



How to “Ace” Your Next SOX Audit:

Eight Steps to Straight A’s



February 2006



Table of Contents

- Abstract..... 3
- Translating SOX Compliance into Data Protection Management 3
- The Straight A's to Acing SOX Audits 5
- Steps 1 & 2: The Planning Stage..... 6
- Steps 3 & 4: Taking Action 7
- Steps 5 & 6: Taking Stock 8
- Steps 7 & 8: Making Progress 8
- Conclusion 9



Abstract

Successfully meeting a SOX audit requires reporting on numerous data protection management activities. Forward-looking organizations often offload the intensive monitoring and reporting on their backup and restore procedures to automated tools. Independent, third-party reporting gives them a rapid, global and impartial view into the effectiveness of IT controls across a wide spectrum of backup/restore applications, servers and network components and helps them meet audit requirements quickly and effectively. Find out how leading corporations are “acing” the data protection portions of their SOX audits using automated tools and learn how to apply the proven eight-step process—the Bocada “Straight A’s” framework for SOX audits—to your environment.



Translating SOX Compliance into Data Protection Management

The Sarbanes-Oxley Act of 2002 has had a significant effect on most IT teams’ priorities and day-to-day work. The wording of SOX Section 404, specifically, brought a renewed focus on the effectiveness of “internal controls” surrounding IT processes.

Originally intended to test the effectiveness of internal controls associated with a company’s financial reporting, Section 404 audits soon broadened their reach to encompass many other IT processes. Many enterprise IT organizations have since seen their original efforts to comply with SOX Section 404 evolve into a much broader set of industry-accepted best practices, typically based on the COBIT (Control Objectives for Information and related Technology)¹ framework used to ensure effective IT governance across a wide spectrum of IT areas.

SOX for Storage Managers

For storage management teams at many of the largest enterprises, this broadening in scope for Section 404 compliance required new processes, tests, automated reports and self-audits to prove effective protection and management of all types of company data.

According to James Damoulakis, chief technology officer at enterprise storage consulting firm GlassHouse Technologies,² the impact of Section 404 compliance on storage managers currently encompasses the following three broad areas:

1. **Data protection** (includes both data security and the management of processes surrounding backup and restore)
2. **Data availability** (includes policies associated with how easily data can be accessed and retrieved from current sources or archives)
3. **Data recovery** (includes processes to ensure data recoverability after disaster strikes)

¹ See <http://www.isaca.org/cobit> for more details about COBIT and the COBIT framework.

² “A Storage Management Perspective on Sarbanes-Oxley,” article by James Damoulakis, published in the Storage & Security Journal, Feb. 3, 2005, <http://issj.sys-con.com/read/48053.htm>.

SOX for Data Protection and Backup Administration Teams

A recent survey of Bocada® enterprise installations indicates that for backup administrators and teams charged with SOX compliance the most important areas of data protection include:

