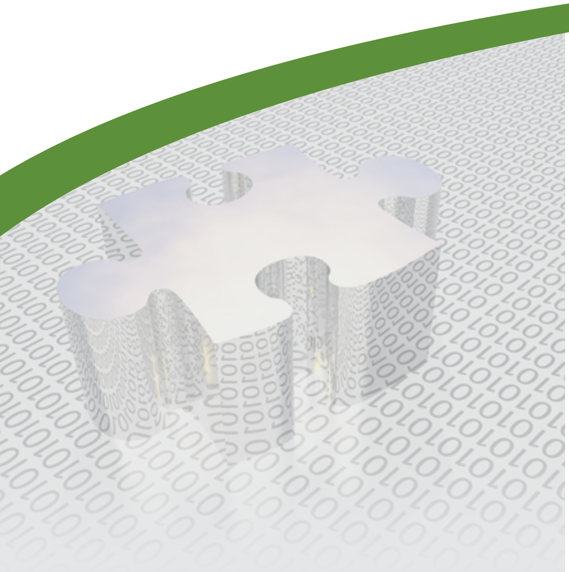
APTARE®

White Paper



The 7 Major Challenges of Backup Compliance and How to Overcome Them

How Data Protection Management Can Ease The Burden

Protection of financial data has always been a requirement for good business. The difference today is that this responsibility no longer lies solely with the CEO. IT now takes on a large portion of this duty, due in large part to the establishment of SOX (Sarbanes-Oxley) in 2002. In addition to SOX, however, IT teams face over 10,000 other regulations in the United States alone, as well as a variety of internal SLAs.

By now everyone is familiar with the parameters of SOX compliance; however, companies still face many operational challenges to the actual implementation of the SOX guidelines. The following paper outlines a set of major compliance challenges and highlights how data protection management (DPM) can help IT organizations address these challenges.

1. Compliance Drains IT Resources

The expense of non-compliance is well-known -- it can cost billions of dollars. But people rarely talk about the expense of compliance. The fact remains, however, that compliance imposes a massive and expensive resource drain on a company's IT staff by placing a substantial added workload on IT in terms of time and effort in monitoring, reporting and auditing to support SOX compliance. Daily compliance tasks such as writing and maintaining scripts, report generation, and interfacing with auditors and compliance committees take hour after hour that IT teams could otherwise spend on more productive storage administration activities.

As the need for both external and internal audits continually increases as part of the SOX compliance process, the IT staff's ability to respond to audits successfully takes a significant amount of time and effort. Every time a company is subjected to an external audit, new auditors come in, each with different requirements and requests than their predecessors, placing an added burden on the IT staff. New requests invariably mean reports need to be changed and new scripts need to be written --a time-consuming manual-labor-intensive task.

Passing the audit is never the end, however, as new audits come up, and the audit process continues to change and grow, ever expanding in scope and frequency. Again the IT staff must respond to these new demands with additional reports requiring even more new or modified scripts.

Auditors often demand complete transparency into a company's data and the underlying IT environment to make sure that the data is protected and secured. The problem is that companies might have tens of thousands of end points that don't have this level of visibility into their networks. It's just too complex.

External audits are only part of the problem. Internal audits and requests from corporate compliance committees and other internal stakeholders further add to the growing load of compliance-related tasks for the IT staff. Most organizations need a dedicated full-time staff member to write scripts to generate reports or retrieve information. In addition, many IT teams need a dedicated person to interface with auditors and internal stakeholders and manage the compliance process.

The DPM Advantage: Data protection management enables users to generate reports in a fraction of the time it takes to write new scripts, minimizing the cost, time, and effort required to be SOX compliant. With predefined reports to address most foreseeable requests and tools to help users easily define and generate new reports, DPM significantly reduces the need for writing scripts. In fact, hours of writing scripts can be reduced to minutes with DPM.

In addition, DPM enables the IT group to respond quickly and efficiently to a variety of requests, while minimizing the amount of time needed to interface with auditors and internal stakeholders making requests. DPM solutions that provide granular visibility into backup processes provide additional support by enabling users to efficiently respond to requests by quickly finding, retrieving and restoring data.

DPM can even provide centralized access to data via a “self-serve” portal, allowing auditors and stakeholders across the organization to find the reports and information they need, without taking time from the IT staff. The ideal DPM solution will provide secure access so the portal users only have access to the exact information they need, while maintaining overall data and system security.

2. Companies Define the Compliance Process

One of the greatest challenges that companies have with SOX compliance is the fact that while SOX outlines what is required, the guidelines do not provide business practices to help companies achieve the goal. The development of a SOX compliance process is left up to each individual company.

In simple terms, SOX requires that a company define the process, follow the process, and then prove that it is adhering to these policies. But the company decides what data needs to be tracked and establishes the processes and policies by which it will achieve these goals. The big question is: how does a company get the job done?

The DPM Advantage: A data protection management solution can be a significant advantage in developing a SOX compliance process. The key is to find a DPM solution that is customizable to the user-defined processes. DPM can also offer change management capabilities which provide a complete audit trail to show successes, failures, and remedies for the failures.

A DPM solution will provide out-of-the-box reports to track processes, and should also be adaptable, enabling customization of those reports, to align reporting with the unique companydefined processes.

In addition, DPM policy management functionality enables users to list all policies that define what is backed up, the schedule for the backup and the retention period.

