries
Patriot Act	Companies doing business in the U.S.
Sarbanes-Oxley	U.S. public companies and private foreign issuers
SEC Rule 17a-3/4	U.S. companies engaged in broker-dealer activities
CA Breach Law	U.S. companies doing business in CA handling Personally Identifiable Information
NASD 3010, 3110, NYSE 342	Member companies

DOCUMENT STORAGE REQUIREMENTS

Sarbanes-Oxley and related regulations have an immediate and permanent effect upon storage and backup strategies and procedures, both for ordinary documents and for e-mail – which presents a special case. The regulations are primarily aimed specifically at financial documents, but it can easily be seen that the need to maintain audit trails and document transactions results in a “best practices” solution that includes most documents generated within the enterprise.

Affected Documents

While the central focus of Sarbanes-Oxley is upon financial records, the general provisions calling for support of audit results and retrieval of documents (including messaging) that may be required in an investigation effectively call for the storage safeguards to be applied to all documents. This is also a reasonable practice, in that it makes it unnecessary to decide which documents might be relevant, and also ensures that new regulatory requirements that might increase the scope of required records can be met.

Specific items that must be included are financial documents, including:

- Individual accounts or groups of related accounts,
- Footnote disclosures included in financial statements,
- All line items and notes, and
- All footnote disclosers included in published financial statements.

The need to maintain an audit trail extends this requirement into transaction- and task-related documents and communications. Priority must be given to the financial records themselves, though other material must also be accessible.

General Storage Rules

Compliance requires an assessment of backup and restore strategies, records archiving, and long-term data retention. All records, including e-mail and instant messaging, must be indexed, and this index needs to be easily searchable. Audit capability is also required to determine if anyone has attempted to tamper with storage. Records stored for more than seven years still need to be accessed. In associated business processes, access to records must be improved, security must be tighter, and detailed record keeping of backup and storage is necessary.

Compliance requires:

- That record integrity be protected for the whole specified retention period. Records must be stored in a way that they cannot be altered, and access to records must be traceable.
- Records must be available within a reasonable period of time.
- Physical security of storage media must also be maintained. This can be ensured by placing duplicate copies of data on separate media stored in different locations.
- Access to storage locations must also be monitored and recorded. Procedures need to be put into place to track and manage access to media as a part of compliance strategy.
- Reliability of the drives and media selected for storage are also important. Higher reliability requirements mean that better quality solutions will be needed.
- All workstations now need to be included in the backup strategy, including all email, instant messaging messages, voice mail, and other personal data.
- Automated storage of data, particularly financial data, will be required on a regular basis with sufficient granularity to support "Real-Time Disclosure." This data collection will need to be continuous and non-disruptive to the operations of the enterprise; it also must be saved in a form that can be certified as unaltered.

- Access to archived data within a reasonable time also becomes important. Access is made more difficult by the vast increase in the amount of storage required, as well as in the need to provide some form of indexing and database access.

Far more than equipment, storage managers need management and operations processes that can demonstrably ensure internal storage infrastructure controls comply with the auditing framework followed by the company. This emphasis on process comes from the Act itself, which states that companies must file an internal control statement with its annual report that includes "an assessment, as of the end of the most recent fiscal year...of the effectiveness of the internal control structures and procedures of the issuer for financial reporting." This means that, not only must the data be retained, but that companies must demonstrate that the financial information is being managed and protected in an appropriate way to ensure compliance. Storage groups must identify and document processes and establish reporting procedures to demonstrate that storage management policies and processes are in compliance. Specific areas that need to be considered are:

- **Data protection.** Data security, and management of backup and restore operations.
- **Data availability.** Policies related to access and retrieval of data from current and archival sources.
- **Data recovery.** Includes disaster recovery.

General areas that need to be considered in each of these areas include:

- **Ensuring policies exist**, are properly documented, and conform to legal and compliance requirements.
- **Processes are supported** by policy and are followed.
- **Reporting is in place** to provide an audit trail and evidence of compliance.
- **A validation process exists**, including testing of controls, processes, and reporting.

