GovRAMP

VERSION 1.4

Continuous Monitoring Escalation Process

February 2026

Table of Contents

Document Revision History

Date	Description	Version	Author
7/22/2022	Policy Approved	1.0	GovRAMP Standards & Technical Committee
8/7/2022	Policy Adopted	1.0	GovRAMP Board of Directors
11/29/2023	Update	1.1	GovRAMP Standards & Technical Committee
11/30/2023	Policy Adopted	1.1	GovRAMP Board of Directors
8/30/2024	Updated Provisional status to Provisionally Authorized status.	1.2	GovRAMP Board of Directors
9/20/2024	Revised language to provide clarity around payment requirements, and updated Provisional status to Provisionally Authorized status.	1.3	GovRAMP Board of Directors
02/18/2026	Updated to reflect change from StateRAMP to GovRAMP	1.4	GovRAMP Staff

This document will be reviewed at the discretion of the GovRAMP Board on an annual basis or as needed.

1. Purpose

This document provides guidance on continuous monitoring and ongoing authorization in support of maintaining a security authorization that meets StateRAMP, Inc. dba GovRAMP (GovRAMP) requirements.

To maintain a GovRAMP verified status of Ready, Provisionally Authorized, or Authorized, the service provider (SP) must monitor their security controls, assess them regularly, and demonstrate that the security posture of their service offering is continuously acceptable.

For more information about GovRAMP, visit the website at www.GovRAMP.org.

2. Introduction

This document explains the actions taken when an SP fails to maintain an adequate continuous monitoring program. GovRAMP continuous monitoring (ConMon) is based on the continuous monitoring process described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

Security-related information collected during ConMon is used to determine if the system security is operating as intended and in accordance with GovRAMP requirements.

When an SP receives one of the three GovRAMP verified statuses for its cloud offering, the SP must adhere to the GovRAMP Continuous Monitoring Guide requirements.

SPs are expected to follow NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and the Risk Management Framework (RMF), continue to effectively deploy all applicable security controls, and act in good faith to maintain the appropriate risk posture. Failure to adhere to *GovRAMP Continuous Monitoring Guide* requirements may result in escalating actions by GovRAMP outlined in subsequent sections of this document.

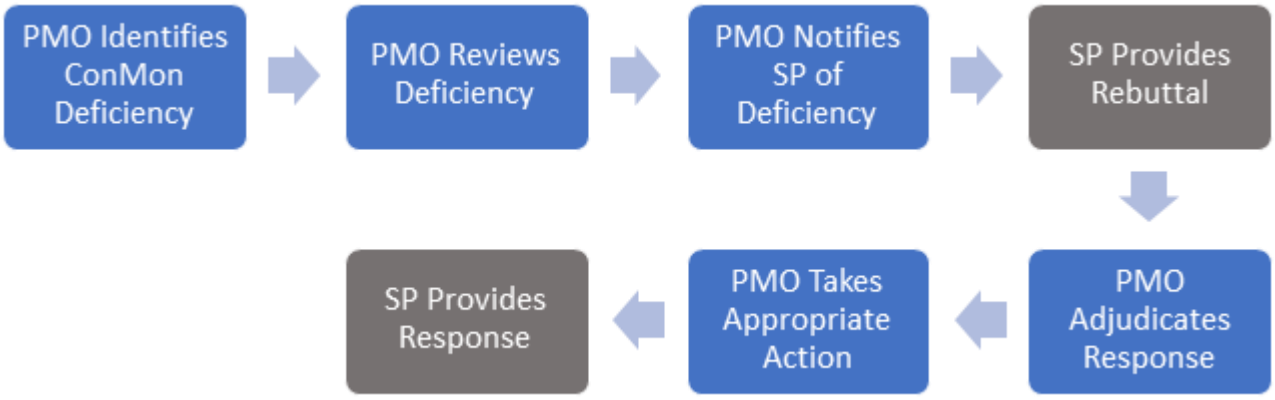
3. Escalation levels and process

As a condition to maintain a GovRAMP verified status, an SP agrees to participate in the GovRAMP ConMon process. If the SP fails to meet the requirements described in the *GovRAMP Continuous Monitoring Guide*, including failure to make timely payments or meet any of the other obligations agreed to in the Continuous Monitoring Agreement executed by both parties, GovRAMP can initiate an escalation process, which may result in one of the escalating levels outlined below, and initiates the process mapped in *Figure 1. The GovRAMP Escalation Process*.

