

FedRAMP Rev. 4 – Low Impact Baseline

FedRAMP Low Impact Baseline defines security controls and authorization processes for cloud services handling low-impact federal information.



What it is

U.S. FedRAMP Rev. 4 (Low Impact Baseline) is a federal cybersecurity compliance framework that establishes a standardized approach to security assessment, authorization, and continuous monitoring for cloud services with low impact data in the U.S. federal government. Its primary purpose is to ensure that cloud products and services meet essential security requirements, particularly for agencies handling information classified as having limited potential impact on organizational operations or assets.

Published by the U.S. General Services Administration (GSA) in partnership with other federal stakeholders, FedRAMP is mandated for all federal agencies procuring cloud services. It focuses on implementing NIST SP 800-53 security controls tailored for cloud environments, addressing areas such as access management, data protection, risk management, and incident response for low impact systems.

At a glance

PUBLISHER General Services Administration (GSA)	TYPE Certification / Assurance Program	VERSION Rev. 4
EFFECTIVE May 30, 2023	DOMAIN Cloud Security	FAMILY FedRAMP
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Moderate		

Source: <https://www.fedramp.gov/legacy/>

Why it matters

- **Strengthen baseline security governance** Establish comprehensive oversight of controls to ensure basic information security for federal cloud services.
- **Enhance regulatory alignment** Support compliance with federal mandates and facilitate consistent adoption of risk management practices across agencies.
- **Increase audit readiness** Enable organizations to efficiently demonstrate security control implementation to auditors and agency partners.
- **Enable secure cloud adoption** Allow agencies to adopt cloud technologies while maintaining appropriate protections for low-risk federal information.

How SmartSuite supports FedRAMP Low

FedRAMP Low Control Library

Structure NIST 800-53 Low baseline controls with mapped owners, implementation tasks, and documentation.

System Security Plan Management

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

Risk Assessment and Authorization Tracking

Track risk assessments, control implementation status, and authorization activities.

Vulnerability and Incident Management

Manage vulnerability findings, remediation actions, and incident response workflows.

Continuous Monitoring Program

Track recurring assessments, patch management, configuration reviews, and monitoring evidence.

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 \(NIST SP 800-66 Rev. 2\)](#)[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 General Document Access Page

Provides general access to all official FedRAMP documents including guidelines and baselines.

fedramp.gov/legacy

FedRAMP FAQs

Describes frequently asked questions about the FedRAMP process and its components.

fedramp.gov/faqs

FedRAMP Marketplace

Outlines the list of cloud service offerings that have achieved FedRAMP compliance.

marketplace.fedramp.gov/#!/products?sort=productName

Frequently asked questions

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

FedRAMP Rev. 4 (Low Impact Baseline) is used to standardize security assessment, authorization, and continuous monitoring for cloud services that process federal information classified as low impact. It ensures that federal agencies and their cloud service providers implement essential security controls to protect less sensitive federal data.

Is FedRAMP Low Impact Baseline mandatory for U.S. federal agencies?

Yes, FedRAMP is required for all U.S. federal agencies seeking to procure or use external cloud services. Agencies must ensure that cloud service offerings meet FedRAMP requirements appropriate to the impact level of the data being handled, including the Low Impact Baseline for less sensitive environments.

What types of systems or data fall under the scope of FedRAMP Low Impact Baseline?

The Low Impact Baseline applies to cloud systems handling data that, if compromised, would have limited adverse effects on federal operations, assets, or individuals. Examples include publicly available information, low-sensitivity internal documents, or systems without sensitive personally identifiable information (PII).

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

FedRAMP Low Impact Baseline requires organizations to implement a specific set of NIST SP 800-53 security controls tailored for low impact systems. Key artifacts include a System Security Plan (SSP), security assessment reports, and continuous monitoring documentation, all of which are assessed by accredited third-party organizations.

How does implementation of FedRAMP Low Impact Baseline work in practice?

Cloud service providers and agencies must select and apply the required security controls, document their security posture, and submit evidence of control implementation for independent assessment. They are also responsible for conducting ongoing risk assessments and continuous monitoring to maintain compliance.

How does FedRAMP Low Impact Baseline relate to other frameworks like NIST RMF?

FedRAMP leverages the NIST Risk Management Framework (RMF) and NIST SP 800-53 controls, adapting them specifically for cloud environments in the federal context. The Low Impact Baseline aligns with these broader frameworks to enable consistency and interoperability in security and compliance.

What are the ongoing compliance and monitoring obligations for FedRAMP Low Impact Baseline?

Organizations must conduct continuous monitoring, submit periodic security updates, perform annual assessments, and respond promptly to incidents. Ongoing compliance requires maintaining evidence of control performance and participating in regular reviews by federal authorizing bodies.

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

SmartSuite supports FedRAMP Low Impact Baseline compliance by centralizing control management, tracking risk registers, and facilitating evidence collection for required security controls. The platform streamlines remediation workflows, maintains audit readiness, and provides real-time reporting and dashboards to monitor compliance status and support continuous governance.

License included / downloadable: Yes FedRAMP Rev. 4 Low Impact Baseline is publicly available on FedRAMP.gov. License included with platform

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