SmartSuite
Framework / Cloud Security / FedRAMP

GovRAMP Security Program (NIST SP 800-53 Rev. 5)

GovRAMP verifies cloud products for U.S. state, local, tribal and education governments against NIST SP 800-53 Rev. 5, from Security Snapshot to Core, Ready and Authorized status.

What it is

GovRAMP, the Government Risk and Authorization Management Program, is a nonprofit program that verifies the security of cloud products sold to U.S. state, local, tribal and territorial governments and public education institutions, using control baselines built on NIST SP 800-53 Rev. 5. It operates as StateRAMP, Inc., doing business as GovRAMP, a 501(c)(6) organization chartered in April 2020 and renamed GovRAMP on February 14, 2025.

Cloud providers earn a verified status for a product: Core, Ready, Provisionally Authorized or Authorized, with Low, Moderate or High impact levels for Ready and above. Verified products appear on the Authorized Product List, and governments that take part write the status they require into their own procurement rules. GovRAMP is not a statute, and federal agencies use FedRAMP instead.

At a glance

PUBLISHER StateRAMP, Inc., doing business as GovRAMP (501(c)(6) nonprofit)	TYPE Certification / Assurance Program	VERSION Security Assessment Framework, Version 4.2 (NIST SP 800-53 Rev. 5)
EFFECTIVE April 21, 2026 (Version 4.2 adopted by the Board)	DOMAIN Cloud Security	FAMILY FedRAMP
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: govramp.org/security-program

Why it matters

- **A defined path from first snapshot to full authorization** Providers can begin with a Security Snapshot of 40 controls, enroll in the Progressing Security Snapshot Program, and advance to Core, Ready, Provisionally Authorized or Authorized status (Security Assessment Framework, section 1.5).
- **Recognition across governments** Verified products are listed on the Authorized Product List, so one government's review can be recognized by other state and local governments (sections 1.4.3 and 1.5.11).
- **Reuse of federal work** Fast Track requires no new audit for products with a FedRAMP Ready, Authority to Operate or Provisional Authority to Operate status (section 1.8.1).
- **Assurance that continues after approval** Providers submit monthly vulnerability scans and plan of action updates, and the PMO and the government can revoke a status through the escalation process (sections 1.7.1 to 1.7.5).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports GovRAMP

Impact Level and Boundary Record

Record the impact level chosen with the Data Classification Tool, the authorization boundary and each interconnected technology that needs its own GovRAMP or FedRAMP status or a current Snapshot (sections 1.5.4 and 1.5.6).

Status Pathway Tracker

Follow each product from Security Snapshot to Core, Ready, Provisionally Authorized or Authorized, with target dates, the 12-month status expiry and the six-month In Process limit.

Security Package Checklist

Track the SSP, 3PAO plan and report, boundary diagram and POA&M, each with an owner and review state, before submission to the PMO (section 1.5.9).

POA&M and Findings Register

Record each weakness from the SAR with a remediation owner, schedule and closure evidence, then track it through continuous monitoring (section 1.5.8).

Continuous Monitoring Calendar

Schedule monthly vulnerability scans, monthly POA&M updates and the annual 3PAO assessment of about one third of controls, and remind owners with SmartSuite automations (section 1.7.1).

Subservice Provider Oversight

Keep a record of each interconnected technology with its GovRAMP, FedRAMP or Snapshot status, contract dates and review notes in Third Party Risk Management.

Common framework mappings

CSA CCM v4 | 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 home page

GovRAMP's home page, with the Security Program, membership options and news.

govramp.org

GovRAMP Security Program

The step-by-step pathway from Security Snapshot to Core, Ready, Provisional and Authorized verification, with overlays.

govramp.org/security-program

GovRAMP Security Assessment Framework (version 4.2)

The framework that defines roles, statuses, the security package, continuous monitoring and Fast Track.

govramp.org/hubfs/GovRAMP%20Security%20Assessment%20Framework%20(July%202026).pdf

GovRAMP Continuous Monitoring Guide and Escalation Process

Monitoring activities, reporting expectations and escalation steps for maintaining a verified status.

govramp.org/hubfs/Continuous%20Monitoring%20Guide%20and%20Escalation%20Process.pdf

Frequently asked questions

What happened to StateRAMP?

StateRAMP announced on February 14, 2025 that it would operate as GovRAMP. StateRAMP, Inc. remains the legal name, and existing contracts and memberships continued without interruption. The change reflected a scope wider than state government, covering local, tribal and educational institutions.

Is GovRAMP required by law?

No. GovRAMP is a nonprofit program, not a statute. A participating government decides whether to require a GovRAMP status in its own procurement policy, and the Participating Government Organizations page on govramp.org lists how each one adopts it. Federal agencies use FedRAMP.

What are the GovRAMP statuses?

Core is validated by the PMO against 60 prioritized controls and needs no 3PAO. Ready adds a 3PAO Readiness Assessment Report. Provisionally Authorized and Authorized need a 3PAO Security Assessment Report and approval by a sponsoring government or the Approvals Committee (Security Assessment Framework, sections 1.5.3 to 1.5.7). Ready and above are assessed at a Low, Moderate or High impact level.

Can a FedRAMP-authorized product use Fast Track?

Yes. Fast Track requires no new audit for products with a FedRAMP Ready, Authority to Operate or Provisional Authority to Operate status. The provider submits the same audit and security package to the GovRAMP PMO and can start before the FedRAMP review finishes (section 1.8.1).

What does a provider do after it is verified?

It maintains continuous monitoring: vulnerability scans at least monthly, a monthly executive summary and plan of action update, and an annual 3PAO assessment of roughly one third of the controls (section 1.7). A provider that fails to maintain monitoring can face escalation and revocation of its status.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

License included / downloadable: Yes The Security Assessment Framework, templates and guides are published free of charge in the GovRAMP Document Library at govramp.org. Membership and PMO fees apply to providers who seek a status.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.