FedRAMP (NIST SP 800-53 Rev.4) - LI-SaaS Baseline

FedRAMP Rev. 4 (LI-SaaS Baseline) provides standardized security requirements and authorization processes for low-impact SaaS used by U.S. federal agencies.

What it is

U.S. FedRAMP Rev. 4 (LI-SaaS Baseline) is a federal cybersecurity framework that establishes standardized security requirements for Low-Impact Software-as-a-Service (LI-SaaS) solutions used by U.S. federal agencies. This specialized baseline outlines the minimum security controls necessary to protect government information processed, stored, or transmitted by cloud services with low confidentiality, integrity, and availability impact levels.

FedRAMP, or the Federal Risk and Authorization Management Program, is published and governed by the U.S. General Services Administration (GSA) in collaboration with NIST and other federal entities. Federal agencies and cloud service providers rely on FedRAMP to assess, authorize, and monitor cloud solutions for compliance with federal security, privacy, and risk management mandates. The LI-SaaS Baseline specifically applies to cloud services handling less sensitive workloads, emphasizing streamlined compliance for public-facing or non-sensitive agency applications.

At a glance

PUBLISHER Federal Risk and Authorization Management Program (FedRAMP)	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/playbook/csp/authorization/getting-started/

Why it matters

- **Strengthen federal cybersecurity governance** Establishes uniform security criteria for cloud services, enhancing centralized oversight and accountability across agencies.
- **Improve data protection assurance** Imposes strict controls that help safeguard federal information from unauthorized access, disclosure, or compromise in cloud environments.
- **Enhance regulatory compliance support** Provides a recognized framework for meeting federal requirements, streamlining audits and support for government compliance mandates.
- **Promote operational resilience** Reduces risk of service interruptions and improves response capabilities to security incidents affecting government cloud deployments.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FedRAMP LI-SaaS (NIST 800-53 Rev.4)

LI-SaaS Control Library

Structure the FedRAMP LI-SaaS baseline controls with mapped owners, documentation, and implementation tracking.

System Security Plan and Boundary Definition

Maintain SSP documentation, SaaS service boundaries, and architecture descriptions required for FedRAMP authorization.

Control Adoption and Risk Remediation

Track control adoption, risk assessments, and remediation activities across SaaS environments.

Vulnerability and Patch Management

Monitor vulnerability findings, patch remediation, and system hardening activities.

FedRAMP Continuous Monitoring Tracking

Track recurring security checks, configuration monitoring, and evidence supporting FedRAMP continuous monitoring.

FedRAMP LI-SaaS Authorization Readiness Reporting

Provide dashboards summarizing control status, open issues, and readiness for FedRAMP LI-SaaS authorization.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · HIPAA · ISO 27001:2022 · ISO 27017 · ISO 27018 · NIST CSF 2.0 · NIST 800-53 Rev.5 · SOC 2

Official resources

FedRAMP Security Assessment Framework

Defines the FedRAMP process for assessing and authorizing cloud services.

fedramp.gov/legacy/playbook/csp/authorization/what

FedRAMP LI-SaaS Baseline

Provides specific requirements for Low Impact Software-as-a-Service applications.

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

FedRAMP General Overview

Outlines FedRAMP's goals, benefits, and authorization process.

fedramp.gov

FedRAMP Templates and Checklists

Offers official templates for assessment and authorization processes under FedRAMP.

fedramp.gov/legacy

Frequently asked questions

What is FedRAMP Rev. 4 (LI-SaaS Baseline) used for?

FedRAMP Rev. 4 (Low Impact Software-as-a-Service Baseline) is used to standardize security assessment, authorization, and continuous monitoring for low-impact cloud services used by U.S. federal agencies. Its goal is to ensure that cloud providers implement adequate security controls to protect sensitive federal data at the low-impact level.

Is FedRAMP LI-SaaS Baseline certification required for all cloud service providers?

FedRAMP authorization is required for cloud service providers (CSPs) who wish to provide LI-SaaS solutions to federal agencies. While not all commercial cloud services need FedRAMP, those handling federal data, even at a low impact level, must achieve authorization to operate (ATO) per FedRAMP requirements.

What types of systems or data are covered by FedRAMP LI-SaaS Baseline?

The LI-SaaS Baseline applies to cloud applications that process, store, or transmit data classified as low impact according to FIPS 199. This typically includes systems where unauthorized disclosure, modification, or destruction of data would have minimal adverse effects on federal operations or assets.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What documentation and artifacts are required for FedRAMP LI-SaaS compliance?

Required artifacts include the System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), and continuous monitoring reports. These documents detail the CSP's security control implementation, assessment results, and remediation plans.

How does an organization implement FedRAMP LI-SaaS Baseline controls?

Implementation involves selecting applicable security controls from the FedRAMP LI-SaaS Baseline, documenting control implementation in the SSP, undergoing third-party security assessment, and maintaining ongoing continuous monitoring to ensure controls remain effective over time.

How does FedRAMP Rev. 4 (LI-SaaS Baseline) relate to other frameworks like NIST 800-53?

FedRAMP is built on the NIST SP 800-53 controls, tailoring them specifically for cloud environments used by the federal government. The LI-SaaS Baseline selects a subset of NIST controls appropriate for low-impact scenarios, ensuring alignment while tailoring requirements for cloud services.

How would SmartSuite support FedRAMP Rev. 4 (LI-SaaS Baseline)?

SmartSuite helps organizations manage FedRAMP LI-SaaS compliance by centralizing risk tracking, enabling structured control management, facilitating evidence collection for security assessments, maintaining audit readiness through real-time monitoring, and providing comprehensive reporting for ongoing compliance activities.

License included / downloadable: Yes FedRAMP Rev. 4 LI-SaaS Baseline is freely available on the official FedRAMP website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/fedramp-li-saas-baseline-nist-800-53-rev-4

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.