GovRAMP Overview

2026

What is GovRAMP?

Creating a framework for continuous improvement in cybersecurity for state & local governments, providers, and the constituents they serve.

Government Risk Authorization Management Program

Who We Are

A 501(c)(6) nonprofit membership organization that supports state, local, federal, educational, tribal, and nonprofit organizations **in securely adopting cloud technologies**.

A Government Engagement Team (GET) and Program Management Office (PMO) working to **advance cybersecurity standards and procurement efficiency** for our participating organizations.

What We Do

Establish a **standardized, streamlined security verification process** for cloud service providers.

Maintain an Authorized Product List of cloud products that meet GovRAMP's security standards.

Serve as a no-cost, trusted partner for SLED agencies.

How We Do It

Leverage NIST 800-53 Rev. 5 framework to assess and verify security of cloud products.

Facilitate a **shared security assessment process** to reduce redundancy and increase procurement efficiency.

Provide transparency through continuous monitoring.

Support governments throughout every step of the GovRAMP adoption process.

As Cyber Threats Grow, How Do You Know…

If a cloud solution that is being used to deliver services that transmit, store, and/or process your data ***could impact security***?

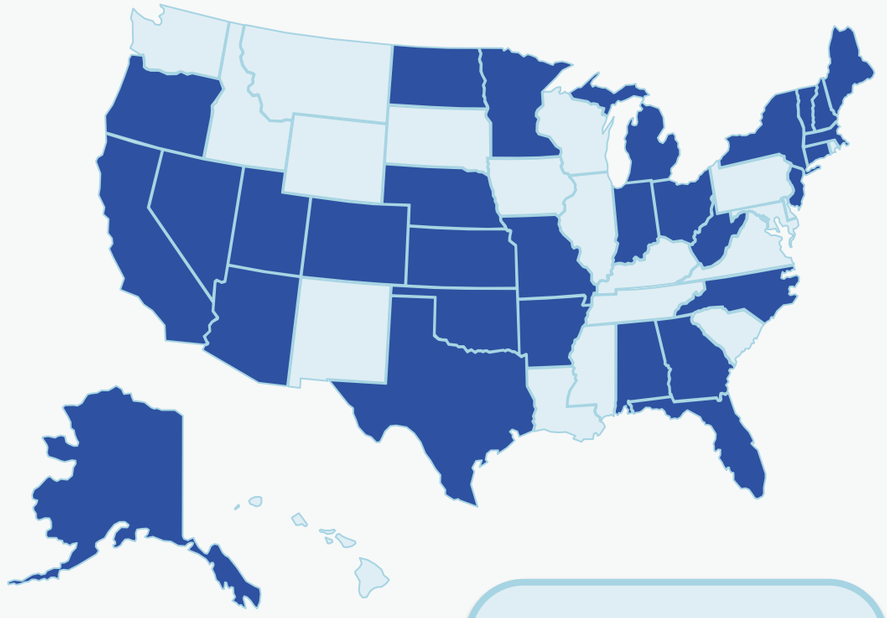
If bidders meet minimum security standards ***before*** making an award for contract?

If a contracted product complies with your security standards ***throughout the duration of the contract***?

Verify Once, Serve Many

As a result of partnership with GovRAMP:

- **Service providers complete one comprehensive verification process,** including continuous monitoring, that is shared with GovRAMP's participating organizations.
- **Governments can increase efficiency in procuring verified cloud products**, reducing costs of managing cybersecurity risk.
- **Governments and service providers are united under one standardized framework** to validate the cybersecurity posture of cloud products serving the public sector.



