Voluntary Product Compliance Statement

Compliance Statement for Sarbanes-Oxley Act (SOX) of 2002

Collabware CLM 2016

Table of Contents

Voluntary Product Compliance Statement

The Sarbanes–Oxley Act of 2002 is a United States federal law that requires all publicly held companies to establish internal controls and procedures for financial reporting to reduce the possibility of corporate fraud. There are also a number of provisions of the Act that also apply to privately held companies, for example the willful destruction of evidence to impede a Federal investigation.

The bill contains eleven sections that cover responsibilities of a corporation's board of directors, defines criminal penalties for misconduct, outlines disclosure rules, audit procedures etc. Compliance with the act is an organizational responsibility to ensure the necessary financial, accounting, business processes and accountabilities are enacted.

While there is no SOX certification for software, the following sections describe how Collabware provides direct support for the SOX requirements for fraud reduction, policy enforcement, and compliance auditing when SharePoint and Collabware CLM are the system of record for documents.

Date	05 May 2016
Name of Product	Collabware CLM 2016
Contact for more Information	contact@collabware.com

Summary

The Sarbanes–Oxley Act of 2002 contains the eleven sections. However, the sections that are specifically relevant for document and records management are:

Section	Topic
Sarbanes-Oxley Section 103	Auditing, quality control, and independence standards and rules
Sarbanes-Oxley Section 404	Management Assessment of Internal Controls
Sarbanes-Oxley Section 802	Criminal Penalties for Altering Documents

Within the Act, and specifically noted in the above sections, key requirements of the act where Collabware CLM can benefit customers include:

- Minimum preservation and retention requirements for specific types of documents
- Discovery and legal holds
- Access control
- Auditing

The following sections describe how Collabware CLM supports these key requirements.

Minimum Preservation and Retention Requirements

SOX Section 802, clause 1519 describes criminal penalties for altering documents. In addition, the section clause 1520 requires all audit and review work papers must be kept for 5 years from the end of the fiscal period in which the audit or review was concluded.

SOX Section 103, clause 2 relates to auditing firms and requires firms to maintain for a period of not less than 7 years, audit work papers and other information related to any audit report, in sufficient detail to support the conclusions reached in such a report.

Collabware CLM will preserve and protect records according to retention policies defined by your organization. Corporate records managers would define a file plan and retention policies in Collabware CLM. All audit and review working papers are classified to the file plan and the appropriate preservation and retention policy come into effect automatically. Collabware CLM provides automated 'content rules' that will automatically classify documents to the correct record classification ensuring that all audit and review working papers are properly classified and come under the correct compliance control.

Once classified to the file plan, Collabware CLM preserves the documents by issuing a SharePoint lock on the item when it is declared a record. The declare process will not only prevent the record from being deleted, but will also make the document immutable and prevent a document and it's metadata from being deleted, updated, or altered in any way. In addition, Collabware CLM prevents the deletion of any sites or libraries that contain declared records, ensuring that the records are properly preserved.

In the event that an update is required to correct a metadata value or a document has been declared a record in error, authorized records managers may undeclare the record, make the necessary change and declare the document as a record again. Versions of the document update are maintained, and a full audit of who, when and what was done to the document is logged in the Collabware CLM audit database.

At the completion of the records retention lifecycle, Collabware CLM provides an audited disposition review and approval process. The disposition review steps are logged and tracked and when approval for destruction is given, the documents are destroyed and a destruction certificate is created to provide evidence of the destruction according to established and approved corporate disposition policies.

Discovery and Legal Holds

SOX Section 802, clause 1519 describes criminal penalties for altering or destroying documents with the intention of impeding or obstructing an investigation. An effective legal hold process will help prevent such misconduct.

In the event of a discovery, investigation or legal action, documents and records in SharePoint, related to the discovery, must be identified. Those documents and records must be preserved and protected from deletion or alteration while under a legal hold.

Collabware CLM provides a powerful Legal Hold system to ensure that content is protected and cannot be modified or used in a disposition process while on hold. Content can easily be added to a hold individually, in bulk, or automatically using advanced rules. Authorized users can view hold information on individual content.

The creation of the legal hold, the addition of documents and records to the log and release events are all logged and tracked in the Collabware CLM audit database for complete accountability.

In the event that documents requested by a legal hold are already destroyed, Collabware CLM provides a destruction certificate for all records destroyed through the normal disposition process (if the records were not part of a legal hold). The destruction certificate lists the complete history of the disposition approval process (date/time, users, comments), the approved retention policy authorizing the disposition and details of the record that was destroyed, allowing for evidence of defensible destruction.

Access Control

SOX does not specifically outline security and access control as part of the act, however, it does describe what obligations an organization is under in order to be complaint. Section 404(a) requires 'establishing and maintaining an adequate internal control structure and procedures for financial reporting'.

The financial reporting working papers, spreadsheets, emails and other materials used in the preparation and production of the financial reports, including the financial reports themselves, must be protected. If SharePoint is used to store any of this information, Collabware CLM can help manage the access controls.

Collabware CLM provides Access Control Lists (ACL's) for organizations to create specific groups of users and privileges. The ACLs utilize SharePoint security and Active Directory groups and users to manage its members. Through ACLs, organizations can control user access to documents, records, sites and record center repositories.

Auditing

In the event of an audit or investigation, a full audit log of activity against documents and records is critical.

Collabware CLM tracks and logs all audit activities performed against all content in a centralized multi-dimensional data warehouse. Authorized users can generate dynamic reports based on audit activities and export the results in Excel format for post-processing. The audit database is also available for customers to view themselves using standard SQL query tools.

Collabware CLM audits:

- All activity performed against all content in SharePoint
- All activities related to a review process, including a destruction approval
- All activities related to a retention schedule

The audit information is retained in the audit database even after the original record has been destroyed.

The Collabware CLM audit features and capabilities empower organizations to track the full chain of custody of documents and records, helping to prevent misuse in the first place and providing audit teams complete information to complete detailed investigations.

Disclaimer

This document is for informational purposes only. Collabware makes no warranties, expressed or implied, in this document.

The information contained in this document represents the current view of Collabware on the issues discussed as of the date of publication. Because Collabware must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Collabware, and Collabware cannot guarantee the accuracy of any information presented after the date of publication.

Collabware regularly updates its websites and provides new information about the adherence to industry standards as that information becomes available.