

FISMA (Pub.L. 113-283, 2014)

FISMA is a U.S. law requiring federal agencies and contractors to secure government information systems and manage cybersecurity risks.



What it is

The Federal Information Security Modernization Act (FISMA) is a United States federal law that sets requirements for securing federal information systems and protecting government data against cybersecurity threats. FISMA establishes a comprehensive framework to strengthen the security of federal digital assets and ensure effective risk management across government agencies.

FISMA is administered by the Office of Management and Budget (OMB) in coordination with the Department of Homeland Security (DHS). It applies to federal agencies, contractors, and other entities managing federal information or systems. The law mandates the implementation of security controls, continuous monitoring, incident response, and compliance oversight, with guidance often informed by NIST standards such as SP 800-53.

At a glance

PUBLISHER Cybersecurity and Infrastructure Security Agency (CISA)	TYPE Regulation	VERSION Federal Information Security Modernization Act of 2014
EFFECTIVE December 18, 2014	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>

Why it matters

- **Strengthen cybersecurity governance** Establishes clear responsibilities and accountability for managing information security risks within federal agencies and related organizations.
- **Enhance compliance support** Aligns organizations with federal cybersecurity requirements, streamlining the process of meeting regulatory obligations and external audit demands.
- **Promote continuous risk management** Requires ongoing risk assessments and monitoring, enabling dynamic identification and mitigation of emerging cybersecurity threats and vulnerabilities.
- **Support effective incident response** Mandates incident reporting and preparedness, improving the organization's ability to detect, respond to, and recover from security events.

How SmartSuite supports FISMA

System Scope and Categorization

Define system boundaries, impact levels, and dependencies with traceability.

Control Baseline and SSP Management

Manage controls, SSP narratives, and implementation statements in one place.

Assessments and POA&M Operations

Track findings, remediation, retesting, and closure verification.

Evidence Collection and Audit Trail

Centralize policies, configs, logs, and proof tied to each control.

Continuous Monitoring Cadence

Schedule scans, reviews, and recurring evidence updates to prevent drift.

ATO and Leadership Reporting

Provide readiness dashboards for authorization decisions and oversight.

Common framework mappings

CIS Controls v8.1

COBIT 2019

FedRAMP Rev. 5

ISO 27001:2022

NIST CSF 2.0

NIST 800-171 Rev. 3

NIST 800-37 Rev.2

NIST 800-53 Rev.4

Official resources

FISMA Overview Document

Provides essential details and requirements outlined by the Federal Information Security Modernization Act.

cisa.gov/federal-information-security-modernization-act

NIST Special Publication 800-53

Provides a catalog of security and privacy controls for federal information systems and organizations.

csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

OMB Circular A-130

Describes management of federal information resources, integrating FISMA requirements and guidance.

whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

NIST Risk Management Framework

Describes the framework for integrating supply chain risk management into system lifecycle.

csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Frequently asked questions

What is FISMA used for?

FISMA establishes a standardized framework for securing federal information systems and ensuring effective risk management to protect government data from cybersecurity threats. It sets requirements for federal agencies and their contractors to assess, implement, and oversee system security controls.

Is FISMA mandatory for all organizations?

FISMA is mandatory for all U.S. federal agencies, as well as contractors and third parties that manage or process federal information or federal information systems. Private sector entities not handling federal data are not required to comply with FISMA unless contractually obligated.

What systems and organizations are in scope for FISMA compliance?

FISMA applies to all information systems operated by or on behalf of federal agencies, including systems managed by service providers, contractors, and cloud vendors processing federal information. The scope is determined by the nature of information and federal governance requirements.

What key documentation and artifacts are required under FISMA?

Agencies must produce and maintain artifacts such as System Security Plans (SSPs), risk assessments, security control assessments, Plans of Action and Milestones (POA&Ms), and continuous monitoring reports. These documents help demonstrate the implementation and effectiveness of required security controls.

How does FISMA implementation work in practice?

FISMA implementation follows a risk management lifecycle involving the categorization of information systems, selection and implementation of security controls, assessment of control effectiveness, authorization to operate (ATO), and ongoing continuous monitoring and incident response.

How does FISMA relate to other security frameworks like NIST SP 800-53?

FISMA relies on NIST guidance—especially the NIST SP 800-53 control catalog and Risk Management Framework (RMF)—to provide detailed security controls and structured processes for compliance. FISMA is often integrated with broader cybersecurity programs and supports alignment with other federal standards.

What are the ongoing compliance requirements for FISMA?

Ongoing requirements include continual risk assessments, regular security control reviews, timely remediation of vulnerabilities, maintenance of compliance documentation, incident reporting, and submission of annual FISMA reports to oversight agencies such as OMB and DHS.

How would SmartSuite support FISMA compliance?

SmartSuite can help organizations operationalize FISMA by importing NIST control libraries, mapping controls to assets, and maintaining a centralized risk register. It supports evidence collection for audits, tracks compliance activities and POA&Ms, streamlines remediation workflows, and enables continuous monitoring and reporting through customizable dashboards.

License included / downloadable: Yes FISMA is United States federal legislation and is publicly available through official government publications.

Full framework page and mappings: smartsuite.com/frameworks/fisma-federal-information-security-modernization-act