

FedRAMP Rev. 5 – Moderate Baseline

FedRAMP Rev. 5 defines standardized security assessment, authorization, and continuous monitoring requirements for cloud services handling moderate-impact federal data.



What it is

At a glance

PUBLISHER Federal Risk and Authorization Management Program (FedRAMP)	TYPE Certification / Assurance Program	VERSION Rev. 5
EFFECTIVE May 29, 2023	DOMAIN Cloud Security	FAMILY FedRAMP
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: https://raw.githubusercontent.com/GSA/fedramp-automation/master/dist/content/rev5/baselines/xml/FedRAMP_rev5_MODERATE-baseline_profile.xml

Why it matters

- **Strengthen risk management oversight** Enable consistent monitoring and control of cloud environments through standardized security requirements and continuous assessment.
- **Enhance regulatory and policy alignment** Support compliance with federal laws and requirements, simplifying security review and authorization processes across agencies.
- **Increase audit readiness** Provide clear documentation and evidence of security controls, improving efficiency and transparency during audits and assessments.
- **Improve data protection measures** Ensure stronger safeguards for sensitive government data, reducing exposure to loss, unauthorized access, or compromise.

How SmartSuite supports FedRAMP Rev.5 Moderate

FedRAMP Moderate Control Library

Structure NIST SP 800-53 Rev. 5 Moderate baseline controls with mapped ownership, implementation tasks, and documentation.

System Security Plan and Authorization Governance

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

Risk Assessment and Control Implementation Tracking

Track risk assessments, control implementation status, and remediation activities across cloud systems.

Vulnerability and Incident Management

Monitor vulnerability findings, remediation workflows, and incident response activities affecting cloud environments.

Continuous Monitoring and Compliance Evidence

Track recurring assessments, configuration monitoring, and evidence required for FedRAMP continuous monitoring.

Federal Security Assessment and Authorization Readiness Reporting

Provide dashboards summarizing control status, open findings, and readiness for federal security assessments and authorization reviews.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GDPR

HIPAA

ISO 27001:2022

ISO 27017

ISO 27018

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

Official resources

FedRAMP Moderate Impact Baseline

Defines security controls and requirements for cloud systems classified as moderate impact.

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

FedRAMP Security Assessment Framework

Defines the FedRAMP process for assessing and authorizing cloud services.

fedramp.gov/legacy/playbook/csp/authorization/what

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 Program Overview

Outlines the Federal Risk and Authorization Management Program and its objectives.

fedramp.gov

Frequently asked questions

What is FedRAMP Rev. 5 Moderate Impact Baseline used for?

FedRAMP Rev. 5 Moderate Impact Baseline is used to standardize security assessment, authorization, and continuous monitoring for cloud service providers (CSPs) handling federal data classified as moderate impact. This framework ensures that cloud services have adequate security controls to protect federal information in accordance with FISMA requirements.

Is FedRAMP Rev. 5 Moderate Impact Baseline mandatory for cloud providers?

Yes, FedRAMP is mandatory for all cloud service providers that wish to provide services to U.S. federal agencies. CSPs must achieve a FedRAMP Authorization to Operate (ATO) at the appropriate impact level before contracting with federal agencies.

What organizations are required to comply with FedRAMP Moderate Impact Baseline?

All CSPs offering cloud services to federal agencies that process, store, or transmit federal information categorized as moderate impact are required to comply. This includes both commercial and government CSPs seeking to achieve or maintain FedRAMP authorization.

What are the key artifacts required for FedRAMP compliance?

Key artifacts include a System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), and Continuous Monitoring documentation. These artifacts provide detailed information on implemented controls, assessment processes, residual risks, and remediation efforts.

How does a cloud service provider implement FedRAMP Moderate controls?

CSPs must implement and document the prescribed NIST SP 800-53 Rev. 5 controls as specified in the FedRAMP Moderate Baseline. The implementation process involves gap analysis, remediation, documentation of control effectiveness, and undergoing a third-party security assessment by a FedRAMP-accredited assessor (3PAO).

How does FedRAMP Rev. 5 differ from other FedRAMP baselines or similar frameworks?

FedRAMP Moderate covers systems impacting the confidentiality, integrity, or availability of federal data at a moderate level, whereas Low and High baselines apply to different sensitivity levels. Compared to other frameworks, FedRAMP Moderate leverages NIST SP 800-53 controls and incorporates additional federal-specific requirements such as continuous monitoring and incident reporting.

What ongoing activities are required to maintain FedRAMP authorization?

Maintaining FedRAMP authorization requires continuous monitoring, including regular vulnerability scans, annual security assessments, incident reporting, and timely remediation of identified risks. CSPs must also submit monthly and annual reports and keep all documentation current to demonstrate ongoing compliance.

How would SmartSuite support FedRAMP Rev. 5 Moderate Impact Baseline?

SmartSuite can help organizations manage FedRAMP compliance by centralizing risk tracking, facilitating control management, and streamlining evidence collection processes. The platform supports organizing documentation, monitoring compliance status, preparing for assessments, and providing audit-ready reporting to simplify ongoing FedRAMP maintenance and demonstrate control effectiveness.

License included / downloadable: Yes FedRAMP baselines are published by U.S. GSA and are publicly available on the official FedRAMP website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/fedramp-rev-5-moderate-impact-baseline