CloudLock

Compliance and Data Governance for Google Docs

Table of Contents

Regulatory Compliance and Data Governance For Google Docs

Compliance regulations such as SOX, HIPAA, FISMA and internal audits performed as part of a risk assessment, are stressful events to any IT organization. When It comes to understanding the relevance of these regulations on sensitive data, it can be boiled down to a simple notion: Proving the IT organization has visibility AND control into the data environment that ensures that only the right people have access to sensitive data stored on Google Docs.

Gaining this type of visibility requires assessing the IT organization's capability of answering a few key questions:

- What data do I have?
- Who has access to what?
- What is accessible to whom?
- How did access rights to sensitive data change at different points in time?
- What do privileged users do with data?

Compliance Regulations And Google Docs

In the following whitepaper, we'll review some of the most commonly applied compliance regulations and will show how companies can enjoy the cost savings and collaboration benefits of Google Docs while maintaining compliance with regulatory requirements and internal data governance best practices.

We will specifically discuss HIPAA, FERPA, FISMA, PCI DSS, PCI Compensating Controls, and Sarbanes-Oxley (SOX). For each regulation, we will discuss the challenges facing companies storing data in the cloud, and how CloudLock can help.

HIPAA Compliance For Google Docs

"CloudLock for Google Docs not only puts our cloud data governance on-par with that of our on-premise data; it actually puts us in a better place.

Having the capabilities to quickly identify data exposures and fix them immediately are the kinds of key IT controls every organization needs."

Hilary Croach,
CIO,
Bay Cove Human Services

CASE STUDY

For an example of a company using Google Docs while complying with HIPAA, see "Bay Cove Human Services selects CloudLock for Google Docs to gain visibility and control of their corporate data stored on Google Docs"

Google Docs HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in August 1996, placing new requirements on thousands of U.S. organizations involved with the provision of health care. The purpose of HIPAA regulations is to protect health information that identifies an individual and is maintained or exchanged electronically.

HIPAA consists of the following 2 rules:

- **Security Rule** – specifies a series of administrative, physical, and technical safeguards for covered entities to use in order to assure the confidentiality, integrity, and availability of electronic protected health information.
- **Privacy Rule** - addresses the use and disclosure of individuals' health information. It permits the disclosure of personal health information needed for patient care and other important purposes.

Organizations that must comply with HIPAA:

- **Health Plans** – individual and group plans that provide or pay the cost of medical care (e.g. HMOs, group health plans etc.)
- **Health Care Providers** – every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions (e.g., institutional providers such as hospitals and non-institutional providers such as physicians, dentists and other practitioners)
- **All Health Care Clearinghouses** (billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions).

Challenges

All HIPAA compliant organizations must take steps to prevent inappropriate access to EPHI (Electronic Protected Health Information) by putting into place both proactive and reactive controls over IT systems. This also applied to document stored in the cloud, including data stored in Google Apps.

CloudLock

HIPAA Compliance For Google Docs

Google Docs HIPAA Compliance

HIPAA Compliance in Google Apps and CloudLock

CloudLock can help organizations meet the following HIPAA requirements:

HIPAA Requirements	Action Required	CloudLock Feature
Security Management Process 164.308(a)(1)	Review permission settings and correct access rights	CloudLock for Google Apps provides domain administrators full visibility into all document access rights and exposure levels. Alerts on new exposures and permission changes are generated on a daily basis
Workforce Security 164.308(a)(3)	Ensure that only authorized workforce members have access to Electronic Protected Health Information	Audit documents and users to ensure that permission rights and sharing settings comply with the regulatory requirements
Information Access Management 164.308(a)(4)	Implement policies and procedures for accessing Electronic Protected Health Information	Receive alerts on new exposures and permissions changes and make sure they comply with the policies
Access Control 164.312(a)(1)	Allow access only to the authorized workforce	Domain administrators can review and fix document access rights to enforce the correct access controls. Permissions can be changed by admins who are not collaborators on the documents.
Audit Controls 164.312(b)	Record and examine activities for Electronic Protected Health Information	CloudLock provides tamper-proof audit logs with all admin activities and changes for audit purposes. The audit log contains all the activities performed by the admin(s) or the end users who are authorized to use CloudLock
Documentation 164.316(b)(1)	Record all activities	Full document history includes all the permission changes in any given document. All the admin activities are automatically recorded in the audit log

FERPA Compliance For Google Docs

Google Docs FERPA Compliance

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

The act has 2 main aspects, ensuring that students can access their educational records while maintaining the privacy of those records:

- **Providing students with access to their educational data** – parents or eligible students have the right to inspect and review the student's education records maintained by the school.
- **Privacy policy** – schools must have written permission from the parent or eligible student (with certain exceptions) in order to release any information from a student's education record.