3. Compliance Requires End-to-End Accountability

SOX compliance requires that a company report on the end-to-end lifecycle of the backups in its environment. The IT team must be able to answer questions such as – What data was backed up and when? What tape is the data on? Where is the media stored? What is the process for retrieving the tape and restoring the data? What is the expiration of the data? And they must be able to answer these questions for any data and backups. They must also be able to report on backup successes and failures, and conduct random restore tests to ensure that all backups are being tracked properly. In fact, an auditor may actually accompany an IT staff member to the location where the tapes are vaulted to see firsthand that the company has the necessary backup and restore processes in place.

The DPM Advantage: Data protection management provides real-time monitoring and reporting capabilities that document the end-to-end management of the data, enabling the IT group to answer all the questions about their backups and prove the data is protected per established policies. DPM provides an ongoing audit trail of adherence and changes to policies governing the protection of data, the status of the protection events, and data restorability.

DPM also simplifies the compliance process by offering a centralized view of complex backup environments across multiple data centers distributed around the world.

A DPM system will enable the user to:

- Identify the location of data or media
- Identify backup contents down to the application
- Report on the success or failure of backups
- Remediate backup errors
- Create an audit trail of remediation notes for failed jobs
- Create an audit trail as the data status changes from primary-secondary-offsite
- Show a random sampling of data protection events
- Provide role-based, secure access with an audit trail of access

4. Compliance Requires Timely and Accurate Information

At any point in time the IT team must be able to access timely and accurate information on data and backups, as part of SOX compliance. Audit frequency continues to increase, and companies often perform quarterly internal audits to prepare for the annual external audit. As the number of audits continues to multiply, the team needs to be able to prove at any moment that information on the company's data is available. Keeping data up-to-date can be a significant challenge.

The DPM Advantage: The right data protection management solution will provide information that is always up-to-date and available. A real-time reporting solution alleviates the constant scrambling to prepare for unexpected audits – all the backup information needed for compliance is always easily accessible and up-to-date through the DPM system. A browser-based DPM console provides an additional advantage by making access to data protection information even easier.

5. Compliance Must Be Sustainable

Compliance is not a one-time event. The compliance process does not end when a certain level is attained. If anything, the compliance burden continues to grow heavier, ever expanding in scope and frequency. So compliance must be sustainable, supported by ongoing processes and systems that are integrated into core IT operations.

Conducting internal audits is a best practice that enables companies to sustain compliance over the long term. Internal audits can prove that the IT team is performance-ready for an external audit at any time.

The DPM Advantage: Data protection management enables sustainable compliance by providing continuous access to accurate and timely information as needed. Companies should not view compliance as a goal to accomplish but rather as a part of a continuous process that can be tested at any time. DPM becomes embedded in the process to provide ongoing support for compliance.

By automating and streamlining processes with DPM, and eliminating redundant manual tasks, a company is better equipped to handle compliance responsibilities over the long term.

A DPM portal providing centralized access to auditors and stakeholders outside the IT organization also helps streamline the process and sustain compliance on a continued basis, reducing the burden of time and resources on the IT staff.

6. Compliance Must Be Objective

The integrity of the compliance process is critical. A company's ability to prove that it meets SOX requirements must be impartial, separated from the organization in a way that provides objectivity. Unfortunately, when the IT staff is writing scripts and generating reports, they bring a potential for inherent bias into the process. It is a natural tendency to show support for the company and the IT team, and this predisposition can impact the results of the reporting.

The DPM Advantage: Data protection management is a third-party solution that reports on the backup environment independent of the company's IT team and backup software vendor, providing a requisite level of neutrality. Because a DPM solution does not rely on scripts written by the internal team, it alleviates the potential bias and provides the objectivity that an audit requires.

7. Audit Requirements Are Constantly Changing

Every audit is different and so is every auditor. Audits expand every year in size and scope, with auditors constantly requesting new reports and more information than the previous year. In addition, new auditors are brought in and they bring new requirements with them. It is the job of the IT team to keep up with these constantly changing requirements, and to be able to meet any request quickly and efficiently.

In addition, a company's backup environment is continuously changing, and this dynamic nature of the environment adds additional burden on the IT staff to manage these changes in terms of compliance. For example, every time a new server is added, the IT staff must account for this change, which requires writing new scripts and modifying reports, not only to protect the data but also to meet compliance requirements.

The DPM Advantage: The ideal data protection management solution will provide the flexibility to scale and easily change as requirements are added. For example, additional reports can be easily configured without additional scripting to meet changing needs. A DPM solution can also provide a discovery feature that will identify unprotected data, simplifying the change management process for the IT team.

Conclusion

Compliance is here to stay. The truth is that SOX compliance is only going to become more challenging as backup environments become more complicated and as new compliance requirements are added. IT organizations will rely more and more on technologies that can automate compliance processes and minimize the expense and resources needed to meet compliance requirements. Data protection management provides an essential strategic advantage by solving many of today's compliance challenges, reducing the compliance burden on the IT organization, making IT teams more productive, and enabling IT to more quickly and effectively respond to requests from auditors and other compliance stakeholders within the organization.

APTARE StorageConsole

To find out how a data protection management solution can help ease your compliance burden contact APTARE at:

Web: www.aptare.com
Email: sales@aptare.com
Phone: 866.9278273