Many of the requirements of Sarbanes-Oxley are really a finetuning of existing best practices in storage management. IT audit frameworks, such as COBIT, specify adherence to “good practice” standards, which would be true of a Sarbanes-Oxley compliant architecture.

Sarbanes-Oxley requires a more sophisticated view of storage than is commonly held at many corporations. The tendency has always been to treat data as data – that is, one undifferentiated byte stream to be managed and stored in case of systems failure. However, Sarbanes-Oxley requires differentiation between critical and routine data, and it requires access to data that has been placed in long-term storage.

E-mail Storage Rules

In today's business environment, e-mail has taken on a special importance, because it is now often the preferred communications medium for agreements, contracts, approvals, and work discussions. Effective e-mail archiving, however, requires filtering to ensure efficient spending, since there is an enormous amount of spam and other unwanted or irrelevant e-mail. Storage of e-mail also provides an audit trail for any litigation the company may be involved in.

Although the requirements for email storage are similar to those for other records, the nature and content of messaging creates a number of special problems. First of all, messages are ubiquitous and tend to be stored locally, at the workstation level. Second, the volume is extraordinarily high, and without filtering can include wholly nonessential items such as advertising and spam. Third, messages can contain documents and other material, and are likely to be of direct relevance to any investigation of transactions.

Although message archiving systems have been available for some time, Sarbanes-Oxley and related regulations add a special urgency to putting an adequate solution in place that provides capability to centrally store all relevant messages as well as permitting search and retrieval of messages in storage. New systems are now coming on the market specifically designed to meet these requirements.

Special requirements include:

- Compliance with regulations specific to e-mail.
- Secure and tamperproof archiving.
- User access controls and an audit trail.
- Smart indexing and archive searching.
- Management of storage media and libraries.

COMPLIANCE FRAMEWORKS AND CONTROLS

The first step in compliance is to develop a basic competency in the regulations. This requires input from a variety of sources, including compliance, risk management, finance and legal departments. Existing corporate policies and directives need to be examined and expanded. It is also important to be familiar with the guidelines that auditors will be applying. COSO is of specific importance as the preferred audit guideline for financial data. COBIT standards for best practices in IT management are also likely to be applied.

COSO and COBIT do not directly address storage; however, general principles will apply. Focus areas are Risk Assessment, Control Activities, and Monitoring Areas.

After assessing risk and processes, action must be taken, addressing shortcomings that have been identified. This may include developing and documenting new operating procedures that can be set as standards, and introducing new monitoring and reporting

Managing compliance is an ongoing process that requires changes in both technology and in business processes. The first requirement is to fully understand the requirements imposed by the regulations, including those that are specific to your industry. A compliance policy needs to be developed, and this requires a dialog between IT personnel, senior management, and legal counsel.

COSO

In its final rules on the Sarbanes-Oxley Act, the SEC made specific references to the COSO recommendations. These recommendations are from the Committee of the Sponsoring Organizations of the Treadway Commission, whose mission is to strengthen financial controls. Of specific interest is Section 404 of the Act, which addresses internal controls over financial reporting. This section also requires management of public companies to assess the effectiveness of these controls and annually report the results of that assessment. This inherently has a high degree of impact on IT.

COSO is a voluntary organization in the private sector, established in 1985 with the goal of improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. It contains representatives from industry, public accounting, investment firms and the New York Stock Exchange. COSO-sponsoring organizations include the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA).

The objective of COSO is to support Internal Control, key concepts of which are stated as:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected by people. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

The COSO framework has become the broadly accepted standard for meeting reporting requirements. The overall risk management approach is designed to achieve objectives defined in four categories:

- Strategic – high-level goals, aligned with the enterprise mission
- Operations - effective and efficient use of resources
- Reporting - reliability of reporting
- Compliance - compliance with applicable laws and regulations.

