Progress Report 2025

INSIGHTS FROM THE PROGRESSING SECURITY SNAPSHOT PROGRAM

December 2025

Prepared by

GovRAMP & GovRAMP Program Management Office (PMO)

Authored by

Andy Chuang & Mattie Gullixson

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Compliance as a Security Strategy

Unorthodox, but effective

In the cybersecurity world, compliance is often seen as a necessary evil — the box-checking exercise that happens after the real work of security is done. But the Program Management Office (PMO) is quietly turning that perception on its head through its support of the GovRAMP Progressing Security Snapshot Program (PSSP).

Designed to provide quarterly assessments and hands-on advisory support for Cloud Service Providers (CSPs), the PSSP is a maturity accelerator.

The data tells a powerful story: structure, repetition, and feedback — the hallmarks of compliance — are becoming the drivers of measurable security progress.

This 2025 analysis draws from 181 CSPs participating in PSSP, encompassing more than 28,600 control-level data points across seven quarters of program participation.

The findings are clear:

- On average, CSPs achieve a “pass” status on controls within 2.2 quarters.
- GovRAMP participation directly correlates with improved security posture over time.
- Controls related to configuration management and identity assurance present the greatest challenge — but also the greatest potential for systemic improvement.

The results underscore an important truth: compliance done right isn’t paperwork — it’s progress.

METHODOLOGY

The findings in this report are derived from quarterly assessments submitted by 181 anonymous Cloud Service Providers (CSPs) participating in the GovRAMP Progressing Security Snapshot Program (PSSP) between January 2024 and September 2025.

Each record in the dataset includes six key variables:

CSP Identifier (anonymized)
Join Quarter – the quarter when the CSP entered the program
Relative Quarter – the CSP's position in the program timeline (1–7)
Current Quarter – the actual calendar quarter of reporting
Control ID – one of the 40 NIST 800-53 Rev. 5 controls monitored
Result – binary outcome (0 = Fail; 1 = Pass or Pass with Concern)

The long-format dataset captures 7 quarters × 40 controls per CSP, totaling **28,600 observations**. Controls span domains such as Access Control (AC), Configuration Management (CM), and Incident Response (IR).

Handling & Limitations

- All provider names and identifiers were replaced with random numeric codes.
- Outliers (CSPs passing all or no controls) were retained to preserve dataset integrity.
- The eighth quarter of data was unavailable at the time of analysis.

This analysis reflects aggregated trends, not individual performance. All data was analyzed for statistical consistency and visualized using quarterly averages.

Table 41: Total Count of SI-07 Passed per Quarter

Control ID	Current Quarter	Passed Count
SI-07	2	2
SI-07	3	3
SI-07	4	10
SI-07	5	15
SI-07	6	19
SI-07	7	22

Table 42: Total Count of SI-07 (07) Passed per Quarter

STATE OF PROGRESS

The data reveals a clear trajectory: **time in the program drives measurable improvement.**

Across seven quarters, the average CSP demonstrates a steady climb in control pass rates, particularly between **quarters 2 through 4**, when most providers consolidate lessons from early advisory engagements and begin integrating corrective actions.

> *GovRAMP participation improves control performance by 40–60% within the first year*

This upward trend illustrates that the PSSP is not merely tracking compliance — **it is facilitating transformation**. CSPs are learning faster, documenting better, and aligning more tightly to government security standards as they progress through the program.

Note: By quarter 7, the data shows a slight dip in aggregate participation and pass counts — a likely reflection of CSPs "graduating" from the PSSP and transitioning toward Core, Ready or Authorized status.

Macro-Level Insight

The pattern is not linear — improvement accelerates through Q4, then stabilizes.

The steady early momentum suggests that GovRAMP's advisory model produces compounding returns.

Providers who remain engaged see both performance and maturity benefits.