1. **Detailed Finding Review**: The GovRAMP PMO will request the SP's security point of contact (POC) to assess a deficiency and report the cause and remedy back to the GovRAMP PMO. If the SP does not resolve a Detailed Finding Review within the agreed-upon timeframe, the GovRAMP PMO may escalate to a Corrective Action Plan.
2. **Corrective Action Plan (CAP)**: A request from the GovRAMP PMO Director for the SP to perform a root-cause analysis and provide a formal plan for remediation. If the SP does not resolve a CAP within the agreed-upon timeframe, the GovRAMP PMO Director may suspend or revoke the system's GovRAMP verified status. If the SP has provided access to any governments for reporting, the governments will be notified of the CAP. See section 3.1 for more details.
3. **Suspension**: A decision to temporarily suspend the information system's GovRAMP verified status until the identified deficiencies are resolved. If the SP does not resolve the deficiency within the agreed-upon timeframe and the GovRAMP PMO Director and the GovRAMP Approvals Committee (SAC) and/or SLED Authorizing Official (AO) determines the SP can no longer meet GovRAMP compliance requirements, the GovRAMP PMO may revoke the system's GovRAMP verified status. A suspension will be noted on the public Authorized Product List. See section 3.1 for more details.
4. **Revocation**: A decision by the GovRAMP PMO Director and the SAC or AO to revoke an information system's GovRAMP verified status. If revoked, the product would be removed from the APL. The SP would be eligible to resubmit the security package once the 3PAO has attested to meeting the GovRAMP Ready, Provisionally Authorized, or Authorized status requirements. See section 3.1 for more details.

When GovRAMP identifies a deficiency in the SP's ConMon process, it initiates the process mapped in Figure 1. The GovRAMP Escalation Process.

Figure 1 GovRAMP Escalation Process



3.1 The Escalation Process

1. **GovRAMP identifies a deficiency (refer to Table 1) with the SP's ConMon information.**
2. **The GovRAMP PMO reviews the deficiency and compares it to the SP's past ConMon performance.**
    a. The GovRAMP PMO typically decides on an escalation level consistent with the guidance described in *Section 4*, *Common Requirements: Deficiency Triggers*. As a result of the review, the GovRAMP PMO takes one of the following actions:
        i. GovRAMP may elect to monitor the SP more closely but take no further action. If so, no additional notice is sent, and the process stops here.
        ii. GovRAMP may increase an SP's existing escalation level. For example, an SP on a CAP may face suspension of their GovRAMP verified status.
        iii. In rare cases, GovRAMP may determine the deficiency is severe enough to make the escalation effective immediately, in which case, steps 3 and 4 are skipped.
3. **The GovRAMP PMO notifies the SP of the deficiency and GovRAMP's intended escalation.**
    a. Depending on the intended escalation level, the notice may come from:
        i. The GovRAMP PMO staff for an intended Detailed Finding Review.
        ii. The GovRAMP PMO Director for an intended CAP, suspension, or revocation.
4. **The SP responds to the notification.**

a. The SP's response should include any information that may rebut the escalation decision. Depending on the intended escalation level, the SP's response must come from:

    i. The SP's security POC for Detailed Finding Review.

    ii. The System Owner for a CAP, suspension, or revocation.