The latest version of the guidelines is the Enterprise Risk Management - Integrated Framework, an extension of the Internal Control - Integrated Framework, which is generally being used as the framework of compliance for Sarbanes-Oxley and other regulations.

The internal controls dimension is the most important from an IT and storage perspective, since it specifies the types of processes and procedures that need to be in place in order to comply with regulations. There are five dimensions of internal controls:

1. Control Environment, which is the top level and sets the tone of the organization.
2. Risk Assessment, used to form a basis for determining how risks should be managed.
3. Control Activities, including policies and procedures that help ensure management objectives are carried out.
4. Information and Communications, including processes and systems that support information transfer in a form and time frame enabling people to carry out responsibilities.
5. Monitoring, or the processes that assess quality and performance of internal control over time.

For any given objective – in this case, reliability of financial reporting – management must evaluate the five components at the organizational and at the process level. Figure 1 illustrates how these dimensions are applied.

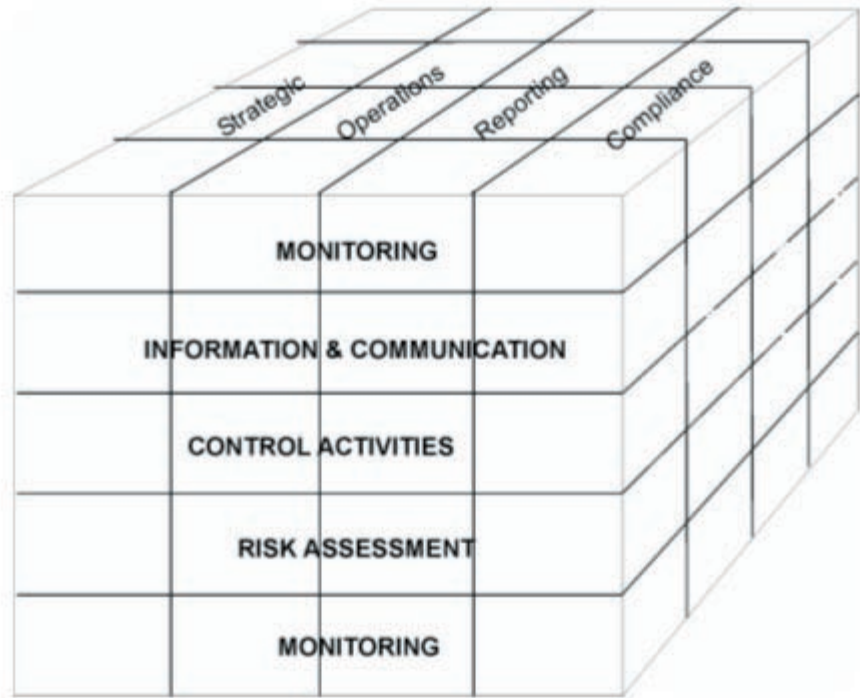


Figure 1: COSO Internal Control Dimensions

The overall effect of COSO with respect to Sarbanes-Oxley is a focus on control activities and the monitoring of those activities. Control Activities need to be in place within the process to reduce financial reporting process risks to an acceptable level. From an information storage perspective, this requires automation of documents storage, establishment of supporting policies and procedures, and development of auditing capabilities to ensure that objectives are being met.

COBIT

The IT Governance Institute (ITGI), established in 1998, was set up to clarify and provide guidance on current and future issues pertaining to IT governance, security, and assurance. The ITGI's main publication is Control Objectives for Information and Related Technology (COBIT). COBIT is becoming an internationally accepted guidance standard for IT governance. It provides a reference framework and common language for management, auditors, and security analysts across the IT sector. It is of specific relevance to Compliance because it is 100 percent compliant with COSO, and so may be used as an extension of COSO into the IT sector. It bridges the communication

gap between IT functions, business, and auditors by providing a common approach.

While there are a number of IT internal control frameworks, the guidelines established by COBIT are generally considered most useful, and have become aligned with COSO and the spirit of the Sarbanes-Oxley Act. COBIT provides both company-level and activity-level objectives and controls.

