

FedRAMP Rev. 4 – High Impact Baseline

FedRAMP Rev. 4 High Impact Baseline defines security controls and the authorization process for cloud services protecting high-impact federal data.



What it is

U.S. FedRAMP Rev. 4 (High Impact Baseline) is a federal cybersecurity compliance framework that establishes rigorous security control requirements for cloud services handling the most sensitive federal data. This baseline is part of the Federal Risk and Authorization Management Program (FedRAMP), which aims to standardize security assessment, authorization, and continuous monitoring of cloud products and services used by U.S. government agencies.

FedRAMP is published by the U.S. General Services Administration (GSA) in collaboration with NIST, OMB, and other agencies. It is mandatory for cloud service providers (CSPs) seeking to offer high-impact cloud solutions to federal departments and covers areas such as access control, incident response, risk management, and data protection for high-value assets.

At a glance

PUBLISHER United States 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/>

Why it matters

- Strengthen security governance** Drive stronger oversight and accountability for information security programs across cloud environments handling highly sensitive federal data.
- Enhance regulatory compliance** Support agencies and vendors in meeting federal mandates for risk assessments, documentation, and continuous security monitoring.
- Improve data protection measures** Mandate robust controls and encryption to safeguard classified or mission-critical information from unauthorized access and breaches.
- Enable rapid incident response** Support early detection and coordinated response to cybersecurity incidents, minimizing potential disruptions and data losses.

How SmartSuite supports FedRAMP Rev.4 High

FedRAMP High Control Library Structure NIST SP 800-53 High baseline controls with mapped ownership, implementation tasks, and detailed documentation.	System Security Plan and Architecture Governance Maintain the SSP, system boundary definitions, architecture diagrams, and security documentation required for high-impact systems.	Risk Management and Control Implementation Tracking Track risk assessments, security control implementation, and remediation workflows across mission-critical systems.
Vulnerability, Patch, and Incident Management Monitor vulnerability findings, coordinate remediation efforts, and track incident response activities.	Continuous Monitoring and Security Evidence Track recurring security assessments, configuration monitoring, and compliance evidence supporting FedRAMP requirements.	Federal Authorization Review Readiness Reporting Provide dashboards summarizing control status, open remediation items, and readiness for federal authorization reviews.

Common framework mappings

CIS Controls v8.1

COBIT 2019

HIPAA

ISO 27001:2022

NIST CSF 2.0

NIST 800-171 Rev. 3

PCI DSS 4.0.1

SOC 2

Official resources

FedRAMP High Impact Baseline Defines security requirements for cloud systems handling high-impact federal data. 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 Continuous Monitoring Strategy Guide Outlines strategies for continuous monitoring of cloud services under FedRAMP. fedramp.gov/legacy/playbook/csp/continuous-monitoring/intro	FedRAMP Plan of Action and Milestones Template Offers a template for tracking remediation efforts related to security findings. fedramp.gov/legacy/assets/LEGACY%20FedRAMP-POAM-Template.xlsx

Frequently asked questions

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

FedRAMP Rev. 4 (High Impact Baseline) is used to ensure that cloud service providers (CSPs) implement rigorous security controls to protect federal data classified as high impact, where loss could have severe or catastrophic effects on operations, assets, or individuals. It provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by U.S. federal agencies.

Is compliance with FedRAMP High Impact Baseline mandatory?

Compliance with FedRAMP is mandatory for all cloud services used by U.S. federal agencies. The High Impact Baseline specifically applies when agencies intend to store, process, or transmit high impact data in a cloud environment, ensuring appropriate safeguards are in place before granting an Authority to Operate (ATO).

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

Any cloud service provider that seeks to offer cloud services to federal agencies handling high impact data must comply with the FedRAMP High Impact Baseline. Federal agencies are also required to ensure the CSPs they use are FedRAMP authorized for the appropriate impact level.

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

What key artifacts are required for FedRAMP High Impact Baseline compliance?

FedRAMP High Impact Baseline compliance requires documentation such as the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Plan of Actions and Milestones (POA&M), and continuous monitoring reports. These artifacts are essential for demonstrating the implementation of required security controls and for the assessment process.

What is the process for implementing FedRAMP High Impact Baseline controls?

The implementation process involves conducting a security assessment based on NIST SP 800-53 Revision 4 controls at the high baseline. CSPs must identify applicable controls, document how each control is implemented, undergo a Third Party Assessment Organization (3PAO) audit, and address any findings before federal agencies can authorize their services for use.

How does FedRAMP High Impact Baseline relate to other frameworks like NIST SP 800-53?

FedRAMP High Impact Baseline is directly based on the NIST SP 800-53 Revision 4 security control catalog, mapping specific controls to cloud environments at the "high" impact level. It adds additional guidance and requirements tailored to federal cloud deployments, complementing but not replacing other federal security frameworks.

What are the ongoing compliance requirements for FedRAMP High Impact Baseline?

Organizations must conduct continuous monitoring, submit periodic security reports, and promptly remediate vulnerabilities. Ongoing responsibilities include monthly vulnerability scans, annual security assessments by a 3PAO, and continuous documentation updates to maintain FedRAMP Authorization to Operate (ATO).

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

SmartSuite helps organizations manage FedRAMP Rev. 4 (High Impact Baseline) compliance by providing integrated tools for risk tracking, control management, and evidence collection. It enables streamlined audit readiness through structured workflows for documenting and updating artifacts, tracking POA&Ms, and generating compliance reports to support ongoing monitoring and authorization activities.

License included / downloadable: Yes FedRAMP Rev. 4 High Impact Baseline is publicly available from the U.S. GSA's FedRAMP website.
License included with platform

Full framework page and mappings: smartsuite.com/frameworks/fedramp-rev-4-high-impact-baseline-federal-risk-and-authorization-management-program