

FedRAMP Rev. 4 – Low / Moderate / High

FedRAMP Rev. 4 standardizes assessment, authorization, and continuous monitoring of cloud service providers to protect U.S. federal data.



What it is

At a glance

PUBLISHER Federal Risk and Authorization Management Program (FedRAMP)	TYPE Certification / Assurance Program	VERSION FedRAMP Rev. 4 (aligned with NIST SP 800-53 Rev. 4)
EFFECTIVE December 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

- **Strengthen security governance** Enable consistent implementation of robust security controls and clear accountability for safeguarding cloud-based information systems.
- **Enhance regulatory compliance** Support ongoing fulfillment of federal compliance obligations and streamline authorization for cloud services across U.S. government agencies.
- **Improve risk management practices** Facilitate continuous risk assessment and prompt mitigation of vulnerabilities, reducing the likelihood and impact of security incidents.
- **Increase audit readiness** Provide comprehensive documentation and audit trails, making it easier for organizations to demonstrate compliance during third-party reviews.

How SmartSuite supports FedRAMP Rev. 4

System Boundary and Scope Management Define authorization boundaries, assets, and dependencies with clear traceability.	Control Baseline and SSP Library Manage Rev 4 controls, SSP narratives, and implementation statements in one place.	Evidence Collection and Audit Trail Centralize policies, configurations, and proof tied to each control requirement.
Assessments and POA&M Operations Track findings, remediation, retesting, and closure evidence for all gaps.	Continuous Monitoring Cadence Schedule scans, patching, reporting, and recurring control activities with proof.	ATO-Ready Reporting Dashboards Provide ATO-ready reporting on control status, POA&Ms, and monitoring metrics.

Common framework mappings

CIS Controls v8.1

FISMA

ISO 27001:2022

ISO 27017

ISO 27018

NIST 800-37 Rev.2

NIST 800-53 Rev.5

Official resources

FedRAMP Security Assessment Framework Defines the FedRAMP process for assessing and authorizing cloud services. fedramp.gov/legacy/playbook/csp/authorization/what	FedRAMP Continuous Monitoring Strategy Guide Outlines strategies for continuous monitoring of cloud services under FedRAMP. fedramp.gov/legacy/playbook/csp/continuous-monitoring/intro
FedRAMP System Security Plan (SSP) Template Provides a template for creating a System Security Plan as required by FedRAMP. fedramp.gov/legacy/assets/LEGACY_FedRAMP-High-Moderate-Low-LI-SaaS-Baseline-System-Security-Plan-(SSP).docx	FedRAMP High Baseline Requirements Details security controls specific to high-impact systems under FedRAMP. fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx

Frequently asked questions

What is FedRAMP Rev. 4 used for?

FedRAMP Rev. 4 is used to standardize the security assessment, authorization, and continuous monitoring of cloud services for U.S. federal agencies. Its primary goal is to protect federal data stored in the cloud by ensuring consistent and robust cybersecurity practices among cloud service providers.

Is FedRAMP Rev. 4 required for cloud service providers?

Yes, FedRAMP Rev. 4 is mandatory for all cloud service providers (CSPs) that wish to host, process, or store federal government data. Federal agencies must only use cloud solutions that have achieved FedRAMP authorization.

What systems or organizations are in the scope of FedRAMP Rev. 4?

FedRAMP Rev. 4 applies to all cloud services used by U.S. federal agencies, including both infrastructure and software-as-a-service offerings. The framework is relevant to any organization seeking to provide cloud solutions to the government, regardless of size or sector.

What are the key artifacts required for FedRAMP Rev. 4 compliance?

Key artifacts include the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Plan of Actions and Milestones (POA&M), and continuous monitoring deliverables. These documents provide a detailed record of security controls, assessment processes, and remediation actions.

FedRAMP Rev. 4 Framework documents updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved. Page 2 of 3

How do organizations implement FedRAMP Rev. 4?

Organizations implement FedRAMP Rev. 4 by adopting the required NIST SP 800-53 security controls, developing the necessary documentation, and engaging a Third Party Assessment Organization (3PAO) for an independent security assessment. After authorization, CSPs must maintain compliance through continuous monitoring and regular reporting.

How does FedRAMP Rev. 4 relate to NIST SP 800-53 and other frameworks?

FedRAMP Rev. 4 is built directly on the NIST SP 800-53 control catalog, using tailored baselines (Low, Moderate, High) to address federal cloud security requirements. It integrates with other federal risk management processes, but is distinct in its cloud-specific focus and mandated federal use.

What are the ongoing compliance requirements for FedRAMP Rev. 4?

Ongoing compliance with FedRAMP Rev. 4 requires continuous monitoring, regular vulnerability scanning, periodic control assessments, incident response updates, and proactive POA&M management. CSPs must provide recurring security reports to maintain their authorization status.

How would SmartSuite support FedRAMP Rev. 4?

SmartSuite streamlines FedRAMP Rev. 4 compliance by enabling organizations to track risks, manage and map controls to the NIST SP 800-53 baselines, collect evidence for audits, and maintain required documentation. The platform supports automated evidence collection, remediation workflows for POA&Ms, audit readiness, and real-time dashboards for compliance reporting and stakeholder oversight.

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-4-federal-risk-and-authorization-management-program