GovRAMP

VERSION 2.0

Continuous Monitoring Guide and Escalation Process

June 2026

Table of Contents

Document Revision History

Date	Description	Version	Governance Body
10/29/2020	Original Publication	1.0	GovRAMP Steering Committee
4/22/2022	Update to reference GovRAMP Continuous Monitoring Performance Guide and other minor edits	1.5	GovRAMP Standards & Technical Committee
4/29/2022	Adopted	1.6	GovRAMP Board of Directors
11/29/2023	Revised language to reflect GovRAMP verified statuses, minor edits to Sections 3.6(1.,5.) added access rights review for GovRAMP document portal; Section 3.7(5. a),	1.6	GovRAMP Standards & Technical Committee
11/30/2023	Adopted	1.6	GovRAMP Board of Directors
9/20/2024	Revised language to provide clarity around payment requirements and updated Provisional status to Provisionally Authorized status.	1.7	GovRAMP Board of Directors
5/7/2026	Revised language to incorporate GovRAMP rebranding, GovRAMP Core, Federal usage of GovRAMP, merging of the GovRAMP Escalation Process manual, and update of deficiency triggers.	2.0	GovRAMP Standards & Technical Committee
6/1/2026	Adopted	2.0	GovRAMP Board of Directors

This document will be reviewed at the discretion of the GovRAMP Board at a frequency of no less than annually.

1. Purpose

Continuous monitoring review procedures outline the process to examine each monthly or quarterly continuous monitoring package submission. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security related risks at a frequency sufficient to support organizational risk-based decisions.

Monitoring security controls is part of the overall risk management framework for information security and the Service Provider (SP) is required to maintain a security authorization that meets GovRAMP requirements. Performing ongoing security assessments determines whether the set of deployed security controls in a cloud system remains effective considering new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time.

To maintain an authorization that meets GovRAMP requirements, the SP must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Ongoing assessment of security controls results in greater control over the security posture of the SP's system and enables timely risk-management decisions. Security-related information collected through continuous monitoring is used to make recurring updates to the security assessment package.

Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows state and local governments the ability to make informed risk management decisions as they use cloud solutions.

2. Roles and Responsibilities

2.1 Service Provider

When an SP has achieved one of the four GovRAMP verified statuses, the SP's security posture is monitored according to the assessment and authorization process. Where applicable, it is the responsibility of the service provider to partner with a GovRAMP certified third party assessment organization (3PAO) to allow for required monitoring requirements.

2.2 SLED Authorizing Body [Non-Federal]

SLED refers to state or local government or higher education bodies contracting with SPs who provide and/or use a SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), or IaaS (Infrastructure-as-a-Service) solution involving the storage, processing, and/or transmitting of

government data including PII (Personally Identifiable Information), PHI (Protected Health Information), and/or PCI (Payment Card Industry).

The SLED Authorizing Body manages the review and approval of all continuous monitoring artifacts submitted by the service provider on behalf of the SLED entity. The SLED entity must review all security artifacts provided by the SP, 3PAO, or GovRAMP PMO to ensure the SP's security posture meets requirements for the SLED entity's use of the system.

SLED Authorizing Bodies should ensure their organization is monitoring the Plan of Action & Milestones (POA&M) and reporting artifacts as well as any significant changes associated with the SP's service offering. SLED entities should use this information to make risk-based decisions about ongoing authorization of the system.

2.3 Federal Authorizing Official [Federal Only]

Federal agencies contracting with SPs who provide and/or use a SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), or IaaS (Infrastructure-as-a-Service) solution involving the storage, processing, and/or transmitting of government data including PII (Personally Identifiable Information), PHI (Protected Health Information), CJI (Criminal Justice Information), and/or PCI (Payment Card Industry) may designate one or more authorizing officials (AO) for their agency.

The Federal AO manages the review and approval of all continuous monitoring artifacts submitted by the service provider on behalf of the Federal Agency. The Federal AO or their delegate must review all security artifacts provided by the SP, 3PAO, or GovRAMP PMO to ensure the SP's security posture meets requirements for the Federal Agency's use of the system.

Federal AOs should ensure their organization monitors the Plan of Action & Milestones (POA&M) and reporting artifacts as well as any significant changes associated with the SP's service offering. Agencies should use this information to make risk-based decisions about ongoing authorization of the system.

