

GovRAMP (NIST SP 800-53 Rev.5) – Moderate

GovRAMP standardizes security assessments and continuous monitoring to authorize cloud service providers handling U.S. federal government data.



What it is

GovRAMP (Government Risk and Authorization Management Program) is a cybersecurity risk management framework that helps government agencies and their contractors assess and authorize cloud service providers to ensure data protection and compliance with federal security requirements. GovRAMP was known as StateRAMP until February 2025.

Developed and maintained by government authorities, GovRAMP is primarily used by U.S. federal agencies and cloud service providers. The program establishes a standardized approach for evaluating security controls, conducting risk assessments, and monitoring ongoing compliance for cloud-based systems that process government data. Its framework closely aligns with federal regulations and incorporates elements from NIST guidance, supporting consistent cybersecurity and compliance oversight across agencies.

At a glance

<div>PUBLISHER</div> Government Risk and Authorization Management Program (GovRAMP)	<div>TYPE</div> Certification / Assurance Program	<div>VERSION</div> Current GovRAMP Baseline
<div>EFFECTIVE</div> 2020	<div>DOMAIN</div> Cloud Security	<div>FAMILY</div> FedRAMP
<div>REGION</div> United States	<div>INDUSTRY</div> Government & Public Sector	<div>ADOPTION MODEL</div> Regulatory Compliance
<div>IMPLEMENTATION COMPLEXITY</div> Very High		

Source: <https://govramp.org/>

Why it matters

- Strengthen risk management practices** Support a consistent approach to identifying, assessing, and mitigating cybersecurity risks associated with cloud services used by federal agencies.
- Enhance compliance assurance** Demonstrate adherence to federal security requirements, reducing uncertainty around regulatory obligations for both agencies and cloud providers.
- Improve security oversight** Enable ongoing independent assessments and continuous monitoring to uphold accountability and enforce high standards of cloud security.
- Increase audit readiness** Maintain thorough security documentation and regular assessment cycles, streamlining the process of responding to compliance audits and inquiries.

How SmartSuite supports GovRAMP

Authorization Scope and System Boundary Define service scope, boundaries, and dependencies with clear documentation.	Control Baseline and Evidence Library Track required controls with owners, implementation evidence, and documentation.	Assessments and Remediation Tracking Manage findings, remediation plans, retesting, and closure evidence.
Continuous Monitoring Operations Schedule scanning, patching, and recurring evidence updates to prevent drift.	Vendor and Subservice Provider Oversight Track third-party controls, contracts, and monitoring evidence for dependencies.	Audit-Ready Reporting Report authorization readiness, open gaps, and monitoring status for stakeholders.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27001:2022

ISO 27017

ISO 27018

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Official resources

GovRAMP Program Description Provides an overview of the GovRAMP framework, its processes, and assessment requirements. govramp.org	GovRAMP Authorization Process Guide Outlines the steps involved in obtaining GovRAMP authorization for cloud service providers. govramp.org/security-program
GovRAMP Security Assessment Framework Defines the security assessment framework and controls that cloud providers must implement. govramp.org/document-library	GovRAMP Continuous Monitoring Guide Describes the continuous monitoring requirements for maintaining GovRAMP authorization status. govramp.org/security-program

Frequently asked questions

- What is GovRAMP used for?**

GovRAMP provides a standardized approach to assess and authorize cloud service providers (CSPs) used by U.S. federal agencies. It is designed to ensure that cloud-based systems handling government data conform to federal security requirements and mitigate cybersecurity risks.
- Is GovRAMP certification mandatory for cloud providers?**

GovRAMP authorization is mandatory for cloud service providers that wish to offer services to U.S. federal agencies. Without an Authority to Operate (ATO) under GovRAMP, federal agencies are not permitted to utilize a provider’s cloud solution.
- Who does GovRAMP apply to?**

GovRAMP applies to all U.S. federal agencies and any third-party CSPs that process, store, or transmit federal information in the cloud. Contractors and subcontractors providing cloud-based services for government agencies are also required to comply.
- What are the key artifacts required for GovRAMP compliance?**

Key GovRAMP artifacts include a System Security Plan (SSP), security assessment reports, and a Plan of Action and Milestones (POA&M). These documents record implemented controls, identified risks, and planned remediation efforts, supporting the authorization decision-making process.

How does the GovRAMP authorization process work?

The GovRAMP process involves defining the system scope, tailoring the FedRAMP/NIST SP 800-53 controls, completing a comprehensive SSP, engaging a 3PAO for independent assessment, and submitting an authorization package to the sponsoring agency or Joint Authorization Board (JAB) for review.

How does GovRAMP relate to NIST frameworks?

GovRAMP mandates the use of NIST SP 800-53 as its control baseline, ensuring alignment with federal information security standards. Compliance with GovRAMP leverages the same risk management principles and control families established by NIST guidelines.

What are the ongoing compliance requirements for GovRAMP?

Maintaining GovRAMP authorization requires continuous monitoring, including regular vulnerability scans, periodic reassessments, timely remediation of POA&M items, and ongoing submission of compliance evidence. Organizations must demonstrate sustained adherence to applicable security controls and respond promptly to emerging risks.

How would SmartSuite support GovRAMP?

SmartSuite supports GovRAMP management by allowing organizations to map and track FedRAMP controls, maintain a comprehensive risk register, collect and organize compliance evidence, and automate workflows for POA&M remediation. Its dashboards and reporting features enable efficient monitoring, audit readiness, and generation of authorization-ready documentation for assessments and reviews.

License included / downloadable: Yes GovRAMP program documentation and security requirements are publicly available through the GovRAMP program and official program resources.

Full framework page and mappings: smartsuite.com/frameworks/govramp-government-risk-and-authorization-management-program