"Now that I have CloudLock for Google Apps, I can delegate tasks to the security team and designated data owners, and can make sure that we are in control of our data - both for meeting data privacy regulations and following data governance best practices."

Brian Bolt,
Systems Engineering Team Lead,
Boise State University

Challenges

With the transition of many schools and universities to Google Apps and the adoption of Google Docs, student educational records are now being stored in the cloud. The same FERPA guidelines apply both on-premise and in the cloud, and require the IT staff of these institutions to maintain adequate access controls to ensure that student records are not exposed.

Meeting FERPA Requirements In Google Docs with CloudLock:

FERPA Requirement	Action Required	CloudLock Feature
Privacy Policy - student educational records should not be public and can be released only with authorization.	Review permission settings and correct access rights	CloudLock provides a full audit of all documents in the domain and their access rights. Domain administrators can notify document owners of document exposure or excessive permissions. They can also correct and change the access rights (even on documents they are not collaborating on). CloudLock's ongoing monitoring and alerting capabilities automatically notify on any changes to access rights and let IT ensure that documents do not become exposed mistakenly.

CASE STUDY

For an example of a company using Google Docs while complying with FERPA, see "Boise State University selects CloudLock for Google Apps to comply with FERPA and other data privacy regulations."

CloudLock

FISMA Compliance For Google Docs

Google Docs FISMA Compliance

The Federal Information Security Management Act is a United States federal law enacted in 2002 and imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government agency or by a contractor or other organization on behalf of a US Government agency.

The act recognizes the importance of information security and requires each federal agency to develop, document and implement programs that ensure integrity, confidentiality and availability of information and information systems. The act applies to the information and information systems that support the operations and assets of the agency, including those provided or managed by another agencies or contractors.

Whether documents are stored on-premise or in Google Docs, they require the same level of protection and control. Federal agencies must not only focus on security but they also need to demonstrate that they are compliant with both agency and congressional mandates.

Challenges

FISMA compliance requires ongoing evaluation and remediation of risks, including ongoing reporting and monitoring of the documents stored in the Google Docs. To verify and monitor compliance for documents stored in the cloud, IT must have the right tools in place. They must do so for all the documents in the domain (including the documents they are not collaborating on).

CloudLock

FISMA Compliance For Google Docs

Google Docs FISMA Compliance

CloudLock can help organizations meet the following FISMA requirements:

FISMA Requirements	Action Required	CloudLock Feature
Categorize information and information systems according to risk level NIST SP 800-60 and FIPS PUB 199	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	CloudLock provides a complete access management system with reporting on user access rights for each document in the domain. This is supported by an automatic discovery of all the documents and the users in the Google Apps domain. With CloudLock, IT has visibility and control of access rights on all documents in the domain (even those they are not collaborating on). CloudLock's dashboard provides document classification by access and exposure levels, providing a quick drill-through to view documents and collaborators.
Security controls and risk assessment NIST SP 800-53 and FIPS 200	Assess security to identify risks and to evaluate existing controls. Organizations must meet minimum security requirements by selecting the appropriate security controls and assurance requirements. A risk assessment is done by identifying potential threats and vulnerabilities and mapping implemented controls to individual vulnerabilities	CloudLock enables IT admins to audit access rights to all documents in the domain. With CloudLock, IT can enforce access controls by changing/ fixing permissions on documents thus reducing the security risks by assigning the proper access rights. All changes are tracked in a tamper proof audit log.
Continuous monitoring	Monitor security controls	CloudLock provides IT with an ongoing monitoring and alerting for all documents in the domain. Changes on access rights and new exposures are sent in a daily report. This ensures that documents do not become exposed mistakenly and give IT continuous and effective monitoring of existing and newly created documents.

CloudLock

PCI DSS Compliance For Google Docs

Google Docs PCI DSS Compliance

PCI compliance rules require organizations that handle bank cards to comply with security standards and follow certain leveled requirements to protect the private information of bank card holders during any transaction. The Payment Card Industry regulation also requires certified auditing procedures.