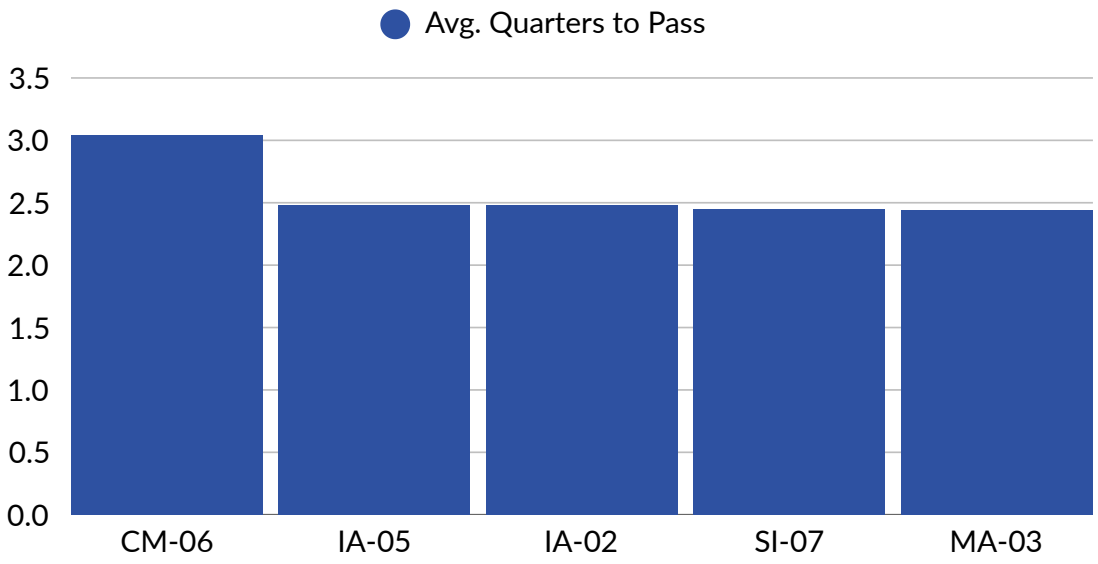
DEEP DIVE

Control Performance & Trends

Not all controls are created equal. Some represent quick wins; others, enduring challenges that test a provider's operational discipline.

Controls that Take the Longest to Pass

Five controls stand out as the most time-consuming to achieve compliance:



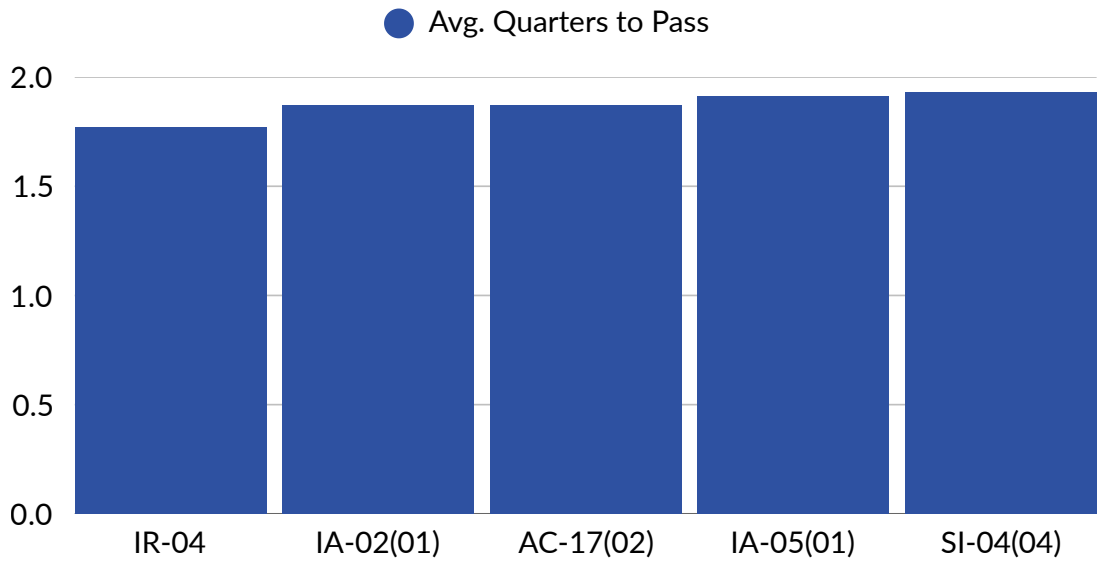
These controls share a common characteristic: they depend not only on policy documentation but also on sustained operational proof. In other words, they are as much about maturity as they are about mechanics.

CM-06 alone accounts for 7.21% of the total scoring weight in GovRAMP assessments — and requires 90 days of evidence before passing. CSPs that plan ahead for this control cut their overall cycle time dramatically.

