Sarbanes-Oxley Compliance

Sections 302 and 404

FILECLOUD
WWW.GETFILECLOUD.COM

Note: This white paper is intended to provide an overview and is not intended to provide legal advice. For more comprehensive information on regulations and their implications, please consult your legal counsel.

Sarbanes-Oxley Compliance

Section 302 and 404

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration (previously known as Enterprise Sharing and Sync - EFSS) platforms to implement document workflows and improve collaboration and productivity.

Strategic Assumption in Gartner's Magic Quadrant for Content Collaboration 2018

For the Third Consecutive Year, Gartner Peer Insights Recognizes CodeLathe's FileCloud as "Voice of the Customer" CCP Customers' Choice

The Sarbanes-Oxley Act came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice, including a number of non-negotiable deadlines for compliance.

The Sarbanes-Oxley Act is arranged into eleven 'titles.' As far as compliance is concerned, the most important sections within these eleven titles are usually considered to be 302, 401, 404, 409, 802 and 906.

Section 302 requires periodic statutory financial reports to include certifications that:

- The signing officers have reviewed the report.
- The report does not contain any material untrue statements or include material omissions that make the report misleading.
- The financial statements and related information fairly present the financial condition and the results in all material respects.
- The signing officers are responsible for internal controls and have evaluated these internal controls within the previous ninety days and have reported on their findings.
- The report lists all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities.
- Any significant changes in internal controls or related factors that could have a negative impact on the internal controls.

Section 404 requires issuers to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement must also assess the effectiveness of such internal controls and procedures.

The registered accounting firm must, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.

Sarbanes-Oxley Act Section 302. Sarbanes Oxley 302 Made Easier. (soxlaw.com)

Sarbanes-Oxley Act Section 404. Sarbanes Oxley 404 Made Easier. (soxlaw.com)

Section	SOX Section 302 Corporate Responsibility for Financial Reports	FileCloud Server	FileCloud Online
Establish safeguards to prevent data tampering			
Section 302.2	Implement a ERP system or GRC software that tracks user logins access to all computers that contain sensitive data and detects break-in attempts to computers, databases, fixed and removable storage, and websites.	**Not Applicable**	**Not Applicable**
Establish safeguards to establish timelines.			
Section 302.3	Implement an ERP system or GRC software that timestamps all data as it is received in real-time. This data should be stored at a remote location as soon as it is received, thereby preventing data alteration or loss. In addition, log information should be moved to a secure location and an encrypted MD5 checksum created, thereby preventing any tampering.	**Yes**	**Not Applicable**
Establish verifiable controls to track data access.			
Section 302.4.B	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**Yes (FTP not supported)**	**Yes (FTP not supported)**
Ensure that safeguards are operational			
Section 302.4.C	Implement an ERP system or GRC software that can issue daily reports to e-mail addresses and distribute reports via RSS, making it easy to verify that the system is up and running from any location.	**Yes**	**Yes**
Periodically report the effectiveness of safeguards.			
Section 302.4.D	Implement an ERP system or GRC software that generates multiple types of reports, including a report on all messages, critical messages, alerts and uses a ticketing system that archives what security problems and activities have occurred.	**Yes**	**Yes**
Detect Security Breaches.			
Section 302.5.A/B	Implement an ERP system or GRC software that performs semantic analysis of messages in real-time and uses correlation threads, counters, alerts, and triggers that refine and reduce incoming messages into high-level alerts. These alert then generate tickets that list the security breach, send out email, or update an incident management system.	**Yes**	**Yes**

Section	SOX Section 404 Management Assessment of Internal Controls	FileCloud Server	FileCloud Online
Disclose security safeguards to SOX auditors			
Section 404.A.1.1	Implement an ERP system or GRC software that provides access to auditors using role-based permissions. Auditors may be permitted complete access to specific reports and facilities without the ability to actually make changes to these components or reconfigure the system.	**Yes**	**Yes**
Disclose security breaches to SOX auditors.			
Section 404.A.2	Implement an ERP system or GRC software capable of detecting and logging security breaches, notifying security personnel in real-time, and permitting resolution to security incidents to be entered and stored. All input messages are continuously correlated to create tickets that record security breaches and other events.	**Yes**	**Yes**
Disclose failures of security safeguards to SOX auditors.			
Section 404.B	Implement an ERP system or GRC software that periodically tests network and file integrity, and verifies that messages are logged. Ideally the system interfaces with common security test software and port scanners to verify that the system is successfully monitoring IT security.	**Yes**	**Yes**

FileCloud - Helpful Documentation

- Audit Logs
- Private Share Permissions for Folders
- Workflow
- Custom Reports
- Centralized Device Management
- Retention Policies
- Smart DLP
- Smart Classification
- Security
- Notifications
- FileCloud Alerts
- Storage Encryption
- SIEM Integration
- File Content Heuristic Engine

FileCloud is used by 1000s of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers.

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support"

Stewart

About Us

FileCloud Server is the commercial of the shelf software solution that helps businesses to securely share, manage, and govern enterprise content. FileCloud software provides the necessary capabilities for organizations to obtain compliance in SOX.

The end-user is responsible for utilizing suitable FileCloud capabilities as well as managing and maintaining the environment where FileCloud is being hosted to ensure the SOX requirements are being met.

FileCloud aids with your SOX compliance efforts under the shared responsibility model.

13785 Research Blvd,
Suite 125 Austin TX
78750

Email: sales@codelathe.com

Website: www.getfilecloud.com

Phone: +1 (888) 571-6480

Fax: +1 (866) 824-9584