2.4 Third Party Assessment Organization (3PAO)

For Service Providers seeking a Ready, Provisionally Authorized, or Authorized verified status, 3PAOs are responsible for:

- Preforming initial assessments of service provider's system by independently verifying and validating the control implementation, documenting test results, and assisting service providers to ensure they properly scope continuous monitoring activities.

- Conducting an annual review of a subset of 1/3 of the selected security controls for the product's impact level, ensuring that all applicable controls are assessed over a three-year lifecycle.
- Submitting an assessment report to GovRAMP in support of the initial assessment and each year thereafter in support of the annual assessment requirement.
- Performing announced penetration testing annually [Provisionally Authorized and Authorized only].
- Performing annual scans of web applications, databases, and operating systems.
- Assessing change controls on an ad hoc basis as requested by GovRAMP, the SLED Authorizing Body, or Federal AO for any changes made to the system by the service provider.

To be effective in this role, 3PAOs are responsible for ensuring that the chain of custody is maintained for any 3PAO-authored documentation. 3PAOs must also be able to attest for the veracity and integrity of data provided by the SP for inclusion in 3PAO-authored documentation.

- If scans are performed by the SP, the 3PAO must either be on-site and observe the SP performing the scans or be able to monitor or verify the results of the scans through other means documented and approved by the GovRAMP PMO.

2.5 GovRAMP Program Management Office (PMO)

GovRAMP PMO oversees and conducts analysis on the service provider's continuous monitoring activities. The GovRAMP PMO also provides information to and may advise the State Authorizing Body or Federal Authorizing Official, who maintains the responsibility on behalf of their organization for continuous monitoring in relation to their contract.

For Service Providers seeking a Core verified status, the GovRAMP PMO is also responsible for:

- Assisting service providers properly scope continuous monitoring activities.
- Conducting initial and annual reviews of the Service Provider's control implementation of applicable controls.
- Assessing change controls on an ad hoc basis as requested by GovRAMP, the SLED Authorizing Body, or Federal AO for any changes made to the system by the service provider

2.6 Standards and Technical Committee

As outlined in the GovRAMP Standards and Technical Committee Charter, the Standards and Technical Committee will consult the GovRAMP PMO on policies, security standards, etc. This committee will have the following responsibilities regarding continuous monitoring:

- Reviewing policy framework for continuous monitoring and security artifacts on a regular basis
- Setting minimum requirements for the PMO to provide the SLED Authorizing Body and Federal AO with a regularly scheduled summary reporting of the SP's continuous monitoring statuses and changes.
- Ensuring the GovRAMP PMO is providing artifacts to all relevant SLED authorizing bodies and Federal AOs in a timely manner.

GovRAMP Standards and Framework will undergo periodic and regular review to address current trends and concerns in cybersecurity. Notice will be provided with a reasonable timeframe for implementation.

3. Continuous Monitoring

The GovRAMP continuous monitoring program is based on the continuous monitoring process described in NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organization*. GovRAMP has created a process that meets the diverse needs of federal, state, and local governments, and education institutions.

GovRAMP

- **Create** a plan for continuous monitoring that elevates awareness of vulnerabilities and utilizes threat protection methods for managing risk events.
- **Implement** a program that collects, analyzes, and reports monitoring data.
- **Respond** to findings by making decisions to mitigate vulnerabilities at all levels of the organization.
- **Review** incidents and themes to increase visibility and awareness to risk.
- **Adapt** and enhance your organizational security.

Figure 1

GovRAMP recognizes that cybersecurity verification is not a "one size fits all" implementation. Therefore, to meet agency specific needs, the GovRAMP PMO will partner with the SLED Authorizing Body, Federal AO, SP, 3PAO, and the GovRAMP Board to make reasonable accommodations, recommendations, and/or modifications to the standard GovRAMP continuous monitoring processes. Figure 1 provides a visual representation of the continuous monitoring process cycle.

Upon obtaining a Core, Ready, Provisionally Authorized, or Authorized Status, the SP is required to maintain a continuous monitoring program. The cadence for submitting continuous monitoring reports to the PMO is quarterly for a verified status of Core and monthly for a verified status of Ready, Authorized, or Provisionally Authorized. The SP is required to deliver the documentation outlined below. The GovRAMP PMO will review and analyze the service provider's continuous monitoring deliverables. This process is required for SPs to retain their Core, Ready, Provisionally Authorized, or Authorized Status. Failure to implement or comply with the continuous monitoring activities can result in a change or loss of the Ready or Authorized Status.

