



Speeding SOX Audits:

*Why Automated DPM Tools
Make Sense*



June 2005



Table of Contents

- Table of Contents..... 2
- Overview..... 3
- About Sarbanes-Oxley..... 3
- About SOX Frameworks, IT and Data Protection 4
- Aligning Key Data Protection Processes with SOX Internal Controls 5
- Addressing Both the Spirit and the Letter of the Law for Data Protection..... 6
- Following the Spirit of the Law: Lessons Learned from Real-World Compliance Efforts and Actual SOX Audits..... 7
- Automated vs. Manual: How Data Protection Management Software Can Speed SOX Compliance and Improve Effectiveness..... 8
- What to Look For: Important SOX-Related Functions Involved in Data Protection Management Software 9
- Conclusion..... 10
- About Bocada..... 11

Overview

This white paper focuses specifically on Sarbanes-Oxley Act (SOX) regulations relevant to data protection, and describes both best practices and automated tools used by today's leading storage managers and backup/recovery teams to meet the mandates of SOX. Information has been drawn from real-world SOX audit experiences and demonstrates how leading companies are benefiting from the use of data protection management software to streamline compliance-related testing and demonstrate documented control over data protection. A specific set of tests to determine if your data protection processes can meet a SOX audit is also provided herein. The paper concludes by outlining key features in data protection management software that can automate aspects of compliance and reduce the cost for both internal and external SOX audits.

About Sarbanes-Oxley

Much has already been written about the Sarbanes-Oxley Act of 2002 and its intent to hold public company executives accountable for the accuracy of their company's financial reporting processes. Sarbanes-Oxley was enacted in an effort to avoid the corporate malfeasance and much-publicized accounting scandals of U.S. companies like Enron, WorldCom and HealthSouth. It holds companies to a high standard of corporate governance, risk management, communications and compliance. This set of standards is commonly referred to as GRC (governance, risk management and compliance).

A recent global report of leading CEOs by PriceWaterhouseCoopers describes GRC as: "More than simply a response to burgeoning laws and regulations, GRC is becoming a value-adding principle that is being embraced by an ever-growing number of leading organizations throughout the global business community."¹

While SOX is applicable only to publicly traded companies, speculation is widespread that SOX and its implied, higher standards of GRC will eventually be extended to private sector companies, including those seeking venture capital or traditional financing, poised to go public and facing acquisition or merger.

Section 404 of the SOX legislation is most relevant to IT organizations, including the storage management and data protection teams, as it requires corporate management (executives and a financial officer) to take:

"responsibility for establishing and maintaining adequate internal control over financial reporting for the company."²

Among other things, it stipulates that corporate management must also identify:

"any **framework** used to assess the **effectiveness** of the company's **internal control** over financial reporting."

In addition, to comply with SOX, management must make a written annual statement available that proves internal control over financial reporting is effective and reports any "material weaknesses" or deficiencies in the effectiveness of any of the company's internal controls surrounding financial reporting. Fines—and even more severe consequences—may await executives whose companies are consistently unable to meet SOX regulations.

1 "8th Annual Global CEO Survey: Bold Ambitions, Careful Choices," by PriceWaterhouseCoopers, published in 2005, [http://www.pwcglobal.com/Extweb/insights.nsf/docid/48C44DA89CB0CC4185256F7F0061C641/\\$file/8thAnnualGlobalCEOSurvey.pdf](http://www.pwcglobal.com/Extweb/insights.nsf/docid/48C44DA89CB0CC4185256F7F0061C641/$file/8thAnnualGlobalCEOSurvey.pdf)

2 Section 404 regulations quoted from "IT Control Objectives for Sarbanes-Oxley," April 2004, published by the IT Governance Institute, p. 13, http://www.isaca.org/Template.cfm?Section=About_ISACA&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406.

About SOX Frameworks, IT and Data Protection

IT organizations and their related processes have come under scrutiny for SOX as well, since much of the financial reporting performed by a company relies on IT applications, systems and data. CIO Magazine laid out the relationship between IT and SOX financial reporting as follows:

“While Sarbanes-Oxley is financial legislation, at its heart it is about ensuring that internal controls or rules are in place to govern the creation and documentation of information in financial statements. Since IT systems are used to generate, change, house and transport that data, CIOs have to build the controls that ensure the information stands up to audit scrutiny.”³

Company compliance officers, internal auditors and IT organizations often use two commonly accepted frameworks, COSO (Committee of Sponsoring Organizations) and COBIT (Control Objectives for Information and related Technology)⁴, to help them translate SOX into an actionable plan for compliance.