Control	Definition	Context for Pass Time
Configuration Settings CM-06	Establish, implement, justify exceptions for, and continuously monitor secure configuration settings to ensure system components operate in the most restrictive yet functional manner.	Requires 90 days of continuous evidence of configuration change management.
Authenticator Management IA-05	Authenticator management ensures that all system authenticators (like passwords, tokens, and certificates) are securely issued, protected, regularly updated, and revoked as needed to verify identities and prevent unauthorized access.	Password and credential management often require architectural changes.
Identification & Authentication IA-02	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Involves identity proofing across users and systems.
Software, Firmware & Information Integrity SI-05	Use tools to detect unauthorized changes to software, firmware, and information, and take defined actions whenever such changes are found.	Integrity verification across components can lag due to tooling gaps.
Maintenance Tools MA-3	Approve, control, and monitor the use of system maintenance tools, and regularly review previously approved tools as required.	Maintenance controls are often delayed by third-party dependencies.

Control Performance & Trends

Conversely, several controls emerge as “early wins” for new participants:



These results suggest that CSPs entering PSSP can build early momentum by prioritizing controls with low dependency and high visibility — establishing “quick wins” that translate to confidence and measurable improvement early in the cycle.

Outliers & Observations

A small subset of providers passed all controls in their first relative quarter, while others remained at 0% after six. These cases likely represent legacy CSPs already near authorization or new entrants with incomplete implementations.

Removing them from analysis marginally altered averages, reaffirming the overall robustness of the dataset.

Control	Definition	Context for Pass Time
Incident Handling IR-04	Establish and coordinate a consistent incident-handling process—covering preparation through recovery—that aligns with plans, integrates lessons learned, and ensures predictable execution across the organization.	Incident response planning is often established early through PMO guidance.
Identification & Authentication IA02-01	Require multi-factor authentication for all privileged accounts to ensure high-risk access is verified with multiple, distinct authentication factors.	Strong identity foundations allow faster verification.
Remote Access AC17(02)	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Remote access controls are among the easiest to implement with automation.
Authenticator Management IA-05(01)	Ensure strong password-based authentication by blocking weak or compromised passwords, protecting passwords in transit and storage, supporting secure password creation and recovery, and enforcing organization-defined complexity requirements.	Password complexity and reuse policies are quickly verifiable.
System Monitoring SI-04(04)	Define what counts as unusual or unauthorized communication activity, and regularly monitor inbound and outbound traffic for those conditions.	Logging and monitoring practices are often already in place.

QUARTER-BY-QUARTER ANALYSIS

Measuring Momentum

Compliance progress, like cybersecurity maturity itself, rarely happens overnight. But when viewed through the lens of the Progressing Security Snapshot Program (PSSP), it becomes clear that momentum is measurable — and the compounding effect of consistent feedback drives meaningful change.

The Momentum Curve

When plotted quarter over quarter, PSSP data reveals a compelling story of acceleration, stabilization, and optimization.

- **Quarter 1:** Baseline. Most CSPs begin the program with fewer than 25% of controls in a passing state.
- **Quarters 2–4:** The sharpest gains occur here, with cumulative pass rates often doubling. This phase reflects the impact of early PMO engagement and advisory coaching.
- **Quarters 5–6:** Gains continue, though more gradually, as providers tackle the harder, evidence-heavy controls.
- **Quarter 7:** A slight decline appears — not from regression, but graduation. CSPs with high maturity typically exit PSSP to pursue Core, Ready or Authorized status.

Momentum builds early — most providers see their steepest improvement between the second and fourth quarters.

Patterns Behind The Progress

Analysis of control-level performance supports this trajectory. Controls like CM-06, IA-05, and SI-07 often remain open until later quarters, while IR-04 and IA-02(01) show gains almost immediately.

In effect, the PSSP functions as a learning curve accelerator: by Q4, a majority of CSPs have turned their initial compliance gaps into structured, auditable strengths.

CONTROL FAMILY INSIGHTS

Where CSPs Excel — and Struggle

Grouping the 40 tracked controls into NIST-aligned families helps clarify where providers advance fastest and where systemic friction remains.

Control Family	Av. Quarters to Pass	Key Observation
Access Control (AC)	2.1	Improves steadily — automation and identity tools accelerate implementation
Audit & Accountability (AU)	2.2	Gains come once logging standards are centralized
Configuration Management (CM)	2.6	The hardest family — requires sustained evidence and change tracking
Identification & Authentication (IA)	2.4	Highly variable; depends on architectural readiness
Incident Response (IR)	1.9	Among the fastest; benefits from advisory coaching and playbook templates
System & Information Integrity (SI)	2.5	Challenging due to verification tooling and dependency chains.

