GovRAMP offers several distinct programs.

Use this checklist to identify the best fit for you.

Then work through the remaining steps to achieve your GovRAMP goals and find out how Securisea can help.

GovRAMP, formerly known as StateRAMP, offers four different programs that each offer some kind of verified status. The work required to achieve verified status differs meaningfully between each GovRAMP program. Selecting the wrong fit could cost your organization significant time and money.

This checklist does two things: It helps you identify which program is the best starting point for your organization, and it walks you through seven preparatory steps to achieving GovRAMP recognition. Each preparatory step calls out specific program-to-program differences you'll want to be aware of. Read the first checklist item, get a sense of which program fits you best, and read the remainder of the checklist through that lens.

☐ 1. Locate yourself on the GovRAMP map

Under GovRAMP, your cloud offering could be eligible for several different programs. The GovRAMP program you select determines the *complexity* of your GovRAMP assessment as well as the potential *benefits* your GovRAMP status provides once you achieve it.

Important note: GovRAMP lets you begin your journey at any of these four points. Companies building up newer security and risk-management programs may benefit from entering at one of the earlier points, such as Progressing Snapshot or GovRAMP Core. Companies with more mature security programs, for example those with pre-existing security certifications and well-documented policies and procedures, may prefer to move more quickly to a GovRAMP Ready or GovRAMP Authorized assessment.

The four lanes at a glance:

Lane	# of Controls to implement and assess	Assessed by	Sponsor required?	Primary artifact	Typical timeline
Progressing Snapshot	40	GovRAMP PMO	No	Quarterly Snapshot score	Ongoing quarterly cycles
Core	60	GovRAMP PMO	No	SSP and evidence package	3 to 6 months
Ready	80 or more	Independent 3PAO	No	Readiness Assessment Report	6 to 9 months
Authorized	Full baseline	Independent 3PAO	Typically Yes	Security Assessment Report and penetration test	9 to 18 months

- *Looking to start from scratch?* The **Progressing Security Snapshot** is the *simplest, lowest-cost entry point to GovRAMP*. Your system undergoes an assessment with the GovRAMP PMO against 40 fundamental NIST controls. This assessment is designed to help you and the PMO understand your current security posture. This assessment is ***repeated quarterly***, and you can take advantage of monthly hour-long advisory calls with GovRAMP's security team as you continuously work to improve the security of your system and "progress" toward one of the next GovRAMP programs. GovRAMP reports that Progressing Snapshot participants improve control performance by 40 to 60 percent within the first year. Note that since January

1, 2026, participants must demonstrate active improvement between quarterly reports to keep their listing, so enrollment in Progressing Snapshot is a commitment to visible, ongoing progress.

- *Looking for a GovRAMP Authorized Product List listing without breaking the bank?* **GovRAMP Core** is the next entry point. Companies seeking GovRAMP Core undergo assessment of 60 foundational NIST controls aligned with the MITRE ATT&CK Framework and the Moderate baseline. GovRAMP Core assessments are reviewed directly by the GovRAMP PMO with no 3PAO assessment. Systems with Core designation can prove that they meet baseline security controls, and these systems are listed on the GovRAMP Authorized Product List, providing crucial visibility to potential customers.
- *Seriously entering the SLED market? Looking for a credible listing on a short timeline?* **GovRAMP Ready** sits between GovRAMP Core and GovRAMP Authorized. Ready requires that you meet the Minimum Mandatory Requirements, approximately 80 controls, assessed by an official 3PAO assessment firm (such as Securisea), and documented in a formal Readiness Assessment Report. GovRAMP Ready is a significant milestone which does not require a government sponsor.
- *Do you have government buyers (non-federal) asking you for full GovRAMP authorization?* You are in the **GovRAMP Authorized** lane. This is the top-line, marquee GovRAMP program. Achieving it requires implementation of all applicable controls for your security baseline, a 3PAO Security Assessment Report, a penetration test, and a government sponsor. (GovRAMP's Approvals Committee may be available to you as an alternate sponsorship route).