- 32 States/Agencies
- 1 Federal
- 9 Higher Ed
- 9 K-12 School Districts
- 17 Local Organizations
- 1 Tribal

GovRAMP's Security Framework & Statuses

Standardizing and streamlining the security verification process for safer, more efficient Cloud procurement

GovRAMP Terminology

Service Provider

Provider who utilizes IaaS, PaaS and/or SaaS to process, store and/or transmit data

3PAO

Third Party Assessment Organizations

Conducts audits and assessments

30+ accredited by FedRAMP

Security Packages

Documentation of a cloud system's security

Impact Levels

Based on sensitivity of data and criticality of system

Aligned with FedRAMP and NIST 800-53 Rev. 5

Security Status

Status of security authorization

Milestone statuses: Core, Ready, Provisionally Authorized and Authorized

PMO

Program Management Office

Reviews 3PAO audits and recommends security status based on board-adopted policies

Authorized Product List

Directory of providers' offerings with GovRAMP Security Status or progressing towards a security status

Fast track process for FedRAMP approved offerings

GovRAMP's Security Framework

GovRAMP's baseline requirements are built on NIST 800-53 Rev. 5.

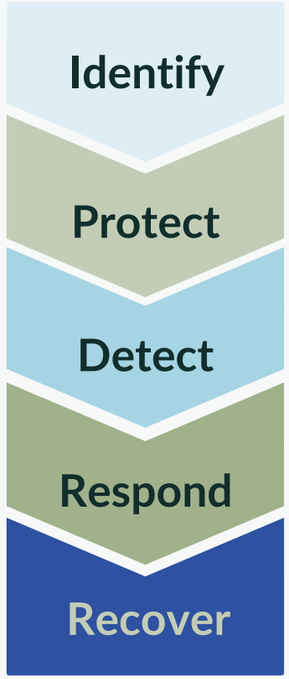
This streamlined, comprehensive authorization process:

- Reduces barriers to security for all sizes of service providers
- Minimizes the cost of security compliance for all service providers
- Provides governments a shared resource for procurement and continuous compliance & monitoring

Incorporating GovRAMP's assessment options of Progressing Snapshot, Core, Ready, Provisionally Authorized, or Authorized at the appropriate Impact Level can help you build out your RAMP program.

Find policies, templates, and resources online at: GovRAMP.org/templates-resources

The 5 Functions of NIST 800-53



GovRAMP Impact Levels

- Not every contract requires GovRAMP authorization status. The key to determining security requirements is assessing the type of data a vendor processes, transmits, or stores.
- The **Cloud Procurement Resource Tool** and **Data Classification Tool** help identify the necessary GovRAMP security requirements for cloud service providers that handle government data.
- GovRAMP has defined the following Impact Level Categories that align to NIST 800-53:

Low

GovRAMP Low Control Baselines

Moderate

GovRAMP Moderate Control Baselines

High

GovRAMP/FedRAMP High Control Baselines

GovRAMP Security Program Risk Acceptance Model

KEY

NIST* – National Institute of Standards and Technology
PMO* – Program Management Office
ConMon* – Continuous Monitoring
3PAO* – Third Party Assessment Organization

Moderate Impact

Security Snapshot

Cyber NIST score of 40 controls

Moderate Impact

Progressing Security Snapshot

Cyber NIST score of 40 controls, monthly advisory, and quarterly snapshot updates

Moderate Impact

Core Status

Demonstrates achievement with assessment of 60 NIST controls by PMO, quarterly ConMon, and documentation

Low, Moderate, and High Impact

Ready Status

Demonstrates achievement with Ready audit of 80 NIST controls by 3PAO, monthly ConMon, annual assessment, and documentation

Low, Moderate, and High Impact

Authorized or Provisionally Authorized Status

Demonstrates achievement with security audit of 300+ NIST controls by 3PAO, monthly ConMon, annual assessment, and documentation

Assessment & validation conducted by PMO

Assessment by 3PAO with PMO validation & ConMon

GovRAMP Program Offerings

Single Snapshot

Achievable in 3-6 Weeks

The evidence-based GovRAMP Security Snapshot helps service providers start their cybersecurity journey, while offering governments a first look at cloud products' risk maturity. It validates the product's maturity by examining the top 40 most impactful controls determined by MITRE's ATT&CK® Framework as the basis. The Security Snapshot is valid for a period of 12 months from the date of issuance and may be leveraged by multiple organizations during that time period.

