State of Utah and GovRAMP

Key Contacts

GovRAMP Program Management Office (PMO)
GovRAMPPMO@rampquest.com
State of Utah Contact
dts-compliance@utah.gov

Applicable Policies

State of Utah - Information Security Policy

Determine the Required GovRAMP Pathway

The required GovRAMP pathway is determined by the government, based on risk, data sensitivity, and system impact.

Common pathways include:

- **Security Snapshot / Progressing Snapshot –** Evidence-based assessment supporting risk visibility and maturity
- **GovRAMP Core –** Baseline cybersecurity requirements
- **GovRAMP Authorized / Provisionally Authorized –** Full authorization with ongoing monitoring

Vendor Action:
□ **Confirm required GovRAMP pathway with the government**
Typical Timing: At procurement kickoff or contract award

GovRAMP Prerequisites

Maintain Active GovRAMP Membership
All vendors pursuing GovRAMP statuses must maintain an active GovRAMP Membership
□ Confirm **GovRAMP membership level**
□ Ensure membership is current (memberships renew annually on June 1)

Review GovRAMP Resources
□ Review applicable GovRAMP templates and guidance
□ Understand artifact and evidence expectations
Tip: Early familiarity with templates reduces delays later in the process.

Select a 3PAO (If Applicable)
For pathways requiring independent assessment:
□ Review the GovRAMP Authorized 3PAO list
□ Engage a 3PAO early to support scheduling and readiness

Assessment & Authorization Activities

The table below outlines typical tasks vendors complete as they progress toward GovRAMP authorization. Governments may adjust sequencing or timelines based on procurement needs.

Complete	Task	Typical Timing	Notes / Remarks
☐	Confirm required GovRAMP pathway with government	Procurement kickoff / contract award	Government determines pathway based on risk and data sensitivity
☐	Confirm active GovRAMP membership	Prior to program entry	Memberships renew annually on June 1
☐	Review applicable GovRAMP templates and guidance	Early in process	Reduces rework and delays
☐	Select and engage a GovRAMP-authorized 3PAO (if required)	Early in assessment planning	Applicable for Authorized pathways
☐	Request Security Snapshot / Progressing Snapshot (if required)	Within 60 days of contract execution	Government may adjust timing
☐	Prepare and submit required evidence and artifacts	Assessment phase	Coordinate with GovRAMP PMO and 3PAO
☐	Complete assessment activities	Ongoing	Address findings as identified
☐	Submit compliance materials through GovRAMP	As required	Track status with PMO
☐	Obtain official GovRAMP status letter	Upon status determination	Active, In Process, Pending, Authorized
☐	Submit GovRAMP status letter to government	Upon receipt	Confirms progress toward requirements
☐	Complete remediation activities (if applicable)	As identified	Required for progression
☐	Submit authorization package through GovRAMP	Pathway dependent	Up to 12–18 months total typical timeline
☐	Confirm listing on GovRAMP Authorized Product List	Upon authorization	Notify government of confirmation
☐	Submit continuous monitoring materials	Ongoing postauthorization	Required to maintain status
☐	Maintain incident response and reporting procedures	Ongoing	Notify GovRAMP and government as required
☐	Conduct vulnerability scanning and penetration testing	Ongoing	Address findings within required timeframes
☐	Ensure continuous monitoring access is granted to government customer upon request	Ongoing	Provides required visibility and transparency to government partners

This checklist aligns to current GovRAMP requirements and guidance. Governments may supplement this checklist with additional procurement-specific requirements as required.

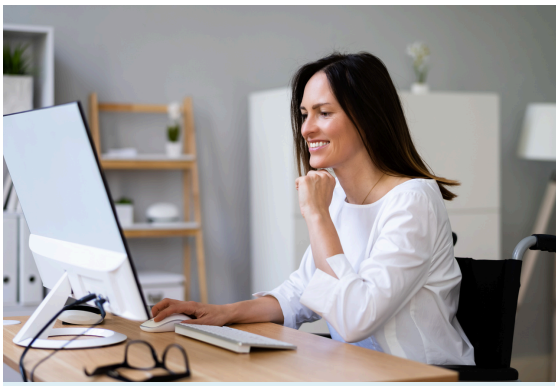
Progressing Security Snapshot

The GovRAMP Progressing Security Snapshot gives service providers clear, quarterly insight into their cloud product's security maturity. Each Snapshot evaluates the 40 most impactful NIST-aligned controls drawn from the current GovRAMP Ready control set, prioritized using the MITRE ATT&CK® Framework, and includes monthly advisory calls with the GovRAMP Program Management Office (PMO) to help providers understand gaps and steadily mature toward Verified Statuses. Snapshots help providers demonstrate measurable progress to their current and future government customers.

GovRAMP

WHO THIS IS FOR

- Early-stage or maturing service providers
- Providers preparing for Core, Ready, or Authorized
- Teams seeking regular, expert-guided security improvements



Process & Timeline

- Become a GovRAMP member
- Enroll in Snapshot Program
- Monthly Advisory Call
- Quarterly Snapshot Assessment
- Receive Maturity Report

Turnaround timeline: Progressing Security Snapshot results delivered **within 3–4 weeks from date of payment**, following enrollment and assessment kickoff.