The standard was developed and backed by the major five payment brands (Master Card, Visa, American Express, Discover and JCB), and provides 12 high level requirements for securing cardholder data. The goal is to establish, maintain and guarantee that cardholder information remains secure. All merchants and service providers who store, process and transmit credit card information must comply with PCI.

Challenges

PCI requires that organizations secure all information related to cardholders regardless of the location of the data. This means that IT is challenged with implementing the appropriate measures and controls to ensure that proper access controls are implemented and audited on an ongoing basis.

PCI Requirements	Action Required	CloudLock Feature
Requirement #7 - Restrict access to cardholder data by a business on a need-to-know basis	Proper access controls should be put in place for all relevant data stored in Google Docs	CloudLock for Google Apps provides IT with visibility and control of access rights to all documents in the domain (even those they are not collaborating on). CloudLock also gives IT the ability to enforce access controls by changing and fixing permissions on these documents. All changes are tracked in a tamper proof audit log
Requirement #8.5 - Identify dormant user access rights	Remove dormant users from the domain while maintaining the documents they own	Reassign document ownership in bulk from users that have left the company. This CloudLock feature allows easy transfer of document ownership. Once the document ownership is transferred, users can be removed from the domain
Requirement #11.5 - Audit and alert on access rights changes	Ongoing verification and control of access rights	CloudLock provides ongoing monitoring and alerting of any change to access rights. Each document contains a full history of all permissions changes. All the permissions changes performed by IT admins are also logged.

CloudLock

PCI Compensating Controls For Google Docs

Google Docs PCI Compensating Controls

For organizations that are unable to comply with the PCI DSS requirements as they are written, the PCI Security Standards Council (SSC) has provided a way to meet these requirements through the documentation of compensating controls.

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement but has sufficiently mitigated the associated risk. According to CS Magazine forty-one percent of merchants are relying on compensating controls to meet PCI DSS requirements

With compensating controls, it's important to have a clear understanding of the specific PCI requirement and its intent. This helps organizations recognize how the requirement affects them so they can work towards minimizing risks, and is considered to be a viable path to compliance.

PCI compensating controls require a significant amount of examination and process. When properly designed and maintained, these controls become another way for organizations to achieve and maintain PCI compliance.

Criteria for compensating controls

As defined by PCI DSS, for a compensating control to be valid, it must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements).
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Compensating controls can be used for almost all the PCI requirements. A proper implementation of compensating controls consist of the following steps:

Step	Information Required
Constraints	List the constraints that preclude compliance with the original PCI requirement
Objectives	Understand the objectives of the original controls and identify the objectives met by implementing the Compensating Controls
Risk	Identify any additional risks associated by not implementing the original PCI requirements
Definition	Define the relevant compensating control and explain how it addresses the objectives and the increased risk (if any) of not implementing the original PCI requirements
Implementation	Validate that the compensating controls were implemented and tested
Maintenance	Define the process to maintain the compensating controls over time

Compensating controls are temporary solutions for compliance gaps that should be assessed annually to ensure that they meet the four criteria listed above. They may help companies lower the bar of compliance in the short term. These however, are not shortcuts to compliance and in many cases they are harder to implement and cost more money in the long run than actually addressing the compliance requirement

Compliance With PCI Compensating Controls For Google Docs

For organizations that choose to implement compensating controls for PCI compliance with Google Docs, CloudLock can help by providing IT:

- Visibility and control of access rights for all documents in the domain (even those they are not collaborating on).
- The ability to enforce access controls by changing and fixing permissions on all documents in the domain. All changes are tracked in a tamper proof audit log.
- The ability to reassign document ownership in bulk from users that have left the company. Once the document's ownership is transferred, users can be removed from the domain.
- Ongoing monitoring and alerting of any change to access rights with a full history of all permissions changes for all documents in the domain. All permissions changes performed by IT admins are also logged

CloudLock

Sarbanes-Oxley (SOX) Compliance For Google Docs

Google Docs SOX Compliance

The Sarbanes–Oxley Act of 2002 also known as the 'Public Company Accounting Reform and Investor Protection Act' and 'Corporate and Auditing Accountability and Responsibility Act' applies to all us public companies (large and small), public accounting firms and firms providing auditing services.

The bill was enacted as a reaction to a number of major corporate and accounting scandals(including those affecting Enron and Tyco International). Although SOX does not apply to privately held companies, those considering or planning for an IPO must demonstrate SOX compliance readiness.