Process:

1. Membership
2. Complete initial GovRAMP Security Snapshot

Progressing Snapshot

First Snapshot Achievable in 3-6 Weeks

A major goal of the GovRAMP Progressing Security Snapshot Program is enhancing cyber maturity among providers and fostering information sharing that facilitates effective government risk management by integrating the principles of "trust but verify" and a consultative approach.

The program includes quarterly assessments (Snapshots) and monthly consultative calls with the GovRAMP PMO Advisory team. Service providers gain insight into their products' gaps in achieving NIST-based security controls and guidance on how to best address those gaps, with a focus on what matters most for improved security outcomes.

Process:

1. Membership
2. Complete initial GovRAMP Security Snapshot
3. Complete monthly consultative calls with GovRAMP PMO Advisory team

GovRAMP Program Offerings

GovRAMP Core

Achievable in 12 Months

The GovRAMP Core security status provides an early step in verified GovRAMP statuses to demonstrate the maturity of a cloud product's security program. This early step demonstrates achievement of baseline NIST 800-53 Rev. 5 controls and documentation requirements as assessed and validated by the GovRAMP PMO. The provider may optionally submit a Pen Test. Like other GovRAMP verified statuses, the Core Status is valid for 12 months and may be extended for an additional 12 months by undergoing an annual assessment prior to the status expiration. There is no limit to the number of extensions a product may obtain.

To maintain a GovRAMP Core security status, the provider must comply with quarterly continuous monitoring requirements that include submission of evidence of Core requirement compliance as requested by the GovRAMP PMO, in addition to Web App Scans, Vulnerability Scans, Policy Compliance Scans and a POA&M spreadsheet.

GovRAMP Ready

Achievable in 12-18 Months

A Ready status indicates that the product meets GovRAMP's Minimum Mandatory Requirements and most critical controls. The Ready requirements are published here and vary by Impact Level for Low, Moderate, or High. The security package for Ready includes a Readiness Assessment Report (RAR) submitted by a GovRAMP 3PAO, attesting to the minimum mandates. The required Ready documentation, including boundary diagram, inventory worksheet, roles, and permissions matrix, must be included in the security package provided to our Security Team through the GovRAMP Program Management Office (PMO). The GovRAMP PMO provides independent validation and verification that the security package and RAR comply with the standards established by the GovRAMP governing board and committees.