3.1 Continuous Monitoring Process

1. Continuous monitoring begins when a service provider obtains one of the four GovRAMP verified statuses. The SP is responsible for making timely payments to the PMO as agreed upon in the Continuous Monitoring Agreement executed by both parties.
    a. Reminder: You may be under contractual obligation to make your ConMon available to Participating Governments for the duration of your contractual agreement.
2. The SP will create a continuous monitoring plan that meets the minimum GovRAMP continuous monitoring standards, including all specific requirements provided by the SLED Authorizing Body and/or Federal AO.
    a. For Service Providers seeking a Core verified status, the service provider's plan must be validated by the GovRAMP PMO.
    b. For Service Providers seeking a Ready, Provisionally Authorized, or Authorized verified status, the plan must be validated by the 3PAO.
3. The SP is responsible for implementing the continuous monitoring plan as agreed upon by GovRAMP, the SLED Authorizing Body, and/or the Federal AO. As outlined in this document, the SP will send the GovRAMP PMO all continuous monitoring and significant change artifacts at the specified intervals.
    a. SP submits all monthly reporting materials.
    b. SP reviews and confirms access rights monthly for their own staff to the GovRAMP document repository. Access changes are reported to the PMO.
    c. For Service Providers seeking a Ready, Provisionally Authorized, or Authorized verified status, the 3PAO submits all annual documentation and all penetration testing reports.
4. The GovRAMP PMO analyzes all submitted artifacts, reviews the ConMon Executive Summary, and records a satisfactory or needs improvement review.
    a. The GovRAMP PMO will provide the SLED Authorizing Body and/or the Federal AO access to view and approve the SP's reporting and all the GovRAMP PMO's analysis.
    b. The SLED Authorizing Body and/or the Federal AO may request raw evidence from the SP or 3PAO to review.
5. The SLED Authorizing Body and/or the Federal AO reviews the SP's continuous monitoring artifacts, including the executive summary.

a. If any party is not satisfied with the findings, the GovRAMP PMO, the SP, the SLED Authorizing Body, and/or the Federal AO will meet to define corrective actions which will be incorporated into the POA&M.
b. Additional continuous monitoring requirements are at the discretion of the SLED Authorizing Body and/or the Federal AO.
c. SLED Authorizing Body and/or the Federal AO approve all continuous monitoring documentation.
d. Any concerns by the SLED Authorizing Body and/or the Federal AO will be addressed on a case-by-case basis and could affect the authorization status.

6. The GovRAMP PMO updates the SP's public profile with documentation and most recent SLED Authorizing Body and/or the Federal AO as needed.

3.2 GovRAMP PMO Monthly Review Process

1. The SP must provide raw vulnerability and compliance scans results in a machine readable format (CSV, XML, or similar format), POA&M spreadsheet, and complete the ConMon executive summary report to the GovRAMP PMO.
    a. For Service Providers seeking a Core verified status, submissions are quarterly.
    b. For Service Providers seeking a Ready, Provisionally Authorized, or Authorized verified status, submissions are monthly.
2. The SP must remediate all discovered high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, and low-risk vulnerabilities within 180 days, unless a shorter duration is specified in an applicable control (ex. the RA-05 control related to the CJIS overlay).
3. The SP with Low or Moderate security categorization will upload the following monthly documents to the GovRAMP document repository:
    a. POA&Ms (Plan of Action and Milestones)
    b. An updated inventory workbook
    c. OS, DB, and web application vulnerability scans
    d. Compliance scan results
        i. Compliance scanning focuses on the configuration settings (or security hardening) being applied to a system. Compliance scans assess adherence to a specific compliance framework.
    e. Risk Adjustments (RA)
    f. Operational Requirements (OR)
    g. False Positives(FP)
    h. Deviation Request Form (when applicable for RA/OR/FP)
    i. An overall executive summary of the above items