Table 1. Common Data Protection Areas impacted by SOX Audits

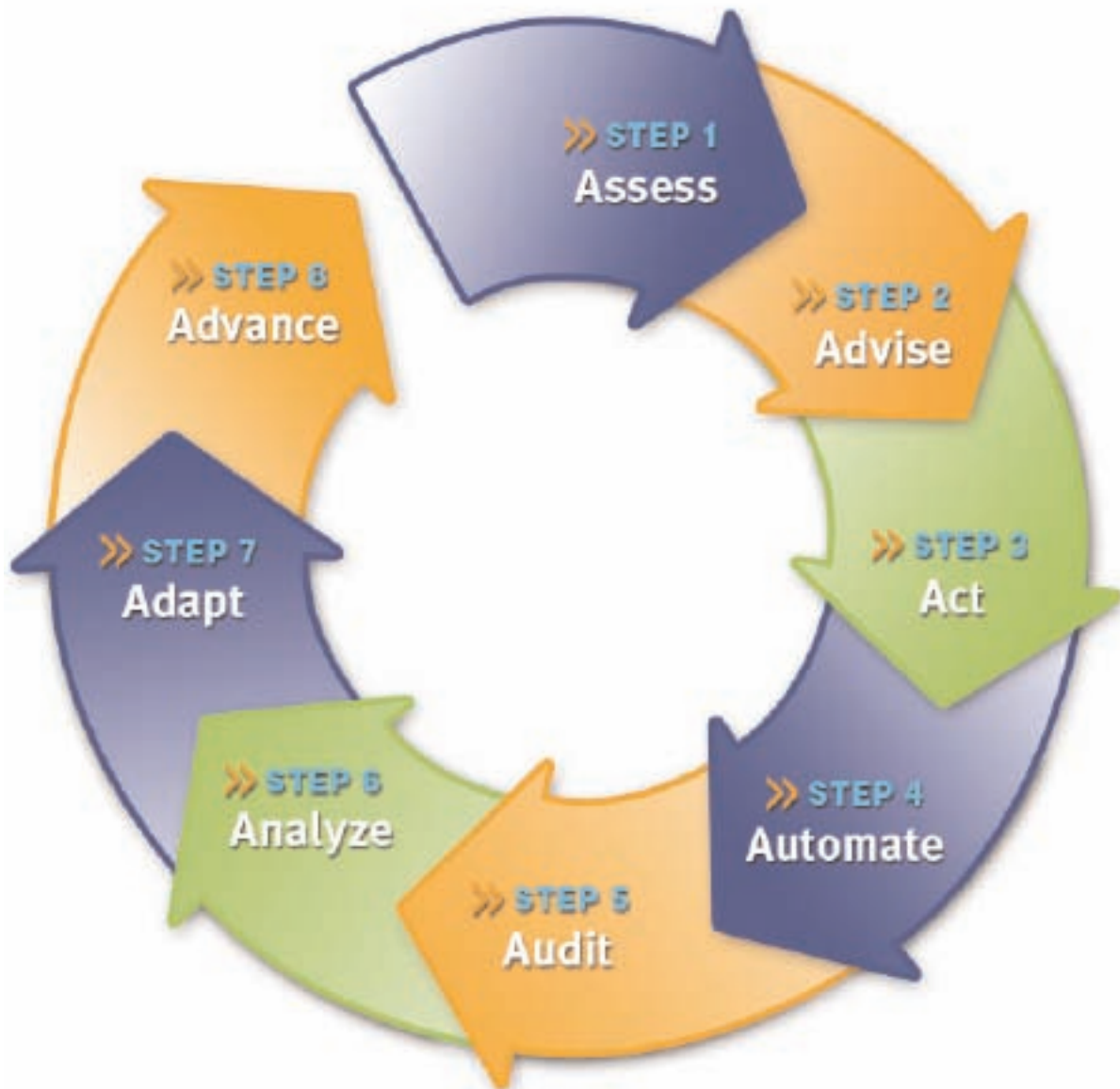
Data Protection Area	Examples
Security	<p>Document policies and procedures that indicate how the following are being logically and physically secured from unauthorized access:</p> <ol style="list-style-type: none">1. Physical backup media in use (backup servers, tape systems, storage systems, etc.).2. Software tools in use for backup or restores.
The Backup Process	<p>Document the backup processes to ensure successful backup of company data. Be prepared for auditors to ask to see both specific samples of backup data, as well as random samples that prove successful backup completion.</p>
The Restore Process	<p>Document the processes to ensure either specific data sets or random samples of data can be successfully restored. This should also outline the process for meeting user restore requests.</p>
Backup/Restore Change Control Practices	<p>Document the steps for changing current processes to incorporate backups of new systems and data or changes to the current backup routine, from the addition or change of backup jobs, etc.</p>
Backup/Restore Problem Identification and Resolution	<p>Document the process for identifying, reporting on or correcting any backup issues, including failed backup jobs, incomplete jobs, etc.</p>
Independent Self-Audits and Tests That Prove Effectiveness of Backup/Restore Processes	<p>Document how you are auditing effectiveness of these backup/restore related controls. This might involve producing an ongoing set of reports (akin to an audit log or audit trails) that demonstrate how well current backup/restore processes are being followed. These should also show that all servers and data have been successfully backed up or are able to be successfully restored.</p>



The Straight A's to Acing SOX Audits

To achieve SOX compliance, some of the most strictly regulated firms (including financial services and insurance companies) follow a common set of processes. Data protection management teams at these companies, using Bocada, have helped outline these common practices. Based on their best practices, Bocada has created an eight-step framework it calls the "Straight A's to Acing SOX Audits". This framework is summarized in Figure 1.

Figure 1. Eight Steps in the Bocada Straight A's to Acing SOX Audits in Data Protection



Steps 1 & 2: The Planning Stage

The first two steps in the Bocada Straight A's framework for SOX audits address the up-front research, planning and documentation of IT controls required by data protection teams. Specifically, these include the activities identified in Table 2.