GovRAMP Program Offerings

GovRAMP Provisionally Authorized

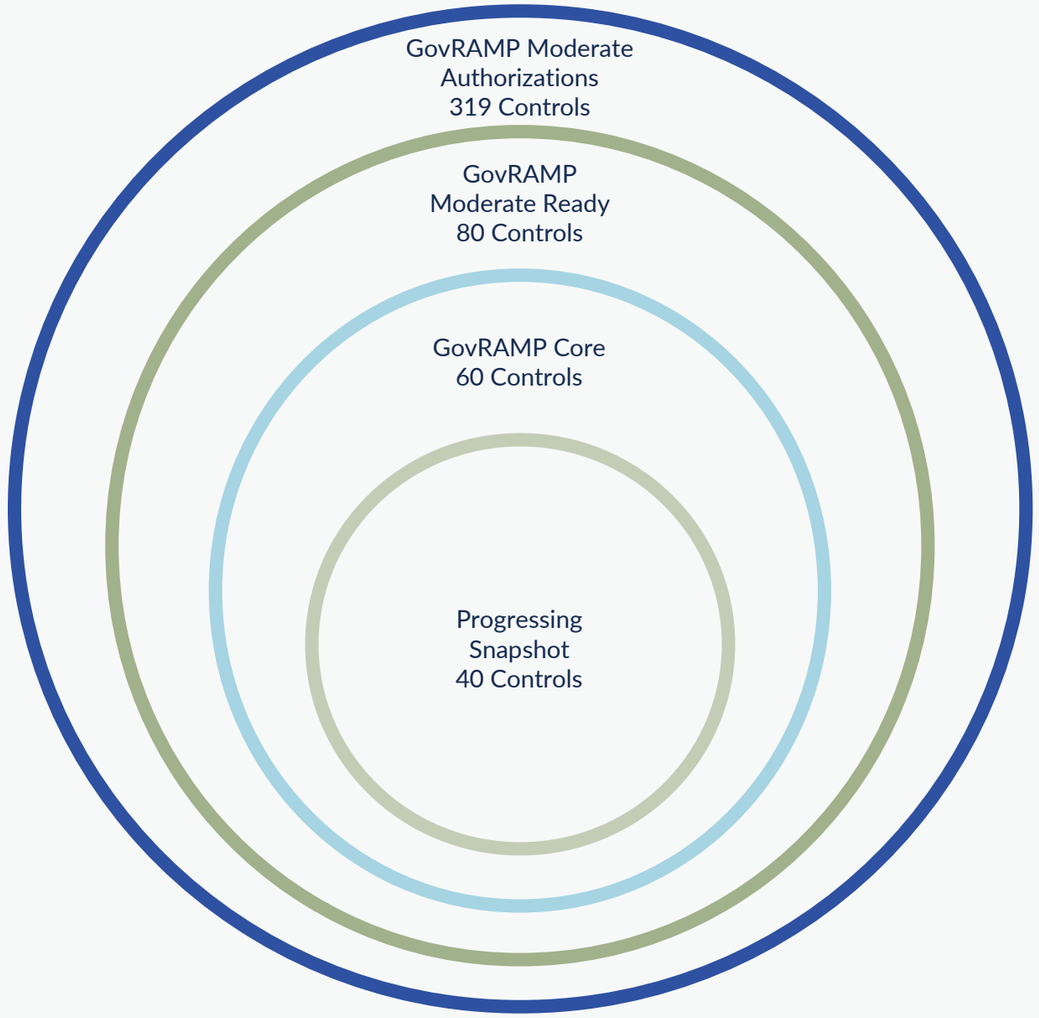
Achievable in 18-24 Months

A Provisionally Authorized status may be assigned by a sponsoring government or Approvals Committee to a package submitted for Authorized Status, if the product meets the Authorization requirements, but one of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized. To achieve Provisionally Authorized, the interconnected technology must leverage a current GovRAMP Security Snapshot.

GovRAMP Authorized

Achievable in 18-24 Months

An Authorized Status indicates the product or offering meets all the required NIST controls by impact level and the provider has completed the necessary documentation, including a 3PAO Security Assessment Report. To obtain Authorized status, a security package needs approval from the Approvals Committee or a Government Sponsorship. They will serve as authorization officials and confirm the package meets GovRAMP requirements.



Which Assessments Work for You?

Making Waves by Advancing Security

Successive Achievement

- Each GovRAMP Status builds on the previous and advances the provider to the next status

Focus on Impact

- NIST Control Selection was based on biggest impact per the MITRE ATT&CK Framework Risk Protection Values

Removing Barriers

- Service providers often don't know where to start; you can right size your risk and show them the path to a more mature cyber posture.

CJIS Overlay

GovRAMP CJIS-Aligned Overlay Control and Parameters - GovRAMP

For criminal justice agencies ensuring that cloud-based solutions meet CJIS standards is critical to protecting sensitive data. The CJIS-Aligned Overlay streamlines the path to conformance, enabling service providers to deliver secure, compliant solutions while reducing the burden on government decision-makers.

