Framework Foundations: FISMA

Introduction to FISMA

The Federal Information Security Modernization Act (FISMA) establishes a comprehensive framework for securing federal information systems. Originally enacted in 2002 and updated in 2014, FISMA requires federal agencies and their contractors to implement information security programs that protect the confidentiality, integrity, and availability of government data.

The 2014 update formalized the Department of Homeland Security's (DHS) role in managing and enforcing federal cybersecurity policies in coordination with the Office of Management and Budget (OMB).

Recent and Upcoming Changes

Under FY 2025 guidance, FISMA compliance emphasizes several new priorities:

- Adoption of Zero Trust Architecture across federal environments.
- Enhanced asset inventories for IoT and OT systems.
- Broader deployment of Endpoint Detection and Response (EDR) tools.
- Integration of cybersecurity performance metrics into budget planning.

These updates align FISMA more closely with the NIST Cybersecurity Framework (CSF) and OMB Memorandum M-25-04, reinforcing continuous monitoring and risk-based security practices.

Objectives of ISO/IEC 27001

- Protect federal information systems from unauthorized access and cyber threats.
- Ensure confidentiality, integrity, and availability of government data.
- Establish accountability for information security across agencies.
- Promote continuous monitoring and risk management practices.

Key Requirements

FISMA compliance mandates a structured approach to securing federal information systems, aligning closely with NIST standards and OMB guidance. The core requirements include:

Cybersecurity Governance

Establish and maintain an enterprise-wide cybersecurity strategy.
Demonstrate leadership accountability for security outcomes.

Supply Chain Risk Management (C-SCRM)

- Identify and mitigate risks from third-party vendors and service providers.
- Implement controls to secure the supply chain.

Risk and Asset Management

- Maintain accurate inventories of IT, IoT, and OT assets.
- Categorize systems using FIPS 199 and apply NIST 800-53 controls.

Configuration Management

- Enforce secure baseline configurations across systems.
- Monitor and remediate unauthorized changes.

Identity and Access Management (IDAM)

- Implement multi-factor authentication (MFA) for privileged and remote access.
- Manage user identities and access rights consistently.

Data Protection and Privacy

- Encrypt sensitive data at rest and in transit.
- Apply privacy controls aligned with NIST 800-122 and OMB A-130.

Security Training

- Provide role-based cybersecurity training for all personnel.
- Track and report completion metrics.

Continuous Monitoring (ISCM)

- Use automated tools to monitor system security posture.

Integrate findings into risk management and incident response processes.

Incident Response

- Maintain documented incident response plans.
- Report major incidents and breaches to DHS and Congress as required.

Contingency Planning

- Develop and test disaster recovery and business continuity plans.
- Ensure critical systems can be restored within acceptable timeframes.

How Cisco Security + Splunk Support Compliance

Meeting FISMA requirements demands a combination of strong governance, continuous monitoring, and advanced threat protection. Cisco and Splunk deliver integrated security capabilities that address these needs across federal environments. Cisco provides identity and access control, network segmentation, endpoint protection, and Zero Trust enforcement, while Splunk offers powerful analytics, SIEM, and automation for compliance reporting and incident response. Together, these solutions enable agencies and contractors to strengthen security posture, reduce risk, and maintain alignment with evolving federal mandates.

Table 1. How Cisco + Splunk supports FISMA compliance

FISMA Requirement	How Cisco + Splunk Support Compliance	Relevant Products and Services
Cybersecurity Governance	Centralizes policy enforcement, visibility, and reporting to support governance and accountability.	Cisco Identity Services Engine (ISE), Cisco Secure Network Analytics (SNA), Cisco Secure Access, Cisco Secure Firewall, Cisco XDR, Splunk Enterprise Security (ES), Talos IR Readiness Assessment, Talos IR Plan Development, CX Advisory Srvices
Supply Chain Risk Management(C-SCRM)	Monitors third-party integrations and data flows, enabling identification and mitigation of supply chain risks.	Cisco Duo, Cisco Secure Endpoint, Cisco Secure Access, Cisco Secure Firewall, Splunk SOAR, Talos Compromise Assessment, Talos Threat Intelligence
Risk and Asset Management	Provides asset discovery, classification, and risk scoring to support inventory and risk assessments.	Cisco ISE, Cisco SNA, Cisco Secure Workload, CIsco XDR, Splunk ES, Talos Compromise Assessment, Talos IR Readiness Assessment
Configuration Management	Supports baseline enforcement, change detection, and automated remediation actions.	Cisco Secure Endpoint, Cisco Secure Firewall, Cisco Secure Workload, Splunk ES, Talos Log Architecture Assessment
Identity and Access Management (IDAM)	Enforces MFA, identity verification, and access logging across systems.	Cisco Duo, Cisco Secure Access, Cisco ISE, Cisco XDR, Talos Purple Team Exercise

Table 1. (continued)

FISMA Requirement	How Cisco + Splunk Support Compliance	Relevant Products
Data Protection and Privacy	Supports encryption, data classification, and privacy monitoring.	Cisco Umbrella, Cisco Secure Access, Cisco Secure Email Threat Defense, Cisco Secure Endpoint, Cisco Secure Workload, Talos IR Plan Development, Talos Compromise Assessment
Security Training	Provides ongoing training that boosts security knowledge, improves threat detection, and strengthens incident response capabilities.	Cisco & Splunk Training and Certifications, Cisco Security Workshops, Cisco U., Talos IR Tabletop Exercises
Continuous Monitoring (ISCM)	Provides real-time telemetry, threat detection, and automated alerting across environments.	Cisco XDR, Cisco SNA, Cisco Secure Endpoint, Cisco Secure Workload, Splunk ES, Talos Compromise Assessment, Talos Threat Hunting
Incident Response	Enables rapid detection, investigation, and coordinated response to security incidents.	Cisco Secure Endpoint, Cisco ISE, Cisco XDR, Cisco SNA, Splunk ES, Talos Emergency IR Services, Talos Tabletop Exercises
Contingency Planning	Supports disaster recovery planning, backup monitoring, and continuity testing.	Cisco XDR, Cisco Secure Workload, Splunk ES, Talos Tabletop Exercises, Talos IR Readiness Assessment

FISMA Compliance with Cisco Security + Splunk

Cisco and Splunk deliver integrated security solutions that help organizations meet FISMA requirements efficiently and effectively. Cisco's portfolio provides centralized policy enforcement, identity and access management, secure network segmentation, and advanced threat detection across endpoints, networks, and cloud environments. These capabilities are complemented by Splunk's powerful analytics and SIEM platform, which enables real-time monitoring, compliance reporting, and automated workflows for incident response.

Together, Cisco and Splunk enable agencies and contractors to implement Zero Trust principles, maintain accurate asset inventories, and continuously monitor security posture. This combined approach supports proactive risk management, rapid incident detection, and streamlined reporting aligned with NIST standards and OMB guidance. By leveraging these solutions, organizations can strengthen governance, reduce supply chain risk, and ensure compliance with evolving FISMA mandates.

Resources

For more information and guidance on FISMA compliance, please refer to the following resources:

- FISMA | CISA
- FISMA | NIST
- Modernizing Government Cybersecurity Solution Brief
- Cisco VMDC Cloud Security 1.0 Design Guide