Configuration Management: The Bottleneck Family

CM controls top every difficulty list — particularly CM-06 and CM-06(01) — due to their dependence on 90-day change-tracking evidence and cross-system consistency. Yet, CSPs that invest in automated configuration baselines early often cut that time nearly in half.

Configuration controls don't just ensure compliance — they institutionalize operational discipline. The payoff is security resilience, not paperwork.

Incident Response: The Early Win

On the opposite end, IR controls consistently rank among the fastest to achieve. IR-04, focusing on testing and response procedures, benefits from repeatable templates provided by the PMO and peer examples from other CSPs.

These opposing families — CM and IR — highlight how the PSSP creates dual value: it streamlines straightforward wins while illuminating deeper organizational challenges.

KEY FINDINGS & THEMES

The GovRAMP Progressing Security Snapshot data underscores a single truth: compliance, when operationalized, is security in motion. The following patterns emerged consistently across the seven-quarter analysis:

Persistence Pays Off

Providers that remain in the PSSP for at least four quarters achieve, on average, 50% higher pass rates than early-exit peers. The longer the engagement, the stronger the outcome — proof that compliance maturity compounds with time and repetition.

GovRAMP's quarterly cadence builds habits, not checklists.

Configuration Management is a Bottleneck

Controls within the CM family take, on average, 25–35% longer to pass than others. Their dependency on continuous monitoring data — not static documentation — makes them both time-intensive and deeply valuable.

Improvement here signals not just compliance, but genuine operational control.

CM-06 and CM-09 together account for 13% of a CSP's overall score weighting.

Quick Wins Exist and They Matter

Early progress on IA-02(01) and IR-04 correlates strongly with higher overall performance by Q4. These controls build momentum and confidence, creating early indicators of long-term success.

The data shows: success breeds success. CSPs that "pass early" tend to stay ahead.

Evidence Quality Drives Outcomes

The controls that require evidence across time windows (e.g., 90-day logging or continuous monitoring) consistently take longer to close. But these are also the controls that deliver the most meaningful proof of resilience.

In PSSP data, the difference between a passing and failing CSP often came down to documentation quality, not capability.

In compliance, what's written is what's proven.

RECOMMENDATIONS: FROM INSIGHT TO ACTION

GovRAMP's Progressing Security Snapshot Program continues to mature not only CSPs — but the entire public sector cloud ecosystem. The data suggests clear next steps for every stakeholder.

For Cloud Service Providers (CSPs)

1. Plan evidence early: Controls like CM-06 and CM-06(01) require 90-day documentation; begin tracking from day one.

2. Leverage early wins: Prioritize IA-02(01) and IR-04 to build early momentum and demonstrate progress quickly.

3. Treat each quarter as an audit rehearsal: Use PSSP's quarterly feedback cycles as iterative readiness checks for future Core, Ready or Authorized designations.

For Agencies & Procurement Leaders

1. Use PSSP participation as a leading indicator of maturity: Time in program correlates with measurable security improvement.

2. Set realistic expectations: Controls requiring time-bound evidence take multiple quarters — but their rigor signals resilience, not delay.

3. Encourage continuity: Vendors that stay engaged through Q4–Q6 show the strongest operational stability.

THE ROAD AHEAD

The GovRAMP Progressing Security Snapshot Program demonstrates what's possible when compliance is reframed as a continuous improvement model rather than a milestone checklist.

Over seven quarters and nearly thirty thousand data points, the pattern is unmistakable: participation drives performance.

Providers who stay engaged make steady, measurable progress toward maturity — and by doing so, they strengthen the collective resilience of government cloud ecosystems.

Looking ahead, the next evolution of this analysis will incorporate Quarter 8 data and longitudinal tracking post-authorization, enabling GovRAMP to measure not only readiness but retention — how well these gains persist once providers graduate from the PSSP.

Compliance isn't the end of the journey. It's the framework that makes sustained security possible.

Compliance, reimagined through GovRAMP, is no longer a checkbox — it's a security strategy that scales.

ACKNOWLEDGMENTS

Special acknowledgement to RAMPQuest, who serves as the GovRAMP PMO through our PMO Agreement. And a special thanks to Andy Chuang, Information Security Analyst with the GovRAMP PMO, for his diligent work in compiling and analyzing the data that made this report possible.