4. The SP with High security categorization systems is solely responsible for conducting the following activities as stated above. The GovRAMP PMO will coordinate a monthly review process with the SP that will meet the security requirements set forth by the information system.
5. The GovRAMP PMO will review the submitted documentation. To facilitate a successful review, the following requirements must be met.
    a. The POA&Ms must account for past due vulnerabilities.
    b. POA&Ms must be remediated within the required timeframes, and evidence of the remediation must be provided.
    c. Past due POA&Ms must include justification with supporting evidence.
    d. All scans must include all inventory components.
    e. Any Risk Adjustments must be accompanied by rationale.
    f. False Positives and Operational Requirements must be clearly documented.
6. Findings resulting from the GovRAMP PMO's review of the continuous monitoring documentation may trigger a greater frequency of reporting activities, as well as impromptu requests for evidence regarding the most recent assessment.
7. Failure to comply with the agreed upon continuous monitoring plan and requirements may result in corrective action or revocation of the verified security status.
8. The GovRAMP PMO or the SLED Authorizing Body may require that additional controls be added to the annual 3PAO assessment based on the SP's continuous monitoring activity.

3.3 Annual Activities

The following activities must take place annually for the SP to retain their verified status and remain in good standing with the GovRAMP PMO and the SLED Authorizing Body.

3.3.1 SP Annual Activities

The SP is solely responsible for conducting the following activities on an annual basis:

1. Review and update the information security policies and procedures.
    a) Policies and procedures for High security categorization must be reviewed and updated annually.
    b) For Moderate and Low security categorization systems, the SP must review procedures annually and review policies every three years.
    c) The SP must insert the updated policy document as an attachment to the GovRAMP System Security Plan (GR-SSP) and submit the updated plan to the

GovRAMP PMO one year after the initial authorization date and each year thereafter.

2. For Service Providers seeking a Ready, Provisionally Authorized, or Authorized verified status, SPs must contract with a 3PAO to assess a subset of their security controls.
    a) The 3PAO will determine which subset of controls are to be assessed, with approximately one-third of controls reviewed annually, with all controls reviewed every three years.
    b) The GovRAMP PMO and/or SLED Authorizing Body may require specific security controls for annual review.
    c) All assessment reports must be submitted to the GovRAMP PMO.
3. For Service Providers seeking a Core verified status, the service provider must resubmit their artifacts annually.
4. For Service Providers seeking a Provisionally Authorized or Authorized verified status, SPs must conduct penetration testing to ensure compliance with all vulnerability mitigation procedures.
    a) Penetration testing must be performed by a 3PAO, and all penetration testing reports must be sent to the GovRAMP PMO.
    b) Additional penetration testing is required when the SP has made a significant change in their product.
        i. Unless required by the SLED Authorizing Body and/or Federal AO, this testing does not have to be conducted by a 3PAO but shall be included in the required annual testing by the 3PAO.
5. The Configuration Management Plan (CMP) must be reviewed, updated, and submitted to the GovRAMP PMO.
6. The GovRAMP Information System Contingency Plan (ISCP) must be reviewed and updated and submitted to the GovRAMP PMO.
7. The Supply Chain Risk Management Plan (SCRM) must be reviewed and updated and submitted to the GovRAMP PMO.
8. The GovRAMP In Continuous Monitoring Plan (ISCM) must be reviewed and updated and submitted to the GovRAMP PMO.
9. An Incident Response Plan test must be conducted, and the corresponding Incident Response Plan must be reviewed and updated.
    a) Record the results of the incident response testing in the GR-SSP in the appropriate control description field indicating when the testing took place, testing materials, who participated, and who conducted the testing.
    b) Insert the updated Incident Response Plan as an attachment to the GR-SSP.

10. The System Security Plan (SSP)/Operational Controls Matrix (OCM) must be reviewed, updated, and submitted to the GovRAMP PMO. SP must also submit payment for the annual review in accordance with the Continuous Monitoring Agreement executed by both parties.

3.3.2 3PAO Annual Activities [Ready, Provisionally Authorized, and Authorized Only]

The 3PAO is solely responsible for conducting the following activities on an annual basis:

1. The development of a Security Assessment Plan (SAP) that describes the scope of the assessment includes:
    a) Security controls and control enhancements under assessment
    b) Assessment procedures to be used to determine security control effectiveness
    c) Assessment environment, assessment team, and assessment roles and responsibilities
2. Assessing the security controls in the SP's information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
    a) Security control assessments include in-depth monitoring, vulnerability scanning, malicious user testing, and insider threat assessment.
    b) Security control assessments for performance and load testing must occur once every three years unless the SLED Authorizing Body specifically requires more frequent testing.
3. Providing a report of vulnerability and compliance scanning to the SP and the GovRAMP PMO.
4. Producing a security assessment summary that documents the results of the assessment.
5. Providing the results of the security control assessment to the GovRAMP PMO.
    a) The 3PAO submits all annual documentation and all penetration testing reports.