COBIT is a framework for managing risk and control in IT. It is made up of four domains, 34 high-level control objectives and 318 detailed control objectives. It includes controls that address operational and compliance objectives across all aspects of IT, although the areas of specific relevance to Sarbanes-Oxley are the financial-related areas.

The four domains are:

1. Plan and Organize.
2. Acquire and Implement.
3. Deliver and Support.
4. Monitor and Evaluate.

The COBIT Framework is the basis of the approach and foundation of the other elements. It provides a fundamental set of principals for organizing IT activities into a process model. The Framework explains how IT processes deliver information the business needs to achieve its objectives through its 34 high-level objectives, each of which describes a separate IT process. The Framework identifies which of seven information criteria and IT resources are required for IT processes to support business objectives.

The seven information criteria are:

1. Effectiveness.
2. Efficiency.
3. Confidentiality.
4. Integrity.

5. Availability.
6. Compliance.
7. Reliability.

IT resources are defined as people, applications, technology, facilities and data.

In support of the Framework, COBIT also publishes Control Objectives, Control Practices, Management Guidelines, and Audit Guidelines, as well as other material.

The elements in these categories can be evaluated according to the COSO framework (Figure 2) to provide a reasonably comprehensive audit model for IT operations. This is the model that is most likely to be used by external auditors, and provides the best guarantee that requirements are being met.

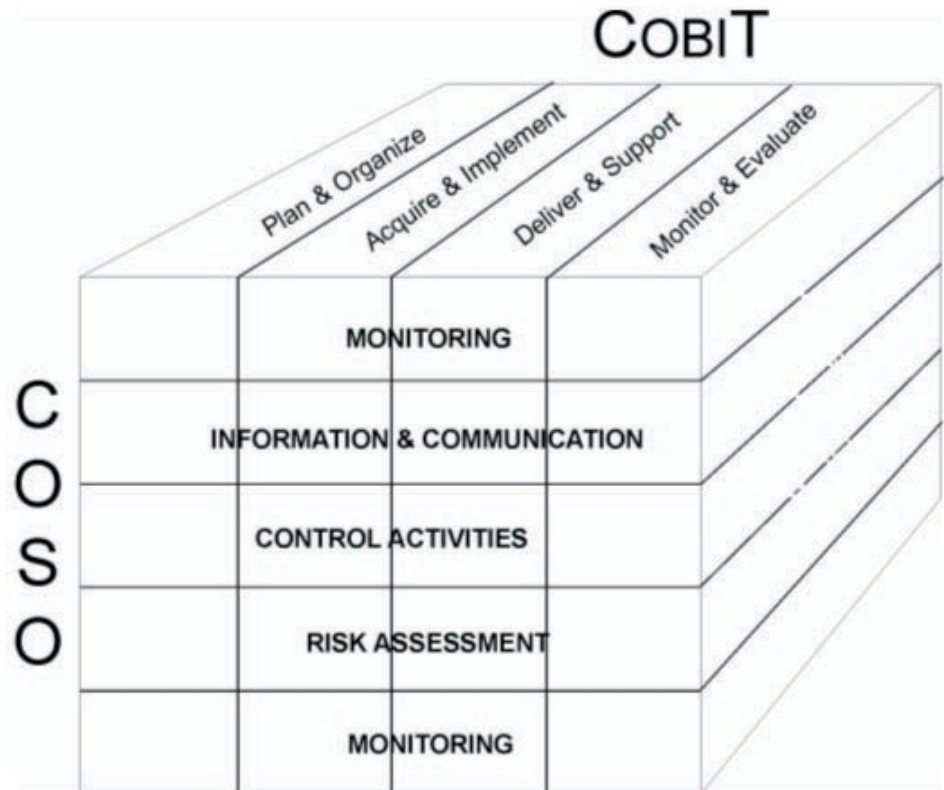


Figure 2: COSO/COBIT Mapping

Although not strictly aligned with storage, COBIT/COSO evaluation is heavily loaded with storage-related components. Potential questions specifically related to storage concerns in each of the target areas are presented below.

