Framework Foundations: FedRAMP

Introduction to FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide initiative designed to standardize the security assessment, authorization, and continuous monitoring of cloud products and services. Its primary goal is to ensure that cloud service providers (CSPs) meet stringent security standards before they can be used by federal agencies.

FedRAMP is evolving through the FedRAMP 20x initiative, which aims to:

- Modernize the authorization process using automation and industry best practices.
- Simplify security requirements for cloud providers.
- Enhance continuous monitoring capabilities.
- Foster stronger collaboration between federal agencies and industry stakeholders.

These changes are expected to accelerate the adoption of secure cloud technologies across the federal landscape.

Objectives of FedRAMP

FedRAMP is built around four core objectives:

- **Standardization:** Create a unified security framework for federal cloud services.
- **Efficiency:** Reduce repeated security assessments to save time and resources.
- **Security:** Maintain strong protection of federal data with continuous monitoring.
- **Reuse:** Enable faster cloud deployment by reusing existing security authorizations.

Key Requirements

To achieve FedRAMP authorization, cloud service providers (CSPs) must meet several critical requirements that ensure the security and integrity of federal data:

Security Assessment

FedRAMP mandates a comprehensive security assessment based on NIST SP 800-53 Rev. 5 controls. This is conducted by a FedRAMP-accredited Third Party Assessment Organization (3PAO).

Authorization

Cloud Service Providers (CSPs) must obtain an Authority to Operate (ATO) from either the Joint Authorization Board (JAB) or a sponsoring federal agency. This process is detailed in the FedRAMP CSP Authorization Playbook.

Continuous Monitoring

After authorization, CSPs must implement a Continuous Monitoring (ConMon) program. This includes monthly vulnerability scans, incident reporting, and performance metrics, as outlined in the FedRAMP Continuous Monitoring Performance Management Guide.

Documentation

CSPs must submit a full authorization package, including:

- System Security Plan (SSP)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

These are required to demonstrate control implementation and risk management.

Risk Management

FedRAMP emphasizes a structured approach to identifying and mitigating risks, especially those associated with inherited controls and shared responsibilities.

Configuration Management

CSPs must maintain strict control over system configurations, including change management procedures and baseline integrity checks. This is part of the NIST SP 800-53 control families required by FedRAMP.

How Cisco Security + Splunk Support Compliance

Cisco and Splunk provide FedRAMP-authorized solutions that support federal agencies by addressing identity management, network visibility, threat detection, and application performance. These tools help agencies manage their environments according to FedRAMP standards and are designed for Moderate and High Impact environments as defined by FedRAMP.

FedRAMP Moderate

- **Cisco Meraki for Government**

Cloud-managed networking platform with secure wireless, switching, firewalls, and SD-WAN.

- **Cisco Duo Federal**

Multi-factor authentication (MFA) compliant with FIPS 140-2 and NIST SP 800-63-3. Supports AAL2 and AAL3 authenticators including biometric and hardware tokens.

- **Cisco Security Cloud Control for Government**

Centralized policy management across distributed environments.

- **Cisco Secure Access for Government**

Unified management with Zero Trust Network Access (ZTNA) and AI-driven threat intelligence.

- **Cisco Umbrella for Government**

DNS-layer security, Secure Web Gateway (SWG), Cloud Delivered Firewall (CDFW), CASB, and Data Loss Prevention (DLP).

- **Cisco Secure Firewall for Government**

Advanced threat protection and firewall capabilities tailored for federal environments.

- **Cisco SD-WAN for Government**

Secure, application-aware networking optimized for cloud integration

- **Cisco Cloudlock for Government**

Cloud-native CASB securing identities, data, and applications with machine learning analytics.

- **Cisco ThousandEyes for Government** (In Process)

Network performance visibility and diagnostics.

- **Splunk Cloud Platform**

Real-time operational insights for non-sensitive environments.

- **Splunk Observability Cloud** (In Process)

Proactive monitoring and optimization of infrastructure and applications.

- **Cisco AppDynamics GovAPM**

Real-time application performance monitoring for secure operations.

FedRAMP High

- **Splunk Cloud Platform**

Robust analytics and monitoring for critical government operations.

Conclusion

As federal agencies and contractors expand their use of cloud technologies, meeting FedRAMP requirements remains an essential step in working with the U.S. government. FedRAMP provides a consistent framework for evaluating cloud services, helping organizations align with federal expectations for security, risk management, and ongoing oversight.

By adopting these solutions, organizations can:

- Simplify the authorization process
- Improve visibility across cloud and network infrastructure
- Reduce the complexity of managing security controls
- Support scalable service delivery across federal environments

FedRAMP's "authorize once, use many times" model promotes efficiency and reuse across agencies. With Cisco Security and Splunk, organizations have access to technologies that support this model and help them move forward with their cloud strategies.

Resources

For more information and guidance on FedRAMP authorizations, please refer to the following resources:

- FedRAMP Marketplace
- Cisco Solutions for Federal Government
- Cisco Trust Portal
- Splunk Security Certifications and Attestations