The COSO framework, developed by the Committee of Sponsoring Organizations of the Treadway Commission,⁵ has been widely referenced by both the SEC and the U.S. Public Company Accounting Oversight Board (PCAOB) as the prevailing standard for further interpreting the meaning of SOX legislation.

COSO identifies five framework components under which SOX-related processes should be interpreted:

- control environment
- risk assessment
- control activities
- information and communication
- monitoring

Under COSO, IT organizations can focus on a sub-area of controls related to technology, which is also known as “general computer controls.” General computer controls are one of the largest sets of internal controls identified by the COSO framework and encompass the IT processes and objectives surrounding today’s corporate data centers, along with the activities of IT managers and administrators who oversee the daily operation of a company’s systems, applications and related data storage. The quality of these computer controls is perceived by SOX auditors as having direct bearing on the accuracy and effectiveness of a company’s financial reporting.

COBIT is another framework more commonly used by IT organizations to define a company’s effectiveness with SOX-related IT controls. It is also used to further translate COSO’s general computer controls into a workable plan for IT. COBIT has been widely adopted by IT organizations thanks to its granularity, and how it defines specific IT processes related to SOX and provides examples of how to test each process.

COBIT is regarded as a model of good practices for operating and assessing effectiveness of IT processes. By identifying four main IT domain areas (see Table 1) and breaking them down to 34 key processes, COBIT offers a workable roadmap for IT to systematically evaluate, assess, test, monitor and report on the effectiveness of each related control.

The following table is a typical COBIT/COSO mapping that shows the key IT-related processes that come under scrutiny in a SOX compliance audit. Rows identify the COBIT domains and the related IT internal control processes applicable to SOX. Columns map each COBIT IT control process to one of the five COSO framework components. (Highlighted rows directly correlate to a company’s data protection processes and are discussed further in the following section.)

3 “Your Risks and Responsibilities,” by Ben Worthen, CIO Magazine, May 15, 2003, <http://www.cio.com/archive/051503/rules.html>.

4 See <http://www.isaca.org/cobit> for more details about COBIT and the COBIT framework.

5 See <http://www.coso.org/> for more details about COSO and the COSO framework.

>> Table 1

IT Internal Controls Mapped to COBIT and COSO Frameworks⁶

COBIT Area	COSO Component				
	Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
PLAN AND ORGANIZE (IT ENVIRONMENT)					
IT strategic planning	X	X		X	X
Information architecture			X	X	
Determine technological direction					
IT organization and relationships	X			X	
Manage the IT investment					
Communication of management aims and directions	X			X	X
Management of human resources	X			X	
Compliance with external requirements				X	X
Assessment of risks		X			
Manage projects					
Management of quality	X		X	X	X
ACQUIRE AND IMPLEMENT (PROGRAM DEVELOPMENT AND PROGRAM CHANGE)					
Identify automated solutions					
Acquire or develop application software			X		
Acquire technology infrastructure			X		
Develop and maintain policies and procedures			X	X	
Install and test application software and technology infrastructure			X		
Manage changes			X		X
DELIVER AND SUPPORT (COMPUTER OPERATIONS AND ACCESS TO PROGRAMS AND DATA)					
Define and manage service levels	X		X		X
Manage third-party services	X	X	X		X
Manage performance and capacity			X		X
Ensure continuous service					
Ensure systems security			X	X	X
Identify and allocate costs					
Educate and train users	X			X	
Assist and advise customers					
Manage the configuration			X	X	
Manage problems and incidents			X	X	X
Manage data			X	X	
Manage facilities		X			
Manage operations			X	X	
MONITOR AND EVALUATE (IT ENVIRONMENT)					
Monitoring				X	X
Adequacy of internal controls					X
Independent assurance	X				X
Internal audit					X

⁶“IT Control Objectives for Sarbanes-Oxley,” April 2004, published by the IT Governance Institute, p. 50, http://www.isaca.org/Template.cfm?Section=About_ISACA&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406.

Aligning Key Data Protection Processes with SOX Internal Controls

For the specific needs of IT data protection teams, data protection processes must be judged by how effectively they meet the requirements of several COBIT control processes. Storage managers and IT professionals involved in backup and recovery efforts should make special note of the control processes related to a company's data protection efforts highlighted in the previous table.