These are based loosely on COBIT objectives from the "Plan and Organize" and "Monitor and Evaluate" areas, and are grouped according to the COSO objectives which will be used in a financial audit. These are:

- Control Environment.
- Risk Assessment.
- Control Activities.
- Information and Communications.
- Monitoring.

Control Environment

IT Strategic Planning

- Is storage management planned to include essential upgrades and to provide a robust and error-free environment as required by business objectives?

IT Organization and Relationships

- Do storage managers have adequate knowledge of regulatory responsibilities and objectives?
- Have key systems and data been adequately inventoried and owners identified?
- Is data integrity ownership in place?
- Are clear lines of responsibility identified, including roles for contractors?
- Are there mechanisms in place to ensure timely notification of security breaches to senior management?

Management of Human Resources

- Are storage requirements well understood, and staff well trained in any changes to the storage environment?

Educate and Train Users

- Are training needs adequately identified for new policies and procedures, particularly with respect to compliance?
- Is adequate security training in place?

Risk Assessment

Assessment of Risk

- Does the IT organization have an assessment framework for risks and possible threats to stored data?
- Is a comprehensive security assessment performed for critical systems based on priority?
- Is risk assessment ongoing?
- Has a business impact assessment been performed that considers the impact of storage failures on financial reporting processes?

Manage Facilities

- Are data storage facilities provided with adequate environmental controls to maintain data in the case of fire, power failure, excessive heat, or other potential threats?

Control Activities

- Are appropriate controls in place to ensure data integrity and reliability of storage?

Information and Communication

Information Architecture

- Have information capture processing and reporting controls been put into place to ensure completeness, accuracy, validity and authorization, particularly for financial information?
- Have data been classified according to security level, and are security measures sufficient?

Communications of Management Aims and Directions

- Are there documented policies and procedures governing storage?
- Are these policies and procedures regularly reviewed?
- Is there a policy in place to investigate and remedy deviations?
- Do storage management and staff understand roles and responsibilities related to compliance?

Monitoring

Compliance with External Requirements

- Is there ongoing monitoring of the regulatory environment, including changes that might impact IT controls – both for IT in general, and for the specific industry?
- Are controls in place, and are they followed?
- Are storage systems capable of meeting timeliness requirements of external regulations?

Management of Quality

- Does adequate documentation of storage processes and policies exist?
- Is there a quality assurance plan in place?

- Does the quality assurance plan provide for periodic testing and review?
- Has data integrity ownership been communicated to data owners?

Manage Performance and Capacity

- Is the performance and capacity of systems and network components involved with storage continuously monitored?
- Is there a policy in place to respond to suboptimal performance?
- Is capacity planning and performance included in design and implementation of storage infrastructure?

Monitoring

- Have performance indicators for storage systems been identified, and are they being monitored with appropriate metrics?

Adequacy of Internal Control

- Are internal controls adequately monitored and assessed?

Independent Assurance

- Are independent reviews undertaken?
- Is documentation available for use by independent auditors?

Internal Audit

- Is there an internal audit department or committee with responsibility for reviewing storage requirements?
- Does the IT audit plan include a risk assessment that includes storage and data security?

TECHNOLOGY SOLUTIONS

Sarbanes-Oxley is seen by many vendors as the next big opportunity to sell equipment since Y2K. This, at least, is the perception by many corporate IT managers. Companies need to review their storage infrastructure and procedures; this means opportunities for new products, as well as for updates of existing systems.

In terms of software, companies need to find solutions that provide auditing of access to storage, access to specific records in storage, and verification that stored records have not been altered. Backup and storage companies are developing systems for documents and records as well as for e-mail, which presents special difficulties.

Technology is critical for compliance. There is now a wide range of software available from point solutions to platform-level solutions that adapt infrastructure designed for other purposes, including business process automation, document management, financial management, or storage management.