The following 2 sections of SOX have a compliance impact on IT:

- **Sarbanes–Oxley Section 302**: Disclosure controls – requires that the company's principal officers (typically the Chief Executive Officer and Chief Financial Officer) certify and approve the integrity of their company financial reports quarterly. Internal access controls should be developed, implemented and reviewed periodically.
- **Sarbanes–Oxley Section 404**: Assessment of internal controls – requires management and external auditors to report on internal controls. Access controls should be maintained, reviewed and reported periodically.

Challenges

With the transition to the cloud and companies storing documents in the Google Docs, the same internal data control requirements must be followed in a cloud file system. IT therefore is tasked with implementing technical controls and continuous access auditing to assure the reliability of data related to financial transactions in Google Docs.

Effective implementation of SOX control processes requires making them repeatable. Automation reduces the amount of resources required to maintain on-going SOX compliance and can provide a positive return on investment.

CloudLock

Sarbanes-Oxley (SOX) Compliance For Google Docs

SOX Compliance in Google Apps and CloudLock

CloudLock for Google Apps can be used as an effective tool to facilitate SOX compliance with Google Docs. It provides a comprehensive system to meet the requirements of SOX sections 302 and 404 for documents stored in Google Docs.

SOX Requirements	Action Required	CloudLock Feature
Section 302 - Disclosure Controls	Report on access controls and asses risk. To comply with SOX, management must have a clear understanding of who owns and who is authorized to access financial documents.	CloudLock provides a complete access management system with reporting on user access rights for each document in the domain. This is supported by automatic discovery of all the documents and users in the domain and classification of documents by access and exposure levels. CloudLock supports review and approval processes to make sure only authorized users can access sensitive financial documents.
Section 302 - Disclosure Controls	Audit and report on all access rights and changes in access permissions to regulated data stored in Google docs. SOX requires organizations to provide ongoing evidence that they are compliant.	CloudLock provides ongoing monitoring of all the documents in the domain. A daily change report for each document details changes in ownership, collaborators and permissions.
Section 404 - Assessment of Internal Controls	Implement access controls to limit user rights based on a need-to-know basis. Identify users with excessive rights to protect financial data from unauthorized activities.	CloudLock provides IT with the visibility and control to all the documents in the Google Apps domain without the need to be shared on these documents. IT can easily secure access rights to financial documents according to company policy, and can transfer document ownership in bulk without manually logging into accounts.
Section 404 - Assessment of Internal Controls	All activities should be reported for auditing and to support forensic investigation.	A complete change report is available for every document. Alerts and email notifications are generated for permission changes and new exposures. All admin activities and changes are reported in a tamper-proof audit trail.
Section 404 - Assessment of Internal Controls	Separation of duties and enable for auditor independence.	Sox auditors can be delegated access to CloudLock to review the access rights to all financial documents. This is done without making them domain administrators or collaborators on these documents.
Section 404 - Assessment of Internal Controls	Organizations must be able to prove that they have accurate and reliable compliance behavior at all times.	CloudLock Vault is a secure, authenticated & tamper-proof digital data vault built on top of Google Docs. Once documents are stored in the vault, they cannot be deleted or modified.

About CloudLock

Regulatory Compliance and Auditing: Data Governance For Google Docs

Whether companies need to prove regulatory compliance (HIPAA, FISMA, SOX, PCI DSS, etc.) or need to follow internal data governance procedures, CloudLock is the only enterprise data protection application for Google Docs. To implement data governance and compliance initiatives in Google Docs, companies need the ability to answer:

- What data do I have?
- Who has access to what?
- What is accessible to whom?
- How did access rights to sensitive data change at different points in time?
- What do privileged users do with data?

Secure Your Google Docs While Saving Time

With CloudLock, you can put Google Docs security on autopilot with scheduled scans, alerts, change history and a full audit trail. Use CloudLock's end-user enablement feature to delegate sharing responsibility to data owners and get automated emails when sensitive data permissions change.

CONTACT US:
For further information about the company and CloudLock for Google Apps, call (781) 996-4332 or visit www.cloudlock.com

About CloudLock

Headquartered in Waltham, Mass., CloudLock is the cloud data protection company that enables control of data while gaining the collaboration and cost savings benefits of the cloud. Unlike expensive custom solutions, CloudLock's enterprise-class products are directly integrated with cloud application providers and are immediately available at a fraction of the cost. For further information about the company and CloudLock for Google Apps, call (781) 996-4332 or visit http://www.cloudlock.com