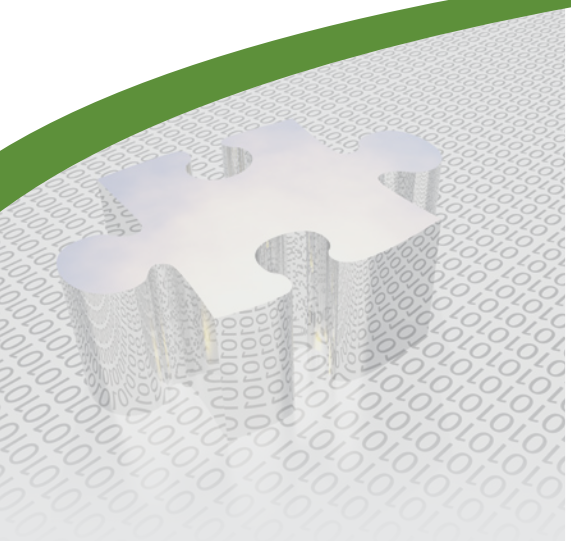
APTARE®



White Paper

Critical Compliance Responsibilities and Backup Capabilities

APTARE Data Protection Management solutions provide end-to-end visibility into the backup environment to ensure sustainable compliance.

Compliance should not be a fire drill that happens once a year. Compliance must be integrated into the core IT systems—with a data protection management solution.

Compliance is a huge burden on the corporation. IT teams face more than 10,000 regulations in the U.S. alone—not including their own internal service level agreements (SLAs).

The Sarbanes-Oxley Act (SOX) deals with the handling of financial records and is one of the most well-known examples of a regulation that requires ongoing compliance. SOX Section 404 applies specifically to IT teams covering the scope and adequacy of the internal control structure and procedures for financial reporting. Section 404 specifies that the CIO is accountable for the IT systems that generate financial reports. Any company with a market cap of $75 million or greater that generates financial reports using a computer must go through a SOX audit once a year.

In terms of compliance, corporations have three responsibilities:

- Define and communicate the control framework for dealing with financial reports and records.
- Follow the control framework. Many companies talk about the control framework but they do not live by it.
- Provide documented proof that the control framework is being followed. Compliance should not be a fire drill that happens once a year because an audit is coming up. Compliance must be integrated into the core IT systems—with a data protection management solution.

Ensuring Compliance with Data Protection Management

Data Protection Management (DPM) is a key technology to ensure compliance. DPM adds a layer on top of backup and replication systems, documenting the end-to-end management of the data while enabling the IT team to answer any question about backups and prove the data is protected per established policies. DPM also provides visibility into—and an ongoing audit trail of—adherence to established data protection policies, the status of protection events, and data restorability.

DPM can address the following compliance challenges:

End-to-End Visibility

Auditors are interested in the life cycle of data. They want to examine all the systems data passes through to reach the final location to ensure the data is protected

throughout every step of the process. To serve this purpose auditors will identify a list of SOX servers. These are all the servers that directly or indirectly impact financial data. DPM offers the IT team end-to-end visibility to track this data—and related compliance to SOX regulations—across the enterprise. The result is sustainable compliance that minimizes the cost, time, and disruption of audits.

Accuracy and Timeliness

Traditional backup technologies cannot effectively report on the status of data. DPM solutions are independent of the backup software vendor and scripts providing a proven independent resource for accurate and timely compliance information.

Audit Frequency

Corporations go through continuous internal and external audits on an annual, quarterly or even monthly basis. DPM is a real-time reporting solution that tracks compliance across the storage and backup infrastructure and it's always up to date.

Changing Audit Requirements

No audit is the same and the auditor adds new compliance requirements every time constantly increasing the scope. Fortunately, a DPM solution can be easily configured to address the new changes without additional scripting.

Multiple Requests for the Same Information

Audits can drain resources as the IT team searches for the requested records—often multiple times for different auditors. A centralized DPM system provides controlled access to the auditor relieving the IT team from many of the manual compliance reporting tasks.

Development of Custom Scripts

Many companies must build custom scripts to perform reporting functions to meet audit requirements. This can be a time-consuming burden requiring teams of software developers. DPM can deliver automated reports, freeing up the IT team for more productive efforts.

Separation of Duties

IT team members who manage the backup process must be able to prove that they do not have access to go back into the system and modify core financial records. DPM solutions provide secure roles-based access to meta data without access to raw data, ensuring the necessary separation of duties.

Leveraging Data Protection Management Reports

The APTARE DPM solution provides a variety of reports to meet SOX compliance needs:

Web-based Compliance Dashboards

The IT team must be able to show the auditor how they are protecting the SOX servers. The auditor analyzes the team's ability to identify, respond to, and fix failures within the backup environment. The web-based Compliance Dashboard provides the end-to-end visibility across all SOX servers required to prove compliance with the capability to drill down into specific servers and files.

Data Protection SLA Status

The Data Protection SLA Status report enables the IT team to drill down into SOX servers, identify which files have been missed in the backup, and address the issues.

SLA Summary by Backup System

The SLA Summary enables the IT team to identify and correct issues with the backup system, such as false positives.

Application-Centric View

Auditors are interested in the applications and clients on the SOX servers because they can impact data. APTARE's Application-centric View allows the IT team to identify and fix application issues that may be causing backup problems or other data protection breaches.

Policy Audit Report

APTARE's Policy Audit Report tracks the company's change control process to ensure compliance policies are being maintained. For example, the retention period is a key variable on backup files. The retention period relates directly to compliance because regulations often stipulate that records must be kept for a specific number of years. Compliance violation could result if retention periods are set incorrectly. The Policy Audit Report enables the IT team to easily keep track of all retention periods and ensure they match the regulatory requirements.

Visit APTARE.com today to learn how you can efficiently and effectively meet compliance requirements.