- Point solutions are specifically focused on Sarbanes-Oxley, provide depth of coverage, and may be appropriate for the first year of compliance in order to put a framework in place and ensure that deadlines can be met.
- Platform solutions provide breadth and may serve as infrastructure supporting broader compliance and risk management objectives. For the long term, an infrastructure level approach is likely to be required.

Short-term compliance packages generally provide a methodology framework, project management, workflow review and approval, documentation management, ad hoc reporting, and integration with third-party reporting tools. In themselves, they can only aid in the process and provide a starting point for a continuing effort. Specialist point solutions include:

- Handysoft SOXA Accelerator.

- Movaris Certainty.
- Nth Orbit Certus.
- OpenPages Sarbanes-Oxley Express.
- Paisley Consulting Risk Navigator.

However, the initial rush toward “point solutions” specifically designed to manage Sarbanes-Oxley compliance is largely over. Companies need to put long-term solutions in place that address not only Sarbanes-Oxley, but also the other regulations that might come into play. Solutions need to be able to withstand an external audit, and IT managers will need to be able to verify that appropriate solutions are in place. Long-term compliance will require platform-level solutions with direct linkage to ERP and process modelling tools. Platform-level solutions include:

- Oracle Internal Controls Manager.
- PeopleSoft Enterprise Internal Controls Enforcer.
- SAP Management of Internal Controls (MIC).
- SAS Institute's Corporate Compliance for Sarbanes-Oxley.
- Documentum-EMC Corporate Compliance and Governance Edition.
- FileNet Compliance Framework.
- IBM Lotus Workplace for Business Controls and Reporting.
- Microsoft Office Solution Accelerator for Sarbanes-Oxley.
- OpenText Livelink for Corporate Governance.
- Stellant Corporate Governance Solution.

In addition to general document storage, special attention must be paid to message storage and archiving. A number of storage solutions are available specifically to solve the e-mail storage issue, such as MessageArchive

by IntelliReach, as well as systems by KVS, Zantaz, iXOS, and AXS-One for Microsoft Exchange. Other solutions are available for Lotus Notes and UNIX.

In terms of hardware, no specific technology is favoured, but the most obvious solution is use of WORM tape, optical media, and data cartridges. Storage must now be tamperproof. WORM provides a built-in protection against rewriting. If more information is to be added, it is appended to the media, thus retaining the original data and organization. WORM tape drives are highly efficient and swift. Optical disks, also providing WORM technology, have restricted capacity and performance, and have a relatively high cost per megabyte of storage. WORM tape drives currently provide capacity of up to 1.3 terabytes and performance of up to 280 gigabytes per hour.

Solutions are now available from Sony and Quantum. The Sony solution is a WORM-enabled Super-AIT (SAIT) and AIT (Advanced Tape Technology) tape drive. These drives use special cartridges, with WORM capability added through firmware stored in the cartridge Remote Memory-in-Cassette chip. The drives themselves accept both WORM and standard read/write tape media. The WORM tape media storage will also last for about 30 years, which is sufficient to meet most storage requirements.

DEVELOPING A COMPLIANCE PLAN

Development of an IT compliance plan for Sarbanes-Oxley should be just one part of an overall compliance effort involving legal, accounting, and senior executive input. The chief focus of the regulation is upon financial procedures, and internal reporting procedures need to remain the key focus. However, the policies and procedures that are developed will require IT support. It is important that IT be represented on the compliance team, because electronic storage of information will be critical to meeting requirements. Changes in storage architecture need to be examined carefully to ensure that the result is adequate, that it is not disruptive of ordinary corporate business, and that it can be implemented at reasonable cost.

Within the IT department, it is important to examine the company's existing backup and storage systems, as well as the information that is being retained. The four basic steps that need to be taken are:

- Scoping and evaluation of documents with regards to the need for retention and continued access.
- Evaluation of current storage and backup practices, procedures, and equipment to determine adequacy of current system and specific changes that might be required.
- Development of new systems and infrastructure, and providing for a minimally disruptive implementation.
- Ensuring comprehensiveness of the new solution in meeting compliance requirements, and compatibility with existing systems.