Table 2. Assess and Advise

Step	Description
<p>1. Assess specific requirements for backup and data protection with legal and compliance teams.</p>	<p>This is a critical first step that ensures agreement by all parties on the goals and parameters of successful compliance surrounding data protection. For help during this phase, consider contacting outside consultants, if needed, as well as information available about commonly accepted frameworks, such as COBIT, COSO and ITIL. (COBIT specifically lists controls and examples of control tests that could be performed to indicate effectiveness of data protection processes along with processes in other IT domains.³)</p>
<p>2. Advise staff and end-user customers, in writing, how you plan to ensure compliance with previously defined data protection goals.</p>	<p>This step is where you must document the control steps you plan to follow for each key SOX-related data protection management process. Some examples include:</p> <ul style="list-style-type: none"> n Documenting the backup processes in places that ensure company data is backed up successfully. n Documenting how backup data is kept guarded and secure from unauthorized access. n Documenting the process used to restore data, or to check for success of either backups or restores. <p>In your process documentation, you must also prepare for the likelihood that auditors will ask to see either specific samples of backup data, as well as random samples that prove the successful completion of backups.</p> <p>In some cases, data protection teams may choose to create and maintain this type of documentation for each workflow using separate Microsoft® Excel worksheets.</p>

Documentation Guidelines for Step 2. The advisory function should provide enough detail to document and accurately depict each data protection-related control process you plan to follow. One rule of thumb for documenting internal controls comes from the reporter's five questions needing to be asked: Who, What, Where, When and How. For example, you might ask the following of each process you plan to document:

- n **WHO** will be responsible for performing the control process (backup administrator, network engineer, DBA, etc.)?
- n **WHAT** specific steps will be performed within the IT control process? (For example, what steps do you take to back up the systems or ensure something is recovered?)
- n **WHERE** — in terms of applications, servers, storage media, data center, platform, work team and backup job names — will the steps be performed?
- n **WHEN**, or how often, must the process steps be executed? (For example, backup processes may run nightly at 2:00 a.m., or weekly starting at 5:00 a.m. Saturday.)
- n **HOW** will you capture and document policies and SLAs for the business units, including notices of policy updates or inadvertent changes? Also, what means will you use to identify and correct out-of-compliance results, such as missed RPO (spell out on first mention), RTO (same comment), and cost issues? Lastly, how will you communicate results to business units and auditors?

³ See Appendix C in the ITGI report, "IT Control Objectives for Sarbanes-Oxley," April 2004, published by the IT Governance Institute, http://www.isaca.org/Template.cfm?Section=About_ISACA&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406.

Steps 3 & 4: Taking Action

The next two steps in the Bocada Straight A's framework for SOX audits move the data protection team from planning into action. With these steps, you can see how well the documented process works.

Table 3. Act and Automate

Step	Description
3. Act — Put the documented process in motion.	Here you start to see how well you've documented the way things actually work, in regards to backing up every component of the system, or performing both large volume and more isolated restore activities. Start with the basics, and build from there. By putting the process into action, you'll gain immediate insights and awareness of any process challenges.
4. Automate whatever you can, especially in regards to performance of ongoing tests, or monitoring and communication of results.	<p>The act of ongoing monitoring and reporting of process performance can be one of the heaviest burdens on IT professionals, in terms of manual work involved, and the increased time required from limited staff.</p> <p>For data protection processes, tools exist such as Bocada Enterprise 4, to perform automated, prescheduled monitoring and reporting of the effectiveness of current backup and restore processes that span as many as hundreds of individual logs.</p> <p>In a recent report by AMR Research, Analyst John Hagerty indicated the use of technologies to automate testing and the outcomes of internal controls can be responsible for reducing the cost of SOX compliance by "upwards of 25 percent."⁴</p>

Lessons in Automating SOX Compliance. The data management team at a property and casualty insurance company had a particular SOX compliance requirement to have monitoring and reports ready for review every 30 days when auditors would visit and review records.

After adopting Bocada, the team was able to automate many reporting and validation tasks surrounding backup and restore operations, and reclaim valuable time in the process. For example, Bocada allowed the team to rapidly drill-down and analyze the root cause of specific backup failures and to develop reports for SOX-specific "zones" that only consisted of the status of backup/restore operations related to key financial application servers and systems.

The team was also able to use Bocada Enterprise 4 to automate testing of restores, setting up the system to perform both random and specific samplings that could quickly display the success or failure of specific restore procedures.

