SmartSuite

Framework / Cloud Security / FedRAMP

FedRAMP Rev. 5 – Low / Moderate / High

FedRAMP standardizes security requirements to assess, authorize, and continuously monitor cloud services that handle U.S. federal data.



What it is

FedRAMP Rev. 5 is a U.S. government security compliance framework that helps organizations assess, authorize, and monitor cloud service providers to ensure the protection of federal data. It establishes standardized cybersecurity requirements for cloud products and services used by federal agencies, focusing on risk management and data protection in cloud environments.

Developed and maintained by the Federal Risk and Authorization Management Program (FedRAMP), this framework draws from NIST Special Publication 800-53 and is mandated for all U.S. federal agencies when procuring cloud solutions. FedRAMP specifies unified security controls, continuous monitoring practices, and authorization processes, supporting federal compliance and data security mandates.

At a glance

PUBLISHER
Federal Risk and Authorization Management Program (FedRAMP)

TYPE
Certification / Assurance Program

VERSION
FedRAMP Rev. 5 (aligned with NIST SP 800-53 Rev. 5)

EFFECTIVE
2023

DOMAIN
Cloud Security

FAMILY
FedRAMP

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Very High

Source: https://www.fedramp.gov/

Why it matters

- **Support consistent risk management** Promote standardized risk assessment and mitigation practices to manage threats across diverse federal cloud service environments.
- **Enhance regulatory alignment** Ensure cloud solutions adhere to federal mandates and integrate with frameworks like NIST RMF for seamless compliance.
- **Improve security oversight** Enable continuous monitoring and independent assessment practices, fostering transparency and accountability in security operations.
- **Increase audit readiness** Provide well-documented controls and processes to streamline audit efforts and facilitate efficient compliance verification.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FedRAMP Rev. 5

Rev 5 Control Baseline and Tailoring

Manage Rev 5 controls and baseline parameters by system and scope.

Transition Planning from Rev 4

Track deltas, remediation tasks, and evidence updates for Rev 5 adoption.

SSP Evidence Linkage

Maintain SSP content and link evidence directly to each control.

Assessments and POA&M Discipline

Run findings and POA&M workflows with retesting and closure verification.

Continuous Monitoring Operations

Schedule scanning, patching, incident reporting, and recurring evidence updates.

Authorization and Readiness Reporting

Report control coverage, gaps, and transition progress for leadership and assessors.

Common framework mappings

CIS Controls v8.1 | CSA STAR | ISO 27001:2022 | ISO 27017 | ISO 27018 | NIST 800-37 Rev.2 | NIST 800-53 Rev.5 | SOC 2

Official resources

FedRAMP Authorization Process Guide

Provides a comprehensive outline of the FedRAMP authorization process for cloud service providers.

fedramp.gov/legacy/playbook/csp/authorization/getting-started

FedRAMP Continuous Monitoring Strategy Guide

Outlines strategies for continuous monitoring of cloud services under FedRAMP.

fedramp.gov/legacy/playbook/csp/continuous-monitoring/intro

FedRAMP Security Controls Baseline

Describes the baseline security controls necessary for FedRAMP compliance.

fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx

FedRAMP Plan of Action and Milestones Template Guide

Outlines the template for managing corrective actions for non-compliant security controls.

fedramp.gov/legacy/assets/LEGACY%20FedRAMP-POAM-Template.xlsx

Frequently asked questions

What is FedRAMP Rev. 5 used for?

FedRAMP Rev. 5 is a U.S. government security compliance framework designed to standardize the assessment, authorization, and continuous monitoring of cloud service providers (CSPs) handling federal data. It ensures federal agencies can safely adopt cloud solutions by mandating specific cybersecurity requirements and risk management practices.

Is FedRAMP Rev. 5 required for all cloud services used by federal agencies?

Yes, FedRAMP is mandatory for all U.S. federal agencies procuring commercial cloud services. Cloud service providers must achieve FedRAMP authorization before their services can be used to store, process, or transmit federal information.

Who does FedRAMP Rev. 5 apply to?

FedRAMP applies to all commercial and government cloud service providers that intend to offer their services to U.S. federal agencies. It also affects federal agency teams managing cloud adoption, requiring them to use only FedRAMP-authorized services.

What are the main artifacts required for FedRAMP compliance?

Key artifacts for FedRAMP compliance include the System Security Plan (SSP), security assessment reports from a third-party assessment organization (3PAO), Plan of Action and Milestones (POA&M), and continuous monitoring deliverables. These documents provide detailed mappings of security controls, assessment findings, and ongoing risk remediation activities.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How is FedRAMP implemented by cloud service providers?

CSPs must implement NIST SP 800-53 Rev. 4 security controls tailored to the Moderate Baseline, conduct a readiness assessment with a Third Party Assessment Organization (3PAO), and submit the required documentation for review. After initial authorization, CSPs must maintain continuous monitoring and reporting.

How does FedRAMP relate to other federal frameworks like NIST RMF?

FedRAMP aligns closely with the NIST Risk Management Framework (RMF) and leverages the NIST SP 800-53 control catalog to establish security baselines. FedRAMP provides a cloud-specific application of federal risk management principles, harmonizing with NIST RMF but focusing specifically on cloud environments.

What are the requirements for maintaining FedRAMP authorization?

Maintaining FedRAMP authorization requires continuous monitoring, regular vulnerability scanning, incident response testing, and submission of periodic reports. CSPs must remediate identified weaknesses promptly and keep documentation up to date to demonstrate ongoing compliance to authorizing officials.

How would SmartSuite support FedRAMP Rev. 5?

SmartSuite supports FedRAMP Rev. 5 management by enabling teams to import and manage control libraries, maintain a centralized risk register, and govern policies and SSP artifacts. It streamlines evidence collection, compliance tracking, and remediation workflows while providing dashboards for audit readiness and robust reporting to demonstrate real-time security posture and ongoing compliance.

License included / downloadable: Yes FedRAMP documentation is publicly available through official U.S. government resources.

Full framework page and mappings: smartsuite.com/frameworks/fedramp-rev-5-federal-risk-and-authorization-management-program