The overlay provides essential guidance for service providers by:

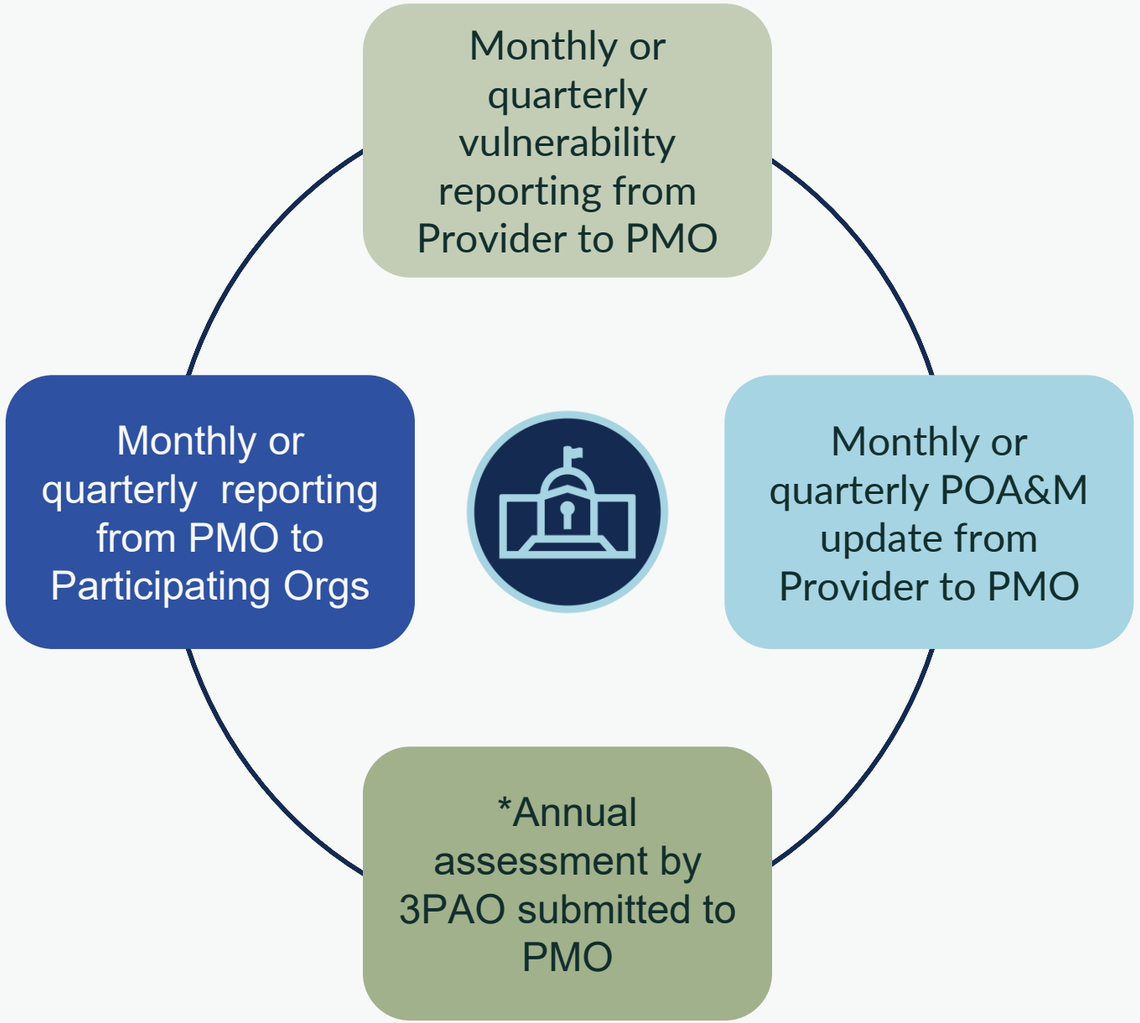
- **Streamlining the Assessment Process**: The overlay consolidates CJIS requirements with GovRAMP's existing framework, reducing redundancy and confusion.
- **Providing Clear Direction**: Each control is mapped to CJIS Policy 6.0, offering straightforward guidance on how to implement and assess compliance.
- **Facilitating Informed Decision-Making**: By clarifying a product's CJIS conformance, the overlay empowers agencies to evaluate cloud solutions confidently.

Reciprocity: FedRAMP Authorizations

To expedite the process of achieving a verified GovRAMP status for FedRAMP Rev. 5 products, organizations can enroll in the GovRAMP Fast Track Program.

