<!-- level 3 or level 4 web page for more about features and semantic support for higher level pages -->

<title>Reporting Features for IT Auditing and Compliance</title>

<meta name="description" content="The reporting features of Likewise associate file events with identities to audit unstructured data for security and compliance."/>

<meta name="keywords" content="IT auditing, file server reporting, compliance reports, access reports, audit unstructured data"/>
==========

<H1>Reporting Features for IT Auditing and Compliance</H1>

By integrating storage, identity, and security, Likewise gives you a panoramic vista from which you can look out across your files servers and see your unstructured data. Patterns of storing data and subsequently accessing it become visible. Security vulnerabilities are exposed so you can fix them. Reports are linked to the identity management system to show who accessed what. Compliance reports compile information to help you fulfill regulatory requirements.

<H2>Connecting File Server Events and User Identities</H2>

The auditing and reporting features of Likewise cull events related to storage and access to put the information that you need to manage the demands of network security and compliance at your fingertips.

The system records information about reading, moving, copying, modifying, or deleting directories or files on a file server. The events are linked to user identities so that you can see not just a change to a file but also who accessed the file and made the change.

Monitoring events such as failed attempts to access a file can help prevent unauthorized access to sensitive resources, a safeguard required by several compliance regulations.

Monitoring attempts to delete files can help preserve important information, ensuring compliance with, for example, the technical safeguards of section 164.312 of HIPAA, a rule of which reads:

<!-- this is a quote from the hipaa law: -->
<blockquote>Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</blockquote>

<H2>Reporting Features</H2>

Likewise includes reports that are based on the following features:

<!--TK LATER WHEN WE HAVE UI -->

<!--PLS BOLD EACH LEDE-IN THROUGH PERIOD.-->

*Identity. The reports that are tied to identity information from your identity management systems.

*Access. The reports are based on user or group access to file servers, shares, directories, and files.

*Events. The reports present information about reading, moving, copying, modifying, or deleting directories or files on a file server.

*Exception-based management. The reports can display exceptions to reveal a security threat or an incident of noncompliance.

*Sensitivity-based tracking. You can mark content as sensitive and then generate reports that show changes to the tracked files, such as modifications of content or security descriptors as well as attempts to delete files or content.

*Compliance tagging. The tagging lets you prepare reports for regulatory audits, including reports for SOX, PCI DSS, and HIPAA.

*Variety. There are a variety of reports, including templates to help comply with the PCI DSS, SOX, ITAR, FISMA, and HIPAA.

*Categories. You can also choose from categories of reports, including access reports, user activity reports, compliance reports, file-change reports, and driver-state reports.

*Custom queries. Templates serve as a starting point to create your own reports to fulfill a diverse set of reporting requirements, whether for external regulations or internal policies.

*Security-aware context. When identity, access, content, and events are tracked at the file server, reports are enriched by contextualized security data -- the correlations that take place at the intersection of users with known roles and entitlements accessing tracked content to perform logged events. The reports provide a visual representation of the security context.

<!--TK LATER WHEN WE HAVE UI
Here's a sample report showing that a file server driver was loaded successfully:
-->

<h2>SQL Server Options </h2>
Reporting data is stored in an Microsoft SQL Server database and can be accessed either on demand or periodically by a set schedule. The SQL Server options available with Likewise are easy to use and adaptable to your needs. If you already own a SQL Server enterprise license, you can easily create a Likewise database by running a Likewise script that formats a SQL Server database instance. If you do not have a SQL server, you can install SQL Server Express, a free version of SQL Server.