In a growing number of cases the market settles the question for you. Nevada's March 2026 mandate requires providers awarded contracts after July 2026 without a verified status to enroll in the Progressing Snapshot within 45 days of award, show quarterly progress toward a Terminal Security Status, and supply ConMon artifacts through the life of the contract. North Carolina opened a one-year on-ramp running April 1, 2026 through April 1, 2027, and multiple states began adopting Core verification in 2025. Texas matters for a different reason: enrolling in the Progressing Snapshot qualifies you for TX-RAMP Provisional status without the standard 18-month expiration, and Core, Ready, and Authorized are each recognized as equivalent to TX-RAMP Level 2. Check the requirements in your target states first as you work to determine best fit.

Any questions? Reach out to Securisea and we can help identify which program best fits your needs.

Already been through this process with FedRAMP? GovRAMP Fast Track offers an expedited route to a GovRAMP status for systems which already hold FedRAMP certification.

☐ 2. Confirm organizational and technical readiness

Before controls and documentation, take stock of the fundamentals that tend to stall GovRAMP projects:

Scope definition. Scope disputes surface early and repeatedly. Efforts without a sponsor who holds decision authority sit idle waiting for someone to settle them. Pay special attention to how your system connects to other, external systems—and make sure to review Step 4 on this checklist for more info.

Budget scope. Budgets built around assessment fees alone leave nothing for the remediation efforts those fees will surface. Achieving and maintaining GovRAMP listing is an ongoing process, not a one-off.

GovRAMP membership. Membership that is not yet in place holds up everything downstream.

Product stability. Brand-new products—those still in active, early development—tend to drift. If the system you document in month one no longer resembles the system under assessment in month five, GovRAMP may prove challenging for your team.

End-of-life software inside the boundary. EOL components in scope are a recurring source of findings. Compensating-control arguments rarely resolve these issues cleanly.

Encryption validation. Be ready to verify that a vendor's claim of FIPS-validated encryption holds up at the module level.

Accountability. Programs run by committee move at the pace of the least available member.

Potential culture changes: Meeting rigorous security controls can require significant changes for organizations that might be used to doing things "on the fly". Be prepared to build (and document!) processes within your organization which are *repeatable, consistent, trackable,* and *enforceable*.

> *These fundamentals apply in every lane. That said, tolerance for an unstable system or documentation-in-progress tends to narrow considerably as you move from Snapshot toward Authorized.*

☐ 3. Categorize your data and select your baseline

Before you draw a boundary, determine the sensitivity of the government data your system will store, process, or transmit. Categorization sets your impact level, your impact level sets your control baseline, and your baseline drives the control count in every item that follows. This decision is expensive to revisit, because it usually surfaces late.

Work through:

- Which categories of government data the system handles
- Whether any of it carries a regulatory overlay such as criminal justice information, protected health information, or federal tax information
- The confidentiality, integrity, and availability impact of a compromise
- Which baseline your categorization supports, and whether your target states or contracts specify one

Document the reasoning, not just the conclusion. Assessors and sponsors will ask why you landed where you did, and a defensible categorization memo keeps the question from being reopened mid-assessment.

> ***Path delta:*** *Progressing Snapshot and Core programs contain the same number of controls for all systems. Once you pursue Ready or Authorized, you'll have to select a baseline and defend that choice.*

☐ 4. Draw your boundary

Determine exactly what sits inside, and at the edge of, your authorization boundary:

- Define boundary architecture
- Identify system components
- Track and depict data flows
- Identify supporting services
- Document *every* external system your product/system connects to

Then produce architecture and data-flow diagrams a reviewer can follow without a walkthrough call. Boundary definition is the most common place readiness efforts stall, and the cause is nearly always unresolved scope rather than missing technology.