The major control element of Sarbanes-Oxley is Section 404. It is this section that requires an independent audit process, and will have the most bearing upon development of IT controls. Overall, compliance should be undertaken as a project that includes:

- Project organization, establishing the team to examine the requirements.
- Development of a project plan, and establishing key success factors, milestones, and checkpoints.
- Establishing a project approach and reporting requirements, including assessment of documentation requirements, definition of control units for evaluating entity-level and process-level controls, and identifying the tools and technology needed to support controls.

CONCLUSION

Sarbanes-Oxley has had a dramatic and continuing effect upon organizations, particularly in the information technology and data storage areas. Although the regulation is designed principally to control accounting practices and ensure transparency in financial reporting, the mechanisms for data storage and verification have come under significant review. Meeting the new requirements requires an examination of in-place technology and procedures with the aim of creating a robust and verifiable system capable of withstanding an external audit.

As Sarbanes-Oxley comes into force, its scope is broadening to directly include more companies as a result of its built-in deadlines, and to include more companies indirectly as the need for compliance causes partnering firms to maintain the same levels of storage integrity and verification. The emphasis upon these processes can, and should, be used to improve IT processes so that they better support the other objectives of the business as well as strengthen disaster recovery.

Although Sarbanes-Oxley is the most important of the recent regulations in this area, it is not the only regulation to affect the storage area. In general, companies are being required to put best practice systems in place, supported by solid procedures that reduce the possibility of records tampering and make it possible to recover relevant material from backups.

The challenge is large, and compliance issues are constantly changing. The real focus, however, must be upon changing how data is viewed – particularly legacy data and messaging. A robust and secure storage system that provides reasonable access to backup documents provides a powerful mitigation tool for a multitude of legal and financial risks.

Compliance needs to become an ongoing process, with periodic reviews, as with other business risks. The IT department, which has often operated on its own, must now bring its policies into line with those of the rest of the firm.



About the Author

Brian J. Dooley is an author, analyst, and journalist with more than 20 years' experience in analyzing and writing about trends in IT. He has written six books, numerous user manuals, hundreds of reports, and more than 2,000 magazine features. Projects include technology research, market research, white papers, magazine features, case histories, online documents, user manuals, Web pages, online help systems and multimedia. Mr. Dooley is the founder and past president of the New Zealand chapter of the Society for Technical Communication. He has been a Senior Analyst for Datapro (Gartner), and a Senior Product Information Specialist for Unisys Corp. He initiated and is on the board for the Graduate Diploma of Technical Communication program at Christchurch Institute of Technology, and he is on the editorial advisory board for Faulkner Technical Reports. Mr. Dooley currently resides in New Zealand.

Research & Analysis

Our research and advisory services offer unparalleled access to IT research specifically geared to the unique needs of IT professionals working in mid-sized enterprises. Research Seats with [Info-Tech Advisor](#) will provide you and your team with the research and analysis needed to succeed with daily IT tasks and management. Research Seats with [McLean Report](#) will support your IT strategy development and provide access to relevant, industry specific research. To compliment both Research Seat options, tap into customized guidance and advice with an [Analyst Inquiry Service](#), and gain access to unlimited, on-demand advice from industry experts.

© 2005 3409945 Canada Limited, operating as the Info-Tech Research Group ("Info-Tech"). All rights reserved. Reproduction in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Info-Tech disclaims all warranties and conditions as to the accuracy, completeness or adequacy of such information. Info-Tech is not liable for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection and use of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Note: All Web links in this document were checked for accuracy and functionality at the time of publication. We cannot, however, guarantee that referenced Web sites will not change the location or contents of linked materials, and will not be held responsible for such changes.

Find out more – www.infotech.com
 888-670-8889 (North America)
 519-432-3550 (International)