These include:

- **IT strategic planning**
- **Assessment of risks**
- **Management of quality**
- **Define and manage service levels**
- **Manage problems and incidents**
- **Manage data**
- **Manage operations**
- **Monitoring**
- **Adequacy of internal controls**
- **Independent assurance**
- **Internal audit**

It's important to note that two IT control processes highlighted above, *Manage Data* and *Manage Operations*, deal specifically with confirming the effectiveness of data protection processes such as routine backup and restore procedures. Other highlighted IT control processes should also be examined when determining how effectively and completely each data protection process complies with overall SOX requirements.

Addressing Both the Spirit and the Letter of the Law for Data Protection

The IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA) have further refined the specific subset of controls, known as "Illustrative Controls," that should be tested for SOX compliance within each of COBIT's IT control processes. They've even provided sample tests to help organizations prove the effectiveness of each control. These samples are known as "Illustrative Tests of Controls." (To review all illustrative controls and illustrative tests of controls, readers should refer back to Appendix C in the ITGI report, "IT Control Objectives for Sarbanes-Oxley.")

For data protection teams, the following table of illustrative controls and tests has been excerpted, summarized or inferred from the ITGI report. Using this table you can test whether your data protection processes are effective enough to meet a SOX audit.⁸

⁷ Ibid, p. 57.

⁸ Ibid, pp. 74-77.

IT Internal Controls Related to Data Protection

COBIT-Related IT Process	Primary Illustrative Controls Related to Data Protection
<p>Manage Data This control should provide a “reasonable assurance that data recorded, processed and reported remains complete, accurate and valid throughout the update and storage process.”</p>	<p>Policies and procedures exist for the handling, distribution and retention of data and reporting output. Illustrative tests include determining “whether policies and procedures are adequate for the protection of data” and “testing evidence that the controls over protection of data ... are operating effectively.”</p> <p>Management protects sensitive information, logically and physically, in storage and during transmission against unauthorized access or modification. Illustrative tests focus on security access issues, and judge whether adequate controls are in place to fulfill the control mandate when data is either being stored or transmitted to other locations either on or off the network.</p> <p>Retention periods and storage terms are defined for documents, data, programs, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication. Illustrative tests require reviewing data distribution and retention procedures, including ones that define retention periods and the assurance that those periods conform to SOX guidelines.</p> <p>Management has implemented a strategy for cyclical backup of data and programs. Illustrative tests determine if the organization “has procedures in place to back up data and programs based on IT and user requirements.” They also recommend selecting “a sample of data files and programs to determine if they are being backed up as required.”</p> <p>Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media. Three types of illustrative tests are offered to prove the effectiveness of this control:</p> <ol style="list-style-type: none"> 1. Inquire whether the retention and storage of messages, documents, programs, etc., have been tested during the past year. 2. Obtain and review the results of testing activities. 3. Establish whether any deficiencies were noted and whether they have been re-examined. Obtain the organization’s access security policy and discuss with those responsible whether they follow such standards and guidelines dealing with sensitive backup data.
<p>Manage Operations This control should provide “reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.”</p>	<p>Management has established and documented standard procedures for IT operations, including scheduling, managing, monitoring and responding to security, availability and processing integrity events. Illustrative tests focus on whether IT operations and procedures have been documented and are subject to periodic review for compliance. They also recommend reviewing a sample of events, such as job scheduling and job monitoring, in order to confirm that response procedures are operating effectively.</p> <p>System event data is sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing. Illustrative tests determine whether enough chronological information is recorded and stored in logs and is available for possible reconstruction, if necessary. Users wanting to test this control should obtain a sample of log entries, to determine if they allow data reconstruction.</p> <p>System event data is designed to provide reasonable assurance as to the completeness and timeliness of system and data processing. Illustrative tests look at “the type of information used by management to verify completeness and timeliness of system and data processing.” They also recommend reviewing a sample of system processing event data to “confirm completeness and timeliness of processing.”</p> <p>User-developed systems and data is regularly backed up and stored in a secure area. Illustrative tests should demonstrate “how end-user systems are backed up and where they are stored.”</p>

Following the Spirit of the Law: Lessons Learned from Real-World Compliance Efforts and Actual SOX Audits

While most IT organizations and backup/recovery teams are doing their best to learn what's required for SOX compliance and are adapting their processes to comply with the letter of the law, many are surprised by additional efforts and documentation that may be required by external SOX auditors. Although the wording of the Sarbanes-Oxley Act stresses internal control related to financial applications, in reality, both internal and external auditors are given wide latitude to assess the effectiveness of virtually any IT operation.

