CloudLock

FISMA Compliance for Cloud Applications

What Is FISMA?

The Federal Information Security Management Act (FISMA) is a United States legislation signed in 2002 to underline the importance of information security to the economic and national security interests of the United States.

FISMA requires federal agencies to develop, document, and implement an information security program to safeguard their information systems including those provided or managed by another agency, contractor, or another third party.

Who Should Care

All government agencies, government contractors, and organizations that exchange data directly with government systems must be FISMA compliant. This may include such diverse entities as data clearinghouses, state government departments, and government military subcontractors in cases where data is exchanged directly with Federal government systems.

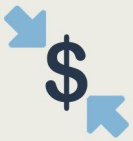
Individuals with the following roles are responsible for FISMA compliance: Agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general.

Why Comply?

FISMA holds federal agencies accountable to secure government information. Failure to pass a FISMA inspection can result in:

Significant administrative sanctions

Unfavorable Publicity



Reduction of IT budget

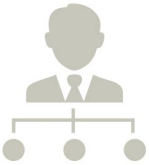
The FISMA Compliance Framework: Defined

- The FISMA Implementation Project of NIST, the National Institute of Standards and Technology, develops and maintains a whole set of standards and guidelines to which IT federal systems must adhere.

The key publications for FISMA are:

- FIPS Publication 199, standard for Security Categorization of Federal Information and Information System is the first of two mandatory security standards required by the FISMA legislation. It requires entities subjected to FISMA to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.
- FIPS Publication 200, Minimum security requirements for information and information systems is the second of the mandatory security standards. It specifies minimum security requirements for information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.
- The last key publication for FISMA, the NIST SP 800-53. Recommended Security Controls for Federal Information Systems and Organizations, describes in details the security controls with the designated impact levels of the organizational information systems.

The security requirements and controls cover seventeen security-related areas that addresses the management, operational, and technical aspects of protecting federal information and information systems.



Management

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Complying with FISMA

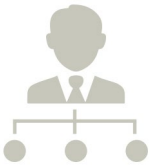
To comply with the federal standard, organizations must:

1. Determine the security category of their information system in accordance with FIPS 199.
2. Derive the information system impact level from the security category in accordance with FIPS 200.
3. Select and apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53. Organizations have flexibility in applying the baseline security controls in accordance to their mission, business requirements and environments of operation.
4. Conduct annual reviews of the information security program and report the results to Department of Homeland Security (DHS).

CloudLock Security Fabric
Supports Your FISMA Compliance in the Cloud

Meeting internal or external compliance regulations can be a tremendous challenge for any IT organization using software as a service (SaaS) applications. CloudLock provides the visibility and control you need to quickly detect and respond to risks of data that is sensitive, toxic, and/or subject to FISMA regulation, while confidently working in the cloud.

CloudLock's cloud security solution helps government agencies, government contractors, and organizations that exchange data directly with government systems achieving FISMA compliance for the following security-controls:



Management

Certification, Accreditation, and Security Assessments (CA)

- Leverage out-of-the box security and compliance reports to meet regulatory requirements with internal and external auditors.
- Use audited data as evidence of compliance to regulations and internal policies.

Operational

Awareness and Training (AT)

- Notify and educate users to encrypt sensitive information based on policy violations of over shared or inappropriately stored data

Incident Response (IR)

- Centrally manage all incidents based on unified policies.
- Investigate flagged content and potentially toxic data in files and documents.
- Easily view and filter incidents based on severity level, object type, cloud app, status, date and other criteria.

- Prioritize and track incidents based on business impact to your organization.
- Create incident reports.
- Automate response actions and notifications to your end users with CloudLock's fully automated remediation management capabilities.
- Integrate CloudLock's incident management service with your own enterprise systems, e.g. IT support and SIEM solutions.

Technical

Incident Response (IR)

- Enforce proper access controls for all relevant apps and data in the cloud.
- Provide ongoing verification and control of access rights.
- Protect your organization from malicious data extraction.

Identification and Authentication (IA)

- Monitor access to your cloud apps and associated data.
- Control and track addition, deletion and modification of users.
- Track inactive accounts.

Audit and Accountability (AU)

- Monitor user activity to detect potential anomalies and significant changes.
- Create alerts and incidents based on suspicious logins.
- Track user access of privileged user changes and change permission history.
- Feed time-sensitive and critical security events into your company-wide SIEM solutions for a consolidated security view.
- Gain real-time insight into the health of your public cloud applications in one unified dashboard.