Benefits:

- No need to re-engage a 3PAO, you may submit the same FedRAMP security package for review even if the FedRAMP review process has not been completed.
- Only required to cover the cost of membership, the GovRAMP PMO technical review and continuous monitoring fees.
- Allows participating organizations to meet continuous monitoring requirements where FedRAMP does not provide continuous monitoring visibility to non-federal agencies.
- GovRAMP does not require a government sponsor or contract in order to receive a verified status.
- Turnaround time is 6-8 weeks from date product entered the GovRAMP PMO queue but may be longer based on the quality of the package submission and/or the number of products in queue ahead of you (including those waiting for approvals committee review).



Continuous Monitoring

Providers must comply with Continuous Monitoring (ConMon) requirements to maintain the status of Core, Ready, Authorized, or Provisionally Authorized.

Providers may grant viewing access to Participating Governments at the Standard Access level or the Elevated Access level.

View GovRAMP policies that establish our security standards & requirements here: **GovRAMP.org/templates-resources**

Continuous Monitoring – Requirements and Reviews

Service Providers with products categorized as Low or Moderate security must follow these upload schedules for the GovRAMP Box Portal:

- **GovRAMP Core**: Upload packages quarterly
- **GovRAMP Ready, GovRAMP Authorized/Provisionally Authorized**: Upload packages monthly

Packages include:

1. POA&Ms (Plan of Action and Milestones)
2. An updated inventory workbook
3. OS, DB, and web application vulnerability scans
4. Deviation Request Form to support POA&M Risk Adjustments, Operational Requirements, and False Positives
5. Executive summary of the above items

The GovRAMP PMO reviews the submitted documentation. The results are recorded and documented in the review document. Findings discovered through the GovRAMP PMO's review may trigger a greater frequency of continuous monitoring activities and impromptu requests for evidence regarding the most recent assessment. Failure to comply with the continuous monitoring plan and requirements may result in corrective action or revocation of the verified security status.

Adoption Models: How do you use the program?

Deciding what adoption model works best for your organization in order to streamline third-party cloud security risk assessments

Adoption Options: GovRAMP Require

Requiring GovRAMP ensures a unified, secure, and efficient approach to managing third-party cloud services within your organization. It provides a standardized framework for assessment and monitoring, reduces duplication of effort, and sets clear expectations for vendors, ultimately strengthening overall information security governance.

GovRAMP Best Practice

Require

Requiring GovRAMP is best practice as it offers the most benefit with the least drawbacks.

- ✓ Streamlined, standardized assessment for all third-party cloud products handling organizational data.
- ✓ Centralized continuous monitoring and artifact repository for improved oversight and transparency.
- ✓ Supports transition to an oversight model, reducing operational burden on agency security teams.
- ✓ Clear signal to vendors about security requirements before contracting, minimizing compliance gaps.
- × Initial change management lift is challenging, but long-term benefits outweigh short-term effort

GovRAMP Adoption Tiers for SLED Agencies

Hybrid	Prefer	Accept
Where organizations can accept, prefer, or require compliance when necessary—offers both benefits and challenges.	Helps promote security and simplifies assessments for compliant products but can create inconsistencies and operational complexity.	Leverages existing security programs and promotes standards, but can create inconsistencies and additional burdens for internal teams.
✓ Leverages GovRAMP Continuous Monitoring - provides ongoing security oversight for participating cloud products, improving risk management. ✓ Encourages Provider Community Alignment with NIST 800-53 - promotes adoption of standardized security controls, strengthening overall security posture. × Lacks Consistent Apples-to-Apples Comparisons - Variability in provider implementations makes it difficult to uniformly compare security levels across vendors.	✓ Encourages provider community alignment with NIST 800-53 standards. ✓ Makes it easier for governments to assess cyber maturity for GovRAMP products. × No guarantee that proposed products meet specific security needs. × No apples-to-apples comparison of products' cybersecurity posture. × Continuous monitoring oversight may be ad hoc or decentralized.	✓ Leverages GovRAMP continuous monitoring for participating cloud products. ✓ Encourages provider community to move toward NIST 800-53 standards. × No apples-to-apples comparison of products' cybersecurity posture. × Continuous monitoring oversight may be ad hoc or decentralized. × Burden remains on internal information security teams to complete risk assessments × Creates a less streamlined security process for the vendor community