Large, well-known companies in the financial services and insurance industries are typically on the cutting edge of SOX/IT compliance because they tend to have the most frequent interaction and communication with external auditors.

From field interviews Bocada has conducted with several Fortune 1000 customers in these industries, a clear picture emerges about what concerns auditors most in regards to data protection.

SOX Audit Case #1: A large investment banking firm's auditors, when assessing the effectiveness of the company's data protection controls, looked for the following:

- An auditable trail that proves data is being backed up successfully.
- An auditable trail that proves data is restorable.
- Proof that the supporting processes associated with data backup and restore can be reproduced.
- The ability to take random samplings of servers or clients that demonstrate data has been successfully backed up or that data can be successfully restored. (Some auditors have even been known to request certain data be restored from a specific point in time, such as two weeks earlier.)

SOX Audit Case #2: A storage management team at an insurance company facing Sarbanes-Oxley audits every 30 days consulted with both internal and external auditors to produce its own SOX-related checklist of all relevant data protection processes and the results of monthly testing of these processes. This team determined that the following eight key backup/restore control activities were the most relevant to a SOX auditor:

1. Process for securing and authorizing access to backup tools, including authorization and approvals for access.
2. Process for securing and authorizing access to physical backup servers and tape libraries, including details about how and where these items are secured.
3. Description of the automated backup process, as follows: The process of performing backups is conducted by automated backup solutions which are used to perform backups of operating systems, applications and data. These backup solutions perform the backup as defined by the backup schedule and catalog the location of backup tapes both on-site and off-site in the event the working production copy is not available.
4. Summary of specific process for backing up new or changed data (i.e., when incremental backups vs. full backups are performed).
5. Monthly review process for new backup requests, including follow-up process for requests submitted but not entered into the system.
6. Process for performing restore requests via an in-house incident management system.
7. Process for monitoring backup jobs that identifies and resolves incomplete or failed backup jobs.
8. Process of conducting a quarterly physical backup audit that ensures all server-class machines are being backed up by one or more scheduled backup jobs.

Automated vs. Manual: How Data Protection Management Software Can Speed SOX Compliance and Improve Effectiveness

Most storage management teams have been forced to develop manual procedures to assess, test and report on the effectiveness of their data protection controls to meet the requirements outlined herein. But manual processes are slow, making it difficult to maintain the necessary assessment, documentation and testing required for SOX compliance issues. More importantly, manual procedures are difficult to replicate, making it virtually impossible for executive IT management, as well as audit and compliance officers, to ensure the integrity of the processes themselves.

A recent survey on emerging trends of internal controls for SOX conducted by accounting firm Ernst & Young⁹ indicated that nearly 60% of companies currently used Excel spreadsheets or an Access database to track remediation efforts they've made to resolve issues previously identified with the effectiveness of their internal controls. Interestingly enough, survey respondents indicated that the largest control set requiring remediation were those that prevented or detected errors in routine data protection processes.

Use of data protection management software can reduce or eliminate the burden of building manual reports and conducting time-consuming manual assessments to support SOX compliance. By automating evaluation, monitoring, assessment, testing and reporting, software is able to minimize the burden SOX places on today's busy storage management teams. Further, an automated solution allows companies to establish and routinely execute compliance audits based on established policies. From the field, Bocada has seen IT groups begin using data protection management and reporting tools as a means to automate and speed much of their ongoing SOX compliance efforts. Recently, more than 30 leading enterprises successfully passed federal regulatory compliance audits of their data backup operations using BackupReport[®] software from Bocada. BackupReport not only serves as the documented control required by many regulations, but also automates the collection, analysis and delivery of comprehensive information on the performance and results of all data backup efforts.

What to Look For: Important SOX-Related Functions Involved in Data Protection Management Software

Data protection management applications and backup reporting applications can aid in and automate many SOX compliance efforts. Data protection teams interested in these applications should look for the features and functions outlined in the following table. *(See next page)*

⁹"Emerging Trends in Internal Controls, Third Survey," by Ernst & Young, Oct. 2004, reprinted in Compliance Week, <http://www.complianceweek.com/articleFiles?ACFB32.pdf>