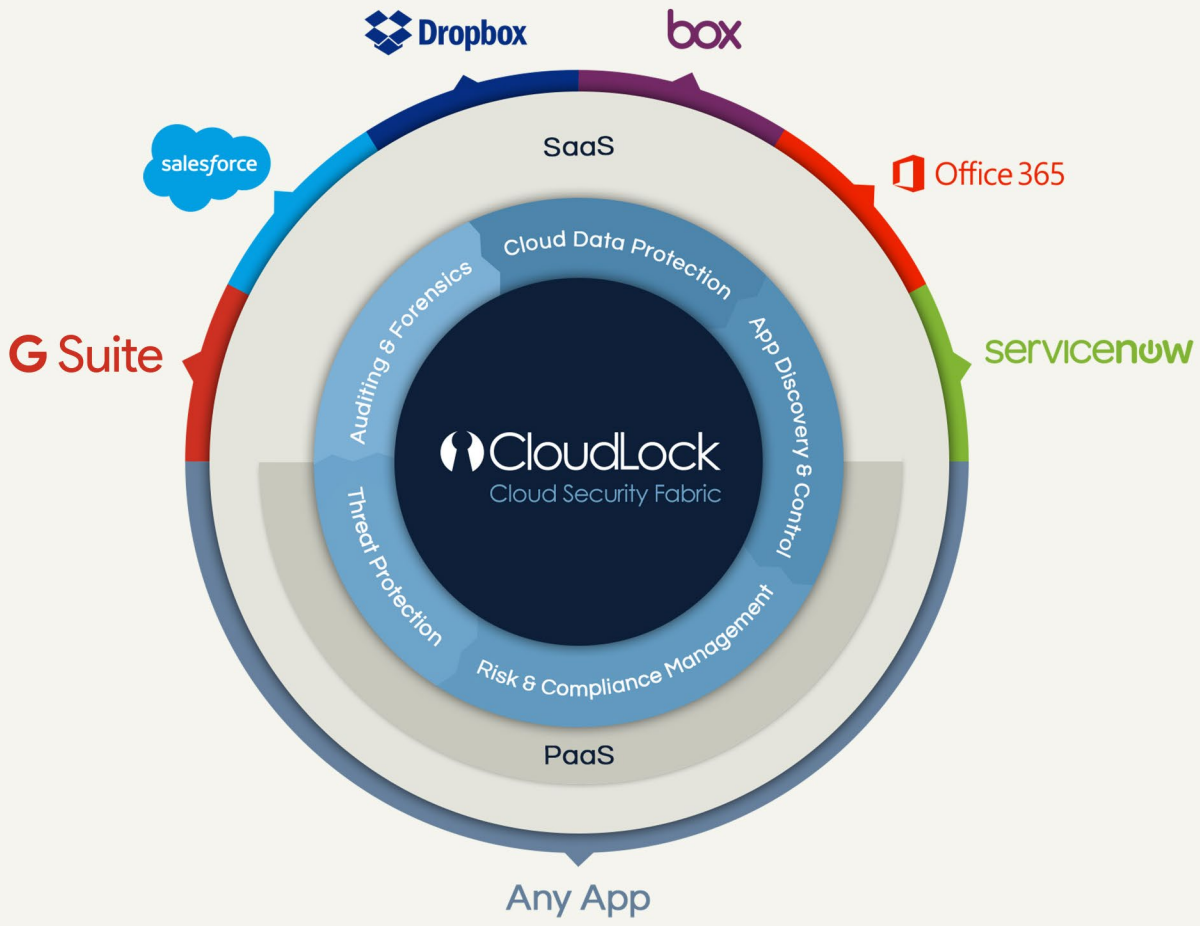
System and Communications Protection (SC)

- Leverage industry best encryption and key management technology, using AES-256 password-based encryption.
- Empower your end-users to selectively encrypt sensitive information as a service and securely share the encryption keys with authorized parties.

The Cloud Security Fabric

CloudLock offers the cloud security fabric enabling enterprises to protect their data in the cloud, reduce risk, achieve compliance, manage threats, and increase productivity.

Learn More



CloudLock

By analyzing 750 million files for more than 6 million end users daily. CloudLock delivers the only complete, risk-appropriate, and people-centric approach to cloud security.

www.cloudlock.com support@cloudlock.com (781) 996-4332