Benefits of GovRAMP Adoption

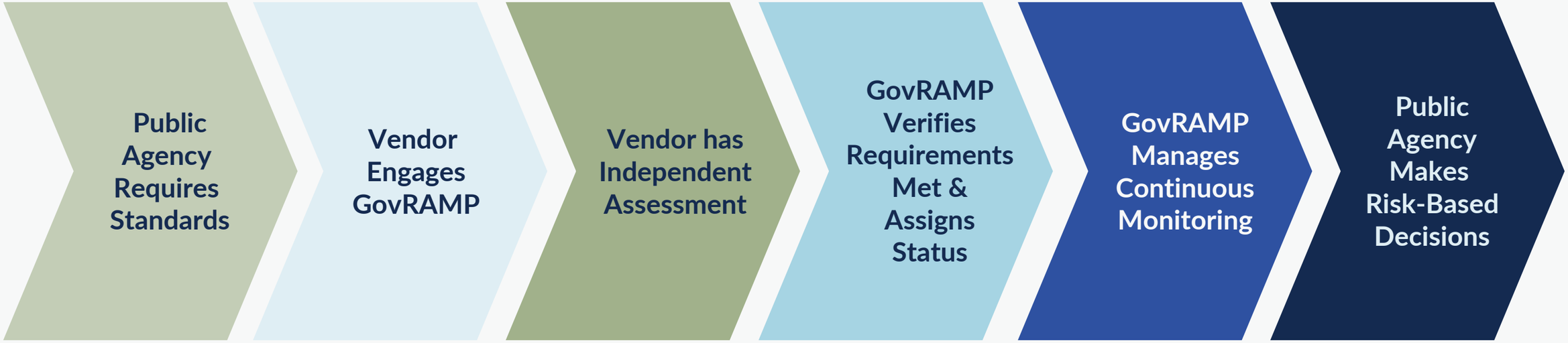
Benefits for Government

- Reduced procurement timelines
- Consistent, reusable risk decisions
- Standardized security expectations
- Continuous monitoring across the contract lifecycle

Benefits for Providers

- Verify once, serve many customers
- Lower compliance and audit costs
- Clear, predictable security requirements
- Expanded access to government markets

GovRAMP: Trust but Verify for Secure Procurement



Authorized Product List

Verified and Progressing Products are listed on the Authorized Product List and updated daily.

- Our Authorized Product List is a public list on **govramp.org/product-list/**
- Section 1: Ready, Authorized, Provisionally Authorized Product
  - Total Products: 135+
- Section 2: Progressing Snapshot Program, Active, Pending, In Process Products
  - Total Products: 190+
- Continuous monitoring is required to maintain a verified listing of Core, Ready, Authorized, and Provisionally Authorized

Participating GovRAMP Governments can be provided secure access to GovRAMP portal to view continuous monitoring upon provider approval.

How Do I Get Started?

Contact Information

To start your adoption journey or if you have questions, please reach out to:
GET@GovRAMP.org.

Interested in becoming a member? Individual and participating government memberships are available at no cost!

Visit https://govramp.org/memberships/ to sign up.

GovRAMP Resources

REV 5 Templates and Resources
Cloud Procurement Resource Tool
Participating Governments
Authorized Product List - GovRAMP
Security Assessment Framework
GovRAMP Memberships

Communications & Events

- GovRAMP Blog
- Register for the GovRAMP Learning Series
- AI Task Force
- Sign up for GovRAMP Communications
- Upcoming GovRAMP Events
- LinkedIn