Software Features That Speed SOX Reporting for Data Protection Processes

SOX Reporting Guide	Software Features to Look For
Demonstrate proof of success with backup-related IT control processes	<ul style="list-style-type: none"> • Provides automated, prescheduled reports that demonstrate the successful completion of all backup jobs in the environment. • Automatically discovers the backup activities related to up to several thousand servers on the network, in a transparent, non-intrusive manner that does not require installation of agents on each server node.
Demonstrate proof of success with restore-related IT control processes	<ul style="list-style-type: none"> • Provides automated reports that demonstrate the success of previously identified data restore jobs.
Demonstrate proof of ability to assess, track and correct backup or restore errors and improve backup/restore processes	<ul style="list-style-type: none"> • Demonstrates trends in backup/restore activities that indicate process improvement over time. • Provides several different views of the same backup/restore data, including further detail about the source of any backup errors.
Demonstrate the ability to perform random, independent audits of backup/restore processes and related remediation efforts	<ul style="list-style-type: none"> • Automatically selects a random sub grouping of servers or targets and runs a report to demonstrate success (effectiveness) of the backup control process. • Automatically selects a random sub grouping of restore jobs recently performed and reports on their relative success or failure. • Produces a random audit report of key, failed backup jobs and demonstrates current remediation of failures and successful backups. • Produces auditable, independent, third-party test reports not tied to any specific backup software application or any desired IT outcome.
Demonstrate compliance with any service level agreements (SLAs) surrounding data protection, backup and recovery	<ul style="list-style-type: none"> • Enables reporting of pre-existing service level agreements (SLAs) related to data protection, backup and recovery, along with the IT group's success or failure at meeting preset SLAs, and trends that indicate SLA performance improvements over time. • Allows definitions of SLA reporting to encompass only a subset of systems, applications and users.
SOX communication and audit reporting surrounding data protection	<ul style="list-style-type: none"> • Reports and independent audit results of backup/restore activities that are easy to produce and disseminate to key internal compliance team or other upper-level management. • Flexible report dissemination to encompass multiple communication methods, including automated e-mail attachments, export to Excel spreadsheets, publishing results to an internal Web site, etc. • Report filtering options to create different classes of data protection owners or zones for more specific Sarbanes-Oxley reporting needs. Examples: <ul style="list-style-type: none"> – Organize servers and targets related to backup of key financial applications into a "SOX financial reporting zone" where backup and restore reporting encompasses only those systems tied to financial applications. – E-mail support systems could be viewed from within an "E-mail compliance reporting zone," where backup and restore reporting covers key e-mail data as a regulated company asset. – Use report filtering functionality to set up an overarching "SOX audit zone" where all system assets are available for reporting, but the backup/restore reports are simplified to indicate only the higher level items SOX auditors want to see regarding process success and failure. An example of a simplified SOX audit report that could be developed from such a report filter is shown here:



Conclusion

Ultimately, Sarbanes-Oxley and related compliance mandates have proven to be a major burden for IT staff and operations. Members of IT organizations at all levels—from CIOs to administrative staff—must now view compliance processes as part of the overall policy framework for IT operations. Looking forward, IT organizations can also expect the burden to grow even greater as specific controls are outlined and processes gain further definition.

To meet these new realities, IT organizations will need the support of automated tools and processes in order to adequately and cost-effectively comply. The use of technology and automated reporting tools by early adopters to aid in these efforts has already paid off in meeting SOX compliance—as well as creating other business advantages. Based on its survey findings, Ernst & Young stated:

“Those that have selected and successfully implemented supporting technology for Section 404 compliance may now be in a position to reap the benefits, as they are better able to strategize testing, evaluate trends in results, and quickly and effectively manage remediation activities.”¹⁰

Indeed, the benefits of data protection management include not only the peace of mind that comes from knowing you have the tools to meet a SOX compliance audit but also the freedom to pursue better business practices. By incorporating trustworthy automated processes for their data protection, IT teams can more readily invest their time in building the IT organization, trimming costs, providing quality services and meeting the goals of the business—rather than dreading audits.

About Bocada

Bocada® was founded in 1999 to help enterprise customers reduce the cost and pain of managing complex data protection systems. Bocada software is deployed at more than 170 leading enterprises worldwide, ensuring the daily success of millions of backup jobs, and the cost-effective protection of more than 600,000 mission-critical servers. Bocada customers routinely experience improvements in their data protection success rates from less than 60% to more than 99.9%, while reducing costs by millions of dollars per year and meeting policy compliance mandates. Bocada serves 25 of the Fortune 100, including market leaders such as Unilever, DeutscheBank, SBC, Sprint, Valero and Xerox. Bocada is privately held with headquarter offices in Bellevue, Washington.

¹⁰ Ibid.



10500 N.E. 8th Street, Bellevue, WA 98004

Tel: (425) 818-4400 | Fax: (425) 818-4455 | sales@bocada.com | www.bocada.com