GovRAMP has specific rules about "system interconnections." System interconnection, in simpler terms, means any connection between YOUR system and some other, external system. A common example might be a cloud-based vulnerability scanner which is developed by a third party, licensed by you, and which scans your infrastructure. The potential issue, in short, is that GovRAMP *wants you to use GovRAMP- or FedRAMP-authorized products.* Relying on interconnected technologies that are not themselves GovRAMP or FedRAMP Authorized typically results in

Provisional Authorization rather than full Authorized status. Draw the Authorization Boundary tightly enough to defend and broadly enough to account honestly for everything that handles government data.

> ***Path delta:*** *every lane requires a defined boundary, but only Ready and Authorized submissions put that boundary in front of a 3PAO.*

☐ 5. Build your documentation package

As you progress through the GovRAMP process, many organizations will require an SSP. (Only the Progressing Snapshot Program does *not* require a completed SSP). GovRAMP provides an SSP template for this purpose, and your completed SSP serves as the anchor artifact for any GovRAMP Core/Ready/Authorized assessment.

GovRAMP also requires detailed policies and procedures which define your organization's processes for meeting various security controls. GovRAMP baselines rest on NIST 800-53 Rev. 5 across 20 control families, and a full authorization spans a significant number of security and privacy controls. Your organization will need to document controls for each of these control families.

> ***Path delta:*** *Progressing Snapshot and Core accept partial documentation completion. Ready requires at least 50% of your documentation be complete. Authorized requires 100 percent documentation.*

☐ 6. Clear your assessment gate

Each lane has one gate, and they are not interchangeable. For Progressing Snapshot and Core, your organization submits directly to the GovRAMP PMO for review, with no third-party assessment in the path.

Ready and Authorized both require you to hire a Third-Party Assessment Organization (3PAO). For both of these programs, your contracted 3PAO will perform assessment, collect evidence, interview your personnel, and prepare a formal report.

For Ready, the assessment ends with a Readiness Assessment Report indicating whether you meet the Minimum Mandatory Requirements. Authorized requires a more detailed 3PAO Security Assessment Report, a penetration test, and a government sponsor, with the Approvals Committee available as an alternative route to sponsorship.

☐ 7. Commit to the monitoring rhythm

Continuous monitoring becomes mandatory once a status is awarded, and it functions as an operating commitment rather than a closeout task. You will need named owners, a scanning and reporting calendar, a POA&M process that closes items instead of accumulating them, and a significant-change process that triggers before changes ship. Continuous Monitoring in some form applies to ***all*** GovRAMP programs, including Progressing Snapshot.

> ***Path delta:*** *the rhythm scales with the lane. Progressing Snapshot participants re-score quarterly and can use the monthly advisory calls to their benefit. Core, Ready, and Authorized carry progressively heavier scanning, reporting, and POA&M obligations, with Authorized subject to the fullest significant-change review.*

Working with Securisea

Securisea maintains both a GovRAMP advisory practice and an accredited 3PAO assessment practice. Independence requirements mean we can serve any single client in one of those roles, never both for the same system. GovRAMP requires a two-year cooldown for 3PAOs between advisory work and any later assessment of that client.

Our **advisory** practice works with providers before assessment: lane selection, categorization, boundary definition, gap analysis, documentation development, and control implementation planning.

Our **assessment** practice performs Readiness Assessments and Security Assessments as an independent third party, evaluating and reporting on what we observe against GovRAMP requirements. In that role we do not design, implement, or remediate the controls under assessment, and we do not advise the clients we assess.

If a state mandate has changed your timeline, tell us where you stand and we will confirm which role we can take, or point you to another qualified firm for the other.

Learn more: securisea.com/govramp-compliance-services

Sources: GovRAMP Advances 2026 Modernization and National Adoption · Upcoming Changes to the GovRAMP Progressing Security Snapshot Program · GovRAMP Progressing Snapshot · FedRAMP Recognizes GovRAMP in Updated Class A Rules · Nevada Office of the CIO GovRAMP Press Release, March 2026 · North Carolina Understanding GovRAMP: Agency Procurement Overview