5. **The GovRAMP PMO reviews and adjudicates the SP's response and renders a formal escalation decision.**

    a. Depending on the escalation level, the decision is made by one of the following:

        i. The GovRAMP PMO staff for a Detailed Finding Review.

        ii. The GovRAMP PMO Director for a CAP.

        iii. The GovRAMP PMO Director for a suspension or revocation of Ready status.

        iv. The GovRAMP PMO Executive Director and the GovRAMP Approvals Committee or the SLED AO for a suspension or revocation of Authorized status.

6. **The GovRAMP PMO notifies the SP of its decision.**

    a. If GovRAMP decides to follow through with an escalation, this notice:

        i. Identifies the criteria for returning the system to a satisfactory state. It may also include a deadline by which the SP must fully satisfy the criteria or face more severe escalation.

        ii. Requires certain actions from the SP. Typically, the GovRAMP PMO requires the SP to perform a root-cause analysis and develop a formal plan for addressing the deficiencies.

7. **The SP responds in accordance with the GovRAMP notification.**

    a. This response must include:

        i. The results of the root cause analysis.

        ii. The SP's plan for fully resolving the issues, with clearly established milestones and dates, including the date of full resolution. For a CAP or

suspension, the plan must be signed by the System Owner. GovRAMP must approve the plan.

iii. Any other items as specified by GovRAMP in its notification.

3.1.1 Escalation Activities:

The following activities can occur when an escalation process has been activated for a noncompliant product. If the provider fails to provide a plan that is acceptable or fails to meet the dates identified in the plan, the GovRAMP PMO may increase the escalation level. Further escalation repeats the same escalation process described in section 3.1.

Monthly ConMon Reporting:

The GovRAMP PMO updates the PMO ConMon Monthly Review document to reflect the cited deficiencies, escalation level, and the SP's identified resolution date. For products listed as Ready, the status will be revoked by the GovRAMP PMO. Products listed as Authorized or Provisionally Authorized that receive an escalation level of suspended or revoked, GovRAMP will notify the SAC or AO. The SP's progress is reported each month to the SAC or AO until GovRAMP determines the issue is fully resolved. If there is a CAP, suspension, or revocation, a letter is posted to the GovRAMP document repository for review by the AO or the SAC, along with the SP's plan for resolution.

GovRAMP discontinues ConMon reporting when the system security status is suspended or revoked.

GovRAMP Authorized Product List (APL):

GovRAMP updates the security status on the APL to reflect the escalation level for suspension. GovRAMP removes the product from the APL if it is revoked. Detailed Finding Reviews and CAPs are not reflected on the APL.

Extension:

If the SP has made good-faith efforts to fully resolve the deficiency and address the plan, but requires more time, they may request an extension from the GovRAMP PMO.

3.1.2 Resolution Activities:

When the GovRAMP PMO determines the provider has fully resolved the cited deficiencies and satisfied the identified criteria communicated in the notification, the GovRAMP PMO takes the following actions:

Provider notification:

The provider's security POC will be notified when the GovRAMP PMO agrees a Detailed Finding Review is fully satisfied. The GovRAMP PMO Director notifies the System Owner when the GovRAMP PMO agrees a CAP is fully satisfied. The GovRAMP PMO Director notifies the System Owner when GovRAMP PMO and SAC or AO agrees a suspension is fully satisfied.

Monthly ConMon Reporting:

The GovRAMP PMO will update the next ConMon Monthly Review document to reflect all cited deficiencies are resolved and the escalation level is no longer in effect. The GovRAMP PMO ConMon Monthly Review document will be marked as "Satisfactory."

Other Postings and Notifications:

The GovRAMP PMO Director will post a letter to the GovRAMP PMO's secure repository indicating that the CAP or suspension is fully resolved to GovRAMP's satisfaction, and the SP is once again in good standing.

GovRAMP Authorized Vendor List:

GovRAMP returns the product's verified status to its prior listing.

