

FedRAMP Rev. 5 – High Baseline

FedRAMP High Impact Baseline specifies security and authorization requirements for cloud services processing high impact federal data.



What it is

U.S. FedRAMP Rev. 5 (High Impact Baseline) is a federal cybersecurity framework that helps organizations secure cloud services used by U.S. government agencies dealing with highly sensitive data. It establishes rigorous security control requirements to ensure cloud providers protect critical federal information systems against advanced threats and data breaches.

Published by the Federal Risk and Authorization Management Program (FedRAMP), the High Impact Baseline is mandatory for federal agencies procuring cloud solutions that process, store, or transmit high-impact data. It closely aligns with NIST SP 800-53 Rev. 5 controls and is used by both cloud service providers and federal security assessors to enforce consistent risk management and compliance across government cloud environments.

At a glance

PUBLISHER U.S. General Services Administration (GSA)	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://www.fedramp.gov/resources/documents/FedRAMP_Baselines_Rev5_Transition_Guide.pdf

Why it matters

- **Strengthen security oversight** Enable consistent monitoring and management of security controls across high-impact cloud services supporting federal agencies.
- **Enhance regulatory compliance** Support adherence to federal information security standards, simplifying the compliance process for both agencies and cloud service providers.
- **Promote operational resilience** Reduce risks of disruption by requiring robust contingency planning, incident response, and recovery capabilities for high-impact systems.
- **Improve threat detection and response** Facilitate timely identification and mitigation of security incidents through prescriptive monitoring and reporting requirements.

How SmartSuite supports FedRAMP Rev.5 High

FedRAMP High Control Library Structure NIST SP 800-53 Rev. 5 High baseline controls with mapped owners, implementation tasks, and detailed documentation.	System Security Plan and Architecture Governance Maintain SSP documentation, system boundaries, architecture diagrams, and security artifacts required for FedRAMP authorization.	Risk Management and Control Implementation Tracking Track risk assessments, control implementation progress, and remediation activities across mission-critical cloud systems.
Vulnerability, Patch, and Incident Management Monitor vulnerability findings, patch remediation status, and incident response workflows across environments.	FedRAMP Continuous Monitoring and Security Evidence Track ongoing assessments, configuration monitoring, and security evidence supporting FedRAMP continuous monitoring requirements.	FedRAMP Authorization Readiness Reporting Provide dashboards summarizing control implementation status, open remediation items, and readiness for federal authorization 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

- What is FedRAMP Rev. 5 High Impact Baseline used for?**

FedRAMP Rev. 5 High Impact Baseline is designed to standardize security assessment, authorization, and continuous monitoring for cloud services used by federal agencies handling highly sensitive, mission-critical data. It sets security controls to safeguard data against advanced threats, ensuring that high-impact cloud solutions meet federal security requirements.
- Is FedRAMP High Impact Baseline mandatory for cloud service providers?**

Yes, FedRAMP compliance is mandatory for all cloud service providers (CSPs) offering cloud products or services to U.S. federal agencies. The High Impact Baseline specifically applies if CSPs store, process, or transmit data where loss of confidentiality, integrity, or availability could have a severe or catastrophic effect on operations.
- What is the scope of applicability for FedRAMP Rev. 5 High Impact Baseline?**

The High Impact Baseline applies to cloud services supporting federal agencies with operations, assets, or individuals at the highest risk level. It covers the protection of sensitive data—such as personal identifiable information (PII) and classified information—where the impact of a breach would be unacceptable.

What are the key security controls required by FedRAMP High Impact Baseline?

FedRAMP Rev. 5 High Impact Baseline specifies 421 security and privacy controls aligned with NIST SP 800-53 Rev. 5. Key controls address access management, incident response, continuous monitoring, encryption, system integrity, and personnel security, tailored to safeguard very sensitive information.

How do organizations implement FedRAMP Rev. 5 High Impact Baseline controls?

Organizations implement FedRAMP controls by defining and documenting security policies, procedures, and technical safeguards that map to specific control requirements. They must prepare a robust System Security Plan (SSP), perform risk assessments, and undergo assessments by a FedRAMP-authorized Third Party Assessment Organization (3PAO).

How does FedRAMP High Impact Baseline relate to NIST and other frameworks?

FedRAMP High Impact Baseline directly leverages the NIST SP 800-53 Rev. 5 controls, tailoring them for cloud environments and federal requirements. It is designed to complement other frameworks like FISMA, CMMC, and ISO 27001, supporting a risk-based approach for high-assurance systems.

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. 5 High Impact Baseline?

SmartSuite helps organizations manage FedRAMP Rev. 5 High Impact Baseline by centralizing risk tracking, control management, and evidence collection. It streamlines audit readiness through workflow automation, keeps compliance documentation current, and enables real-time reporting to support ongoing monitoring and authorization efforts.

License included / downloadable: Yes FedRAMP Rev. 5 High Impact Baseline is published by U.S. FedRAMP (GSA) and is publicly available for free on the official FedRAMP website. License included with platform

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