Contact Information

Email
info@govramp.org

Website
www.GovRAMP.org

APPENDIX

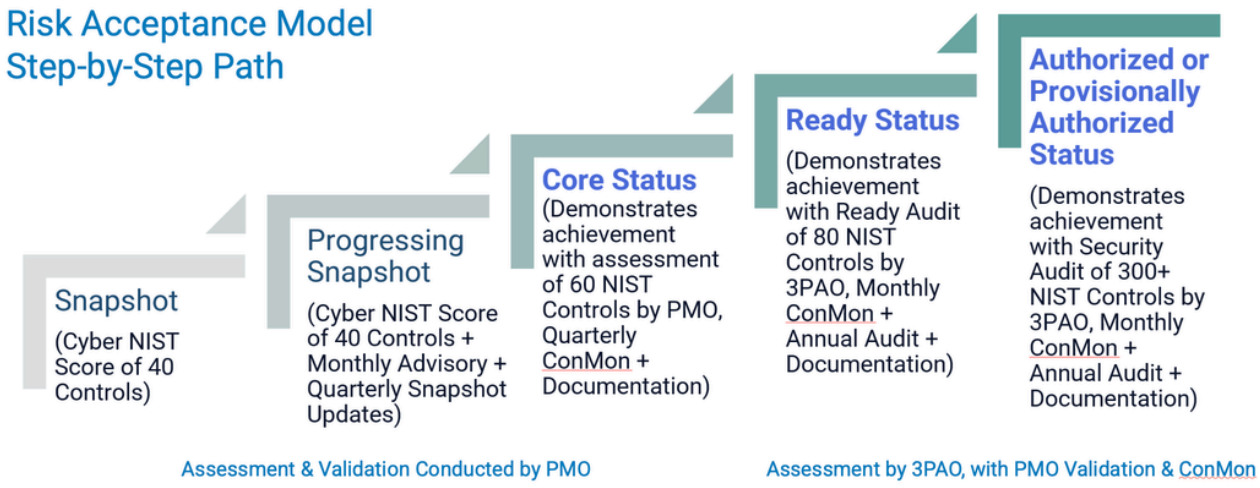
About GovRAMP

GovRAMP was founded in 2020 to meet a growing need: helping state and local governments confidently assess the security of the cloud solutions they use. At the time, there was no standard process to verify cybersecurity across vendors—making it difficult for agencies to know which services were truly secure.

What started as an effort to serve state and local governments has since grown. Today, GovRAMP supports public agencies across all levels of government, including higher education and K–12 schools, by offering a standardized, transparent approach to cloud security.

GovRAMP is a 501(c)(6) nonprofit membership organization made up of service providers, third party assessors, and government officials. Our members work in communities across the country, united by a shared mission: to strengthen cybersecurity and protect the public through collaboration, education, and verified security standards.

The following outlines the progressive steps cloud service providers can take to improve and demonstrate their security maturity, highlighting how the Progressing Security Snapshot is a key element to accelerating security work for providers of all sizes and revenue levels.



Additional data is available upon request.

Average Time (Quarters) for CSPs to Pass Each Control

Control ID	Relative Quarter to Pass
AC 02	2.21
AC 02 (01)	2.23
AC 02 (07)	2.28
AC 04	2.10
AC 06	1.94
AC 06 (02)	2.32
AC 06 (10)	2.30
AC 17	2.22
AC 17 (02)	1.87
AU 07	2.34
AU 07 (01)	2.16
AU 11	2.15
CM 02	2.43
CM 02 (02)	2.07

CM 02 (02)	2.07
CM 04	2.25
CM 05	2.09
CM 05 (01)	2.20
CM 05 (05)	2.08
CM 06	3.04
CM 06 (01)	2.11
CM 09	2.36
IA 02	2.48
IA 02 (01)	1.87
IA 05	2.48
IA 05 (01)	1.91
IR 04	1.77
IR 04 (01)	1.96
MA 03	2.44
RA 05 (05)	2.15

SC 07	2.21
SC 07 (03)	2.07
SC 28	1.94
SI 02	2.27
SI 02 (02)	2.06
SI 03	2.25
SI 04	2.00
SI 04 (04)	1.93
SI 07	2.45
SI 07 (07)	2.18