4. Conmon Requirements: Deficiency Triggers

To ensure consistent expectations and enforcement, GovRAMP defines risk management deficiency triggers. When an SP's performance exceeds one or more of the thresholds defined in Table 1 Risk Management Deficiency Triggers, GovRAMP will, at a minimum, take the prescribed action.

Table 1. Risk Management Deficiency Triggers

CONMON AREA – OPERATIONAL VISIBILITY	
DEFICIENCY TRIGGERS	**ESCALATION LEVEL**
Unique Vulnerability Count Increase 20% from the annual vulnerability baseline (or 10 unique vulnerabilities, whichever is greater) *Note: A request for rebaseline of a unique vulnerability count, accompanied with proper justification, can be submitted to the GovRAMP PMO, and may be approved on a case-by-case basis.*	Detailed Finding Review
Non-compliance with the scanning requirements outlined in the *GovRAMP Vulnerability Scan Requirements Guide*, first incident in the previous six months. *Unauthenticated scan results delivered as part of the initial SAR*	Detailed Finding Review

submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission result in the SP being placed on a Detailed Finding Review. This applies only to the first SP submission that is non-compliant with authenticated scan requirements.	
Non-compliance with the scanning requirements outlined in the *GovRAMP Vulnerability Scan Requirements Guide*, for each subsequent incident beyond the first within six months. *Unauthenticated scan results delivered as part of the initial SAR submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission, result in the CSP being placed on a CAP, when a second or greater CSP submission is non-adherent to authenticated scan requirements.*	CAP
Late Remediation High Impact Vulnerabilities *Five or more unique vulnerabilities or POA&Ms aged greater than 30 days.*	Detailed Finding Review
Late Remediation High Impact Vulnerabilities *Five or more unique vulnerabilities or POA&Ms aged greater than 60 days.*	*CAP*
Late Remediation Moderate Impact Vulnerabilities *Ten or more unique vulnerabilities or POA&Ms aged greater than 90 days.*	Detailed Finding Review
Late Remediation Moderate Impact Vulnerabilities *Ten or more unique vulnerabilities or POA&Ms aged greater than 180 days.*	*CAP*
Late Delivery of Annual Assessment Package *Delivery of full Annual Assessment Package after 30 days from the GovRAMP Ready or Authorized anniversary letter date.*	*CAP*
Poor Quality of Deliverables *Lack of clarity, consistency, conciseness, or completion of any deliverable, including (but not limited to) the SSP, the SSP Control Matrix, authorization boundary diagrams, monthly ConMon documents, etc.*	*Detailed Finding Review*
Lack of Transparency *Willful failure to report known issues to GovRAMP or purposely manipulating scans to avoid risk management deficiency triggers.*	*CAP*
Multiple Recurrences *Any trigger that is realized multiple times within a six-month timeframe.*	*CAP*
Insufficient Notice of Significant Change *Notification received less than 30 days before a significant change or insufficient documentation of the Security Impact Analysis.*	*CAP*

CONMON AREA -CHANGE CONTROL	
DEFICIENCY TRIGGERS	**ESCALATION LEVEL**
Late Notice of Emergency Significant Change *Notification received longer than five days after the change.*	*CAP*
Undocumented /Unreported Significant Change *No notification of a change.*	*CAP*
CONMON AREA – INCIDENT RESPONSE	
DEFICIENCY TRIGGERS	**ESCALATION LEVEL**
Late Incident Notification *Late notification of incident not in accordance with the GovRAMP Incident Communications Procedure.* Note: An incident is a violation of computer security policies, acceptable use policies, or standard computer security practices, according to NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 2.	*CAP*
Incident Frequency of Recurring Type *Any incident with recurring type and/or cause*	*CAP*
CONMON AREA – CONTINUOUS MONITORING AGREEMENT ISSUE	
DEFICIENCY TRIGGERS	***ESCALATION LEVEL***
Failure to Comply with Agreed Upon Terms This includes, but is not limited to, failure to make timely payments for monthly Continuous Monitoring, annual reviews, or GovRAMP membership.	*CAP*