

FedRAMP Rev. 5 – Low

FedRAMP Rev. 5 Low Impact Baseline standardizes security assessment, authorization, and monitoring for low-impact cloud services used by U.S. federal agencies.



What it is

At a glance

PUBLISHER 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/rev5/documents-templates/>

Why it matters

- **Support secure cloud adoption** Enable organizations to confidently leverage cloud technologies while ensuring adequate protection of federal information systems.
- **Strengthen compliance oversight** Provide a recognized framework for demonstrating compliance with federal security requirements and third-party risk assessments.
- **Enhance incident detection and response** Facilitate timely monitoring, reporting, and mitigation of cybersecurity incidents within cloud environments.
- **Promote consistent security practices** Encourage uniform application of security controls and processes across all cloud service providers used by federal agencies.

How SmartSuite supports FedRAMP Rev.5 Low

FedRAMP Low Control Library

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

System Security Plan and Authorization Governance

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

Risk Management and Control Implementation Tracking

Track risk assessments, control implementation progress, and remediation actions across cloud systems.

Vulnerability and Incident Management

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

Continuous Monitoring Program

Track recurring security assessments, configuration monitoring, and compliance evidence supporting FedRAMP requirements.

FedRAMP Authorization Readiness Reporting

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

Common framework mappings

CIS Controls v8.1

COBIT 2019

HIPAA

ISO 27001:2022

ISO 27017

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

FedRAMP Low Impact Baseline

Defines the security and risk management requirements for Low Impact cloud systems under FedRAMP.

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

FedRAMP Security Controls Baseline

Describes the baseline security controls necessary for FedRAMP compliance.

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

Frequently asked questions

What is FedRAMP Rev. 5 (Low Impact Baseline) used for?

FedRAMP Rev. 5 (Low Impact Baseline) is used to provide security assessment and authorization requirements for cloud service providers (CSPs) serving U.S. federal agencies when the information systems have a low impact level. It ensures that even systems with minimal potential impact on federal operations follow consistent security standards. This baseline addresses the protection of information categorized at the low impact level as defined by FIPS 199.

Is compliance with FedRAMP Rev. 5 required for all cloud providers?

Compliance with FedRAMP Rev. 5 is mandatory for cloud service providers seeking to offer services to U.S. federal agencies. Federal agencies must ensure all cloud solutions used are FedRAMP authorized at the appropriate impact level. Low Impact Baseline is specifically required for systems processing, storing, or transmitting only low impact federal data.

What systems are in scope for the FedRAMP Low Impact Baseline?

The FedRAMP Low Impact Baseline applies to cloud information systems that process, store, or transmit federal information classified as low impact under FIPS 199. Typical use cases include systems with publicly available or non-sensitive information such as collaboration tools or public-facing websites used by federal agencies. Systems with moderate or high risk do not fall under this baseline.

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

The Low Impact Baseline specifies a subset of NIST SP 800-53 Rev. 5 security controls tailored for systems with minimal risk. Controls include basic access controls, incident response, maintenance, configuration management, and audit as required for federal environments. A complete list of applicable controls is provided in the FedRAMP Low Baseline documentation.

How do organizations implement FedRAMP Low Impact Baseline requirements?

Organizations implement FedRAMP Low by selecting, documenting, and putting in place the prescribed security controls, typically through supporting policies, technical safeguards, and operational procedures. They must also prepare artifacts such as a System Security Plan (SSP) and demonstrate control effectiveness through assessment. Ongoing monitoring and reporting are essential for maintaining compliance.

How is FedRAMP Low Impact Baseline related to other federal security frameworks?

FedRAMP Low Impact Baseline aligns closely with NIST SP 800-53 and uses FIPS 199 for information categorization. It complements broader federal compliance programs but is specifically tailored for cloud systems. Other frameworks like FISMA or FedRAMP Moderate/High Baselines contain more rigorous controls for higher risk environments.

What are the ongoing compliance and monitoring requirements for FedRAMP Low?

Maintaining FedRAMP Low compliance requires quarterly vulnerability scans, annual assessment of controls, continuous monitoring, incident reporting, and periodic updates to documentation. Cloud service providers must submit regular security status reports and retain authorization through demonstrated, ongoing adherence to baseline requirements.

How would SmartSuite support U.S. FedRAMP Rev. 5 (Low Impact Baseline)?

SmartSuite can help organizations manage FedRAMP Low Impact Baseline compliance by tracking risks, mapping and monitoring control implementation, and centralizing evidence collection for audits. With workflow automation, SmartSuite supports ongoing assessment activities, alerting users to compliance gaps and facilitating audit readiness. Its reporting features enable organizations to demonstrate continuous compliance to federal stakeholders.

License included / downloadable: Yes FedRAMP Rev. 5 Low Impact Baseline is publicly available from the FedRAMP website. License included with platform

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