Overall, Bocada Enterprise 4 provided the team with valuable information that allowed them to move quickly to remedy failures, measure outcomes and rapidly improve on overall process management. As a result, they passed their SOX audits with straight A's.

Automation reduces costs of SOX Compliance

In a recent study by AMR Research, Analyst John Hagerty reported the use of technologies to automate testing and the outcomes of internal controls can be responsible for reducing the cost of SOX compliance by "upwards of 25 percent."⁵

⁴ See "SOX Decisions for 2005: Step Up Technology Investments," AMR Research Report by John Hagerty, January 14, 2005, available at <http://www.amrresearch.com/content/view.asp?pmillid=17887>

⁵ See "SOX Decisions for 2005: Step Up Technology Investments," AMR Research Report by John Hagerty, January 14, 2005, available at <http://www.amrresearch.com/content/view.asp?pmillid=17887>

Steps 5 & 6: Taking Stock

The third phase of the Bocada Straight A's framework for SOX audits allows data protection teams to see patterns, identify any gaps in the process, and start to troubleshoot and correct perceived weaknesses in the current controls process.

Table 4. Benchmark Your Progress

Step	Description
<p>5. Audit how well your teams are following the documented process as well as how well they resolve any subsequent issues.</p>	<p>This is a critical step in the process and should be performed frequently at the start to encourage adoption and standardization of the new workflows surrounding compliance.</p> <p>Automation tools, mentioned in the previous section, can also play a large part with their ability to gather information and qualitatively measure progress against goals such as RTO and RPO.</p> <p>Automated audit reports, like those found in Bocada Enterprise4, can also demonstrate trends over time. As data protection teams mature in their ability to spot and correct problems in backup/restore, they'll see a corresponding decline in the number, frequency, and severity of problems.</p>
<p>6. Analyze actual performance against the original goals of the process.</p>	<p>Pay close attention to any possible gaps in backup/restore workflows—especially tasks that are resource-intensive or time-intensive, which may lead to bottlenecks. Get the team's input and recommendations on how best to improve on the effectiveness of the current process. Exercise some caution: focus on the basics first. Do not try to optimize the entire process immediately.</p>

Steps 7 & 8: Making Progress

The last phase in the Bocada Straight A's framework for SOX audits supports the continuous improvement in IT controls goal of most organizations. When combined self-assessment and continuous improvement in processes pave the way for meeting high standards of IT governance surrounding data protection.

Table 5. The Final Steps

Step	Description
<p>7. Adapt your actions and ongoing activities in order to respond to or correct significant gaps that have been identified.</p>	<p>At this stage, it's important to remember to keep documenting any actions taken by you or other members of the data protection team to correct the issue. This should also include documenting changes you made to existing backup or restore processes.</p>
<p>8. Advance to step one.</p>	<p>This is the final step and the one that brings the entire eight-step process back full circle. Here, you need to reassess whether all requirements have been met, and whether or not there are new requirements that must now be addressed. Are you considering a new backup platform? Will you be adding remote replication? The ensuing steps in the framework will allow you to improve, communicate and act upon any new information and requirements, along with subsequent revisions of policies or procedures.</p>



Conclusion

There's no doubt that meeting Sarbanes-Oxley requirements in data protection can add to existing workloads. But many organizations have already discovered that offloading much of the intensive monitoring and reporting on their backup and restore procedures to automated tools like Bocada Enterprise 4 relieves much of the burden. In many cases, auditors have also begun to take advantage of these independent, third-party reporting tools because it gives them a rapid, global and impartial view into the effectiveness of IT controls across a wide spectrum of backup/restore applications, servers and network components.

Derived from compliance efforts at some of the most forward-looking IT organizations in the world, the Bocada "Straight A's framework to acing SOX audits" now gives data protection teams a straightforward, working roadmap to SOX audit success.

About Bocada

Founded in 1999, Bocada Inc. pioneered development of software that validates data protection system performance against business goals. Our flagship product, Bocada Enterprise 4, powered by BackupReport® technology, provides objective insight on service level delivery and performance, helping companies reduce their exposure to unrecoverable data, increase the utilization and performance of their infrastructures, reduce the cost of their service delivery, and comply with regulations. More than 180 brand-name customers and partners worldwide trust Bocada, including Amgen, Cap Gemini, Ernst & Young, CocaCola, Commerzbank, Microsoft, SBC, Sprint, Unilever, and Xerox. Bocada is a private company funded by leading venture investors and headquartered in Bellevue, Washington.



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

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