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

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

==========
METADATA

Title: FISMA Compliance for File Servers and Storage Systems

Description:
Likewise delivers FISMA compliance by implementing security controls that protect the confidentiality, availability, and integrity of stored data.

Keywords: FISMA, data storage compliance, information security, IT compliance, compliance security, unstructured data, storage NAS, file servers, continuous monitoring

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

H2 Subtitle:
Managing Unstructured Data for Information Security

FISMA mandates that you protect information and information systems to provide confidentiality, integrity, and availability. To do so, you must implement security controls.

Technical security controls for unstructured data stored on file servers and NAS systems take the form of authentication, access control, auditing, monitoring, and reporting.

<!-- these are all h3s I guess:: -->

Architecture for Continuous Monitoring

In the details of the regulations and in the emerging standards from the National Institute of Standards and Technology, there is the basis of an architecture for implementing security controls to protect unstructured data. Beyond authentication and access control, the architecture promulgates four basic functions, as specified by the Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST Special Publication 800-137):

<!-- verbatem quote: pls either offset or add quotes -->

<blockquote>The core requirements of an architecture implemented to support ISCM are data collection, data storage, data analysis capabilities, and retrieval and presentation (reporting) capabilities.
</blockquote>

Translated into the context of information stored on a file server or NAS system, the

requirements are as follows:

1. Collect and aggregate events.
2. Store events.
3. Provide methods to query and analyze events.
4. Create reports on events.

Security Events on Storage Systems

In the context of unstructured data stored on file servers and NAS systems, events are generally of three types:

1. Authentication requests and access attempts.

2. Attempts to view, modify, add, or delete directories and files.

2. Attempts to modify the security descriptors of files.

Likewise collects and stores these events and ties them to the identity of users. Collecting events and associating them with the identities of users goes beyond authentication and access control to cover several additional aspects of FISMA's information security requirements.

The Minimum Security Requirements for Federal Information and Information Systems, the document also know as FIPS 200, defines information security as follows:

<!-- this is a verbatim quote from above federal doc, so pls either offset somehow or enclose it in quotation marks. -->

<blockquote>The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.</blockquote>

Likewise Security Controls for File Servers and NAS Systems

Likewise software helps ensure the confidentiality, availability, and integrity of information in storage systems by implementing security controls that protect against unauthorized access, use, disclosure, disruption, modification, or destruction.

Specifically, Likewise cost-effectively puts in place the following security controls:

Monitoring: Likewise monitors attempts to access, modify, or delete directories and files. It also tracks attempts to change security descriptors. When monitoring can associate events, such as a denied attempt to delete a file, with a user's identity, it is a powerful security control: You can see who is attempting to take what action. Monitoring helps guard against fraudulent access, unauthorized use, disclosure, disruption, and destruction.

Authentication: Likewise securely authenticates users with either Microsoft Active

Directory or another user directory regardless of whether they are accessing storage from a Unix or Windows computer. Authentication protects systems against unauthorized access by making sure the person accessing the system is who they claim to be.

Access control: Likewise controls access to servers, directories, and files. Storage access control protects directories, files, and other resources from access, modification, or destruction by unauthorized personnel.

Auditing: Likewise collects and stores all access, modification, addition, and deletion events for directories and files so the events can be queried and analyzed later, whether for a security audit, forensics, or to fine-tune security policies.

Reporting: Likewise lets you create reports tailored to show that your security controls are working as designed.

For detailed information about the FISMA security requirements that Likewise addresses, see the Likewise FISMA Compliance for File Servers and Storage Fact Sheet.

The Business Value of Likewise

*Comply with a number of FISMA requirements and guidelines.

*Protect the confidentiality, integrity, and availability of unstructured data.

*Cost-effectively implement security controls that reduce the risk of security breeches, internal threats, and fraud.

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

Trusted by Federal Agencies

In the past, such government agencies as the U.S. Army, the U.S. Government Printing Office, and the U.S. Department of State have trusted Likewise technology for their security needs.

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

Features
*Continuous monitoring of storage systems
*Compliance reports for FISMA
*Access control and access reports
*File modification reports
*Templates for custom reports
*Historical reports for auditing and forensics

*Monitoring dashboard with custom views
*Alerts for policy violations
*User authentication
*Event aggregation from NetApp, EMC NAS systems, etc.