Suggested URL for this landing page:
http://www.likewise.com/solutions/compliance/sox.php

Pls link to this page from
http://www.likewise.com/solutions/compliance/index.php

==========
METADATA

Title:
SOX Compliance for File Servers and Storage Systems

Description:
Likewise Data Analytics and Governance delivers SOX compliance by securing, monitoring, and auditing financial information on file servers and NAS systems.

Keywords:
SOX, Sarbanes-Oxley, SOX compliance, IT compliance, information security, unstructured data, storage NAS, file server

==========
H1:
SOX Compliance for File Servers and Storage Systems

H2 Subtitle:
Managing Unstructured Data for Sarbanes-Oxley

The requirements for SOX compliance represent something of a shifting goal. Instead of specific IT compliance requirements, Sarbanes-Oxley relies on general principles. Problem is, they are subject to interpretation by auditors. Different auditors might ask different questions; expectations might change from year to year; controls deemed adequate one year might be insufficient the next. So the key question becomes: How can you put in place internal controls that address different auditors, shifting objectives, and various risks?

A powerful approach is to implement internal controls that establish a strong foundation for Sarbanes-Oxley compliance. Such controls include authentication, access control, a monitoring system, auditing capabilities, and compliance reports. The business value of generalized controls represents a rapid return on investment:

*Improve SOX compliance.

*Protect the confidentiality, integrity, and availability of sensitive documents.

*Reduce the risk of noncompliance, security breeches, internal threats, fraud, and legal problems.

*Cut the costs of compliance, storage, and security.

==========

<h2>SOX Compliance Solutions for Mitigating Risk
</h2>
When it comes to SOX compliance, risk is the underlying factor that drives control objectives. It is the potential that a given threat, whether internal or external, will exploit the vulnerabilities of an asset to cause loss or damage to the asset. The severity of the risk is proportional to the business value of the potential loss and to the estimated frequency of the threat. To put it simply: What could go wrong? Sensitive data, for instance, could be stolen and your reputation could be damaged.

The risks that you face yield control objectives -- objectives that ultimately translate into internal controls. In fact, the fundamental principles of compliance are straightforward enough: establish internal controls and then enforce them, monitor their effectiveness, and report on them.

Likewise establishes the following generalized internal controls to secure, monitor, and audit unstructured data stored on file servers and network attached storage (NAS) systems:

*Cross-platform authentication that supports a single, unique identity for each user.

*Access control that authorizes users' access to servers and files.

*Monitoring to track who accesses and modifies what data at what time.

*Auditing capabilities for server access, file views, file changes, and various other events, including those from NetApp and EMC NAS systems.

*Reports, including templates tailored to help show the effectiveness of internal controls.

==========

<!-- these are h3s:: -->

User Authentication for File Servers and NAS Systems
Secure authentication is a best practice for Sarbanes-Oxley compliance. Likewise Storage Services communicates with Microsoft Active Directory or another user directory to authenticate users with a single, unique ID. For more information about Likewise authentication, see Likewise Storage Services.

Access Control for Unstructured Data
Firmly established identity and role-based authorization are essential to making informed access control decisions. The Likewise Storage Services platform controls access to sensitive resources stored on file servers and NAS systems by using Microsoft Active Directory or another directory service, such as LDAP. See Storage Access Control: Securing Access to Files Servers and NAS Storage.

Access Monitoring

One of the principles of SOX compliance is to monitor internal controls. Likewise includes several methods of monitoring controls to provide a solid foundation for dealing with annual audits. Likewise logs every server access attempt, file-view attempt, and file-change attempt and then centrally manages the event data. Likewise will, for example, monitor which users and groups have access to which storage systems. See Exception Monitoring and Reporting: Identity-Aware Exception Monitoring for Security and IT Compliance.

Content Monitoring

To comply with Section 404 of Sarbanes-Oxley, you must be able to demonstrate that important documents -- minutes of board meetings, financial reports, bank records, and so forth -- are genuine and have not been altered. Likewise lets you design and implement controls for content monitoring and chain of custody. See File Activity Monitoring: Tracking Unstructured Data for Security and Compliance.

Auditing Unstructured Information for IT Compliance

<!-- pls add link to the auditing white paper -->

Likewise can audit stored unstructured content in a security-aware context of user identities, patterns of access, and file change events. Auditing can detect potential sources of data loss, fraud, inappropriate entitlements, access attempts that should not occur, and a range of other anomalies that are indicators of risk -- especially when the audit associates data access with user identities. See Auditing Unstructured Data: Identity-Aware Storage, File Activity Monitoring, and Compliance Reporting Across Platforms.

Compliance Reports

Reporting can inspect access rights, show patterns of access and change, and double-check levels of protection -- all of which can help prove compliance with Sarbanes-Oxley. Likewise includes reports geared specifically for SOX so you can show auditors the effectiveness of your internal controls. See Reporting Features for IT Auditing and Compliance.

Compliance Dashboard

The Likewise dashboard lets you monitor storage servers and their log data in near real-time for authentication, authorization, file views, and file-change events, including the IP addresses of both clients and servers. Likewise accepts events and log data from NetApp, EMC NAS devices, and other storage systems. See Likewise Data Analytics and Governance.

==========
<!-- list of features is tailored for each page:: -->

Features

*Compliance reports for SOX
*Authentication and access control
*Access reports
*File modification reports
*Templates for custom reports
*Historical reports for auditing and forensics
*Chain of custody for data used in reports
*Dashboard with custom views
*Alerts for policy violations
*User activity monitoring
*Exception monitoring
*Event aggregation from NetApp and EMC NAS systems

==========