

FedRAMP Rev. 4 – Moderate Baseline

FedRAMP Rev. 4 Moderate baseline defines security assessment, authorization, and continuous monitoring for cloud services used by U.S. federal agencies.



What it is

U.S. FedRAMP Rev. 4 (Moderate Impact Baseline) is a federal cybersecurity framework that enables U.S. government agencies to securely adopt cloud services by standardizing security assessment, authorization, and continuous monitoring processes. The Moderate Impact Baseline defines the minimum set of security controls required to protect government data that, if compromised, could have a serious adverse effect on operations or assets.

FedRAMP is published and managed by the Federal Risk and Authorization Management Program (FedRAMP), governed by the U.S. General Services Administration (GSA) in collaboration with NIST and other federal bodies. Federal agencies and cloud service providers (CSPs) use FedRAMP to demonstrate compliance with federal information security requirements, focusing on areas such as risk management, data protection, access control, and incident response.

At a glance

PUBLISHER General Services Administration (GSA)	TYPE Certification / Assurance Program	VERSION Rev. 4
EFFECTIVE April 22, 2013	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/legacy/assets/LEGACY_CSP_Annual_Assessment_Controls_Selection_Worksheet%203.1.xlsx

Why it matters

- **Strengthen security governance** Establish clear policies and accountability for managing cloud service security across the organization's infrastructure.
- **Enhance regulatory compliance** Support alignment with federal security requirements, making it easier to demonstrate adherence during audits and assessments.
- **Increase audit readiness** Leverage standardized security controls and assessment procedures to streamline preparation and response for official audits and reviews.
- **Improve risk management** Enable organizations to proactively identify, assess, and mitigate risks associated with cloud service providers and information systems.

How SmartSuite supports FedRAMP Rev.4 Moderate

FedRAMP Low Control Library

Structure NIST 800-53 Low baseline controls with mapped owners, implementation tasks, and documentation.

System Security Plan Management

Maintain the SSP, architecture documentation, and system boundary definitions required for authorization.

Risk Assessment and Authorization Tracking

Track risk assessments, control implementation status, and authorization activities.

Vulnerability and Incident Management

Manage vulnerability findings, remediation actions, and incident response workflows.

Continuous Monitoring Program

Track recurring assessments, patch management, configuration reviews, and monitoring evidence.

FedRAMP Compliance and Reporting

Provide dashboards summarizing control coverage, open findings, and readiness for FedRAMP authorization reviews.

Common framework mappings

CIS Controls v8.1

GDPR

HIPAA (NIST SP 800-66 Rev. 2)

ISO 27001:2022

ISO 27017

ISO 27018

NIST CSF 2.0

NIST 800-171 Rev. 3

NIST 800-53 Rev.5

SOC 2

Official resources

FedRAMP Moderate Baseline

Defines security requirements for cloud services under the FedRAMP Moderate Impact Level.
[fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx](https://www.fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx)

FedRAMP Program Overview

Outlines the Federal Risk and Authorization Management Program and its objectives.
[fedramp.gov](https://www.fedramp.gov)

FedRAMP Security Controls

Provides detailed security control matrices for FedRAMP compliance.
[fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx](https://www.fedramp.gov/legacy/assets/LEGACY%20FedRAMP_Security_Controls_Baseline.xlsx)

Frequently asked questions

What is FedRAMP Rev. 4 (Moderate Impact Baseline) used for?

FedRAMP Rev. 4 (Moderate Impact Baseline) provides security requirements for cloud services used by U.S. federal agencies that handle controlled, unclassified information with moderate risk. Its purpose is to standardize cloud security assessments and authorizations, ensuring adequate protection of federal data in cloud environments.

Is FedRAMP required for cloud service providers?

Yes, FedRAMP is a mandatory program for cloud service providers (CSPs) that want to offer cloud services to U.S. federal agencies. CSPs must comply with FedRAMP requirements and obtain an Authorization to Operate (ATO) before their services can be used by federal customers.

What is the scope of FedRAMP Moderate Impact Baseline?

FedRAMP Moderate applies to cloud systems and services that process, store, or transmit federal information categorized as "moderate impact" under FIPS 199. It covers both infrastructure and software services and is applicable to CSPs seeking federal contracts involving sensitive but unclassified data.

What key documents and artifacts are required for FedRAMP compliance?

Key FedRAMP artifacts include the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Plan of Action and Milestones (POA/M), and Continuous Monitoring Program (CMP). These documents demonstrate the implementation and ongoing management of required security controls.

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 Moderate relate to other frameworks like NIST and FISMA?

FedRAMP Moderate is directly based on NIST SP 800-53 security controls and aligns with FISMA requirements for federal information systems. It tailors these controls for cloud environments and provides a unified approach for federal cloud security authorization.

What are the ongoing compliance requirements for FedRAMP Moderate?

CSPs must perform continuous monitoring, including regular vulnerability scans, control assessments, and POA&M updates. They must report security incidents, review control effectiveness, and update documentation to maintain an active FedRAMP authorization status.

How would SmartSuite support FedRAMP Rev. 4 (Moderate Impact Baseline)?

SmartSuite can help organizations manage the FedRAMP Moderate program by centralizing risk tracking, aligning control management with FedRAMP requirements, and collecting evidence needed for audits. It enables teams to maintain audit readiness, streamline reporting, and ensure continuous compliance with all FedRAMP documentation and monitoring obligations.

License included / downloadable: Yes FedRAMP Rev. 4 Moderate Impact Baseline is publicly available on FedRAMP.gov. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/fedramp-rev-4-moderate-baseline