SmartSuite

Framework / Cloud Security / FedRAMP

FedRAMP Rev. 5 – High Baseline

FedRAMP Rev. 5 High baseline: the 410 NIST SP 800-53 Rev. 5 controls and enhancements for high-impact cloud services, FedRAMP parameters and the Consolidated Rules for 2026 dates.



What it is

The FedRAMP Rev. 5 High baseline is the largest FedRAMP control profile: 410 NIST SP 800-53 Rev. 5 items, 191 controls and 219 enhancements in 18 families, that a cloud service offering must implement, have independently assessed and keep certified when it holds federal information categorized High under FIPS 199, where a loss of confidentiality, integrity or availability could have a severe or catastrophic effect. The Rev. 5 baselines received Joint Authorization Board approval on May 29, 2023; the Rev5 process is now a legacy certification path under the FedRAMP Consolidated Rules for 2026 and closes to new applications on June 11, 2027.

At a glance

PUBLISHER
U.S. General Services Administration (GSA), FedRAMP Program Management Office; baselines approved by the FedRAMP Joint Authorization Board

TYPE
Certification / Assurance Program

VERSION
Rev. 5 High baseline (410 items, approved May 29, 2023); legacy Rev5 Certification process under the Consolidated Rules for 2026

EFFECTIVE
May 29, 2023 (Rev. 5 baselines approved and released; phased transition followed); Consolidated Rules for 2026 in effect July 4, 2026

DOMAIN
Cloud Security

FAMILY
FedRAMP

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: fedramp.gov/legacy/

Why it matters

- **The full federal control set** 410 items from NIST SP 800-53 Rev. 5 with FedRAMP-defined assignments, additional requirements and monitoring periodicity for each, published in the FedRAMP Security Controls Baseline workbook.
- **Tighter cadences than Moderate or Low** Annual policy review (AC-1), monthly privileged account review (AC-2(j)), account disablement after 35 days of inactivity (AC-2(3)) and annual privilege reviews (AC-6(7)).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FedRAMP Rev. 5 High

Rev. 5 High Control Library

Load the 191 controls and 219 enhancements by family with the FedRAMP-defined assignments, additional requirements and continuous monitoring periodicity from the baseline workbook.

Security Decision Records

Record each control's implementation, provider-defined parameter values and the inherited or customer-responsibility split that forms the Certification Package Overview and Security Decision Record.

Contingency Planning and Backup

Manage the CP family in Operational Resilience & Business Continuity: the ISCP, the annual CP-2 review, CP-9 backup schedules and recovery tests with evidence attached.

Vulnerability and Accepted Weaknesses

Track RA-5 scan findings, SI-2 patch deadlines and the Accepted Weaknesses list in Cyber & IT Risk, with the 30-day high-risk clock on each finding.

Supplier Assessments

Run the SR-6 annual supplier assessments in Third Party Risk Management, recording each vendor's alignment to NIST SP 800-171 or a commensurate framework.

Ongoing Certification Dashboards

Report weekly audit reviews, monthly inventories and scans, annual penetration tests and overdue items on dashboards for the assessor and agency reviews.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · HIPAA (NIST SP 800-66 Rev. 2) · ISO 27001:2022 · ISO 27017 · ISO 27018 · NIST CSF 2.0 · NIST 800-171 Rev. 3 · PCI DSS 4.0.1 · SOC 2

Official resources

FedRAMP High Baseline Requirements

Details security controls specific to high-impact systems under FedRAMP.

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

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

Frequently asked questions

How many controls are in the FedRAMP Rev. 5 High baseline?

410 items: 191 base controls and 219 control enhancements from NIST SP 800-53 Rev. 5 across 18 families, as listed on the High tab of the FedRAMP Security Controls Baseline workbook. The largest families are Access Control (50 items), Contingency Planning, System and Communications Protection and System and Information Integrity (35 each), Configuration Management (34) and Identification and Authentication (30). The Moderate baseline has 323 items and Low 156.

What makes the High baseline stricter than Moderate or Low?

Beyond the extra controls, FedRAMP sets tighter parameters. At High the access control policy is reviewed at least annually (AC-1) instead of every three years at Low, privileged accounts are reviewed monthly and other accounts every six months (AC-2(j)) instead of annually, inactive accounts are disabled after 35 days (AC-2(3)), privileges are reviewed annually (AC-6(7)) and information at rest must be protected for confidentiality and integrity (SC-28).

 © 2026 SmartSuite Inc. All rights reserved.

Which monitoring cadences does FedRAMP fix for High systems?

The baseline workbook sets weekly audit record review (AU-6), at least 90 days of online audit retention (AU-11), a monthly system component inventory (CM-8), monthly operating system, web application and database scans with high-risk findings mitigated within 30 days (RA-5), patches within 30 days of release (SI-2), monthly configuration scans and annual assessor-run scans (CA-7), an annual penetration test (CA-8), daily incremental and weekly full backups (CP-9) and annual supplier assessments (SR-6).

Can a High-impact cloud service move to FedRAMP 20x yet?

Not yet. The fedramp.gov 20x page states that rules are finalized for Class A, Class B and Class C certifications and that Class D certifications will be developed during 20x Phase 4, a High pilot with an estimated FY27 Q1 to Q2 window. FedRAMP will stop accepting new Rev5 certifications on June 11, 2027 and has said it will provide a transition path for existing Rev5 offerings by the end of Phase 5.

What do the Consolidated Rules for 2026 require of an existing Rev5 High certification?

From January 1, 2027 all new Rev5 applications must follow the Consolidated Rules, and existing certifications must adopt the rulesets within the published grace periods, all of which expire on February 1, 2028; an offering not fully following the rules then loses its FedRAMP Certification with public notice. The rules rename continuous monitoring to Ongoing Certification, replace POA&Ms with Accepted Weaknesses, move packages from Word and Excel templates to JSON schemas and let providers define most organizational parameters themselves.

License included / downloadable: Yes The FedRAMP High baseline, the legacy Security Controls Baseline workbook and the Consolidated Rules for 2026 are U.S. Government works available free on fedramp.gov; NIST SP 800-53 Rev. 5 and SP 800-53B are free from NIST.

Full framework page and mappings: smartsuite.com/frameworks/us-fedramp-rev-5-high-impact-baseline-federal-risk-authorization