Learn more about which governments recognize GovRAMP assessments: **www.govramp.org/participating-governments**

Key Highlights

- **Quarterly Snapshot assessments** with actionable insights
- **Monthly PMO advisory calls** focused on practical maturity gains
- **Prioritized control analysis** using high-impact, NIST-aligned controls
- **Reusable assurance** that supports multiple government engagements

Outcome for Service Providers

- A clear, data-driven understanding of current security maturity
- Continuous guidance toward Core, Ready, or Authorized
- Sharper positioning when working with government customers
- **"Verify once, serve many" value — Snapshot results can be reused across participating governments**, reducing repetitive security conversations and simplifying go-to-market efforts

2026 Fees & Investment

- **$750 / month** for providers with <$1M annual revenue
- **$1,000 / month** for providers with $1M-$5M annual revenue
- **$1,600 / month** for providers with >$5M annual revenue

Core Verification

GovRAMP Core Status demonstrates that your cloud product meets a defined set of baseline NIST 800-53 Rev. 5 controls and documentation requirements. Core gives service providers an early, Program Management Office (PMO)-validated checkpoint of their foundational security maturity without requiring a full 3PAO audit.

Achieving Core helps providers build confidence with government customers and prepares them for the more advanced Ready or Authorized assessments. Core can also strengthen market positioning by demonstrating measurable progress to prospective government customers.

GovRAMP

WHO THIS IS FOR

- Service providers building toward Ready or Authorized
- Teams preparing for full NIST control implementation
- Providers wanting PMO-validated proof of baseline security maturity



Process & Timeline

- Become a GovRAMP member
- Submit Core Evidence Package
- PMO Evidence Review
- Core Status awarded (12 mo)
- Provider Annual Assessment

Turnaround timeline: Core Verification is valid 12 months from the award date.

Learn more about which governments recognize GovRAMP assessments: **www.govramp.org/participating-governments**

Key Highlights

- PMO-validated control and documentation review
- Annual assessment with a consistent, predictable renewal path
- Clear feedback to support next-step readiness
- Recognized across participating government programs

Continuous Monitoring Requirements

Core includes **quarterly continuous monitoring**. Required submissions include:

- Updated POA&M
- Updated inventory workbook
- Operating system, database, and web application vulnerability scans
- Deviation Request Form (for risk adjustments, operational requirements, false positives)
- Executive summary of submitted materials

2026 Fees & Investment

Annual Core Assessment:

- $9,000 (< $1M revenue)
- $11,000 ($1M–$5M revenue)
- $17,000 (> $5M revenue)

Quarterly Continuous Monitoring:

- $250/qtr (< $1M revenue)
- $500/qtr ($1M–$5M revenue)
- $1,000/qtr (> $5M revenue)

Authorized / Provisional Verification

Authorized is the highest GovRAMP verification level. It requires a full 3PAO Security Assessment Review (SAR), a complete security package (including the SSP and boundary documentation), Program Management Office (PMO) validation, and final approval from a sponsoring government or the GovRAMP Approvals Committee.

Provisionally Authorized is issued when a product meets authorization requirements except for a small number of remediable issues—such as an interconnected technology requiring a GovRAMP Snapshot or minor findings that can be addressed through a POA&M entry.

GovRAMP

IMPACT LEVELS

Low Impact
Moderate Impact
High Impact
Moderate + CJIS Overlay



Process & Timeline

- Become a GovRAMP member
- 3PAO performs full SAR
- Submit Complete PMO Package
- PMO Validates Evidence
- Sponsor Issues Status
- Monthly Continuous Monitoring

Turnaround timeline: Authorized or Provisionally Authorized status is achieved **within 18–24 months** from enrollment, following 3PAO assessment, PMO validation, and sponsor approval.

Learn more about which governments recognize GovRAMP assessments: **www.govramp.org/participating-governments**

Who This Is For

- Service providers ready for full GovRAMP authorization
- Providers completing the final steps through a provisional path
- Teams needing independently audited NIST 800-53 control compliance
- Cloud products entering or expanding government markets

Continuous Monitoring Requirements

Authorized and Provisionally Authorized products follow **monthly continuous monitoring**, which typically includes:

- Updated POA&M
- Updated inventory workbook
- Operating system, database, and web application vulnerability scans
- Deviation Request Form (for risk adjustments, operational requirements, false positives)
- Executive summary of submitted materials

2026 Fees & Investment

Annual Review:

- $1,500 (< $1M revenue)
- $5,000 ($1M–$5M revenue)
- $7,500 (> $5M revenue)

Monthly Continuous Monitoring:

- $250/mo (< $1M revenue)
- $500/mo ($1M–$5M revenue)
- $1,000/mo (> $5M revenue)

3PAO assessment fees are separate and not set by GovRAMP.