3.4 Data Calls

Upon rare occasions, the information security community identifies a vulnerability affecting products or technologies that are widely used across multiple organizations that may have implications for national security and require accelerated remediation:

The PMO Director, upon approval of GovRAMP Executive Director or designee, may issue an out-of-cycle "Data Call" to service providers to determine whether such a vulnerability is present within a service provider's system. Such accelerated timelines shall be based on

guidance from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) or a similar organization.

4. 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 above, 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 2. 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 4.1 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 4.1 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 4.1 for more details.

When GovRAMP identifies a deficiency in the SP's ConMon process, it initiates the process mapped in Figure 2. The GovRAMP Escalation Process.

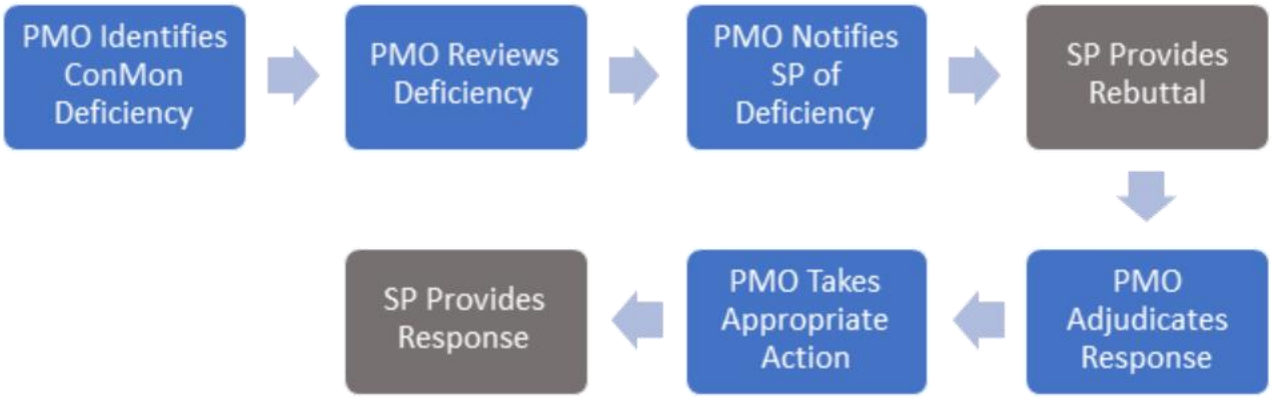

Figure 2 GovRAMP Escalation Process

4.1 The Escalation Process

1. **GovRAMP identifies a deficiency (refer to Table 1 below) 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 5, 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.

4.1.1 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 4.1.

Quarterly ConMon Reporting (Core Status Only):

The GovRAMP PMO updates the PMO ConMon Quarterly Review document to reflect the cited deficiencies, escalation level, and the SP's identified resolution date. For products listed as Core, the status will receive an escalation of suspended or revoked by the GovRAMP PMO. The SP's progress is tracked each quarter 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 Participating Governments with access to the SPs ConMon package, along with the SP's plan for resolution.

Monthly ConMon Reporting (Ready, Provisionally Authorized, or Authorized Statuses):

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 Sponsoring Body. The SP's progress is reported each month to the Sponsoring Body 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 Sponsoring Body and governments with ConMon access, along with the SP's plan for resolution.

GovRAMP may discontinue 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.

4.1.2 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.

Quarterly/Monthly ConMon Reporting:

The GovRAMP PMO will update the next ConMon Quarterly or Monthly Review document to reflect all cited deficiencies are resolved and the escalation level is no longer in effect. The GovRAMP PMO ConMon Quarterly or 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.

5. 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)	Detailed Finding Review

First incident in the previous 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 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 *The greater of five (5) or more unique vulnerabilities or POA&Ms aged greater than 30 days or 5% of inventory.*	Detailed Finding Review
Late Remediation High Impact Vulnerabilities *The greater of five (5) or more unique vulnerabilities or POA&Ms aged greater than 60 days or 5% of inventory.*	*CAP*
Late Remediation Moderate Impact Vulnerabilities *The greater of ten (10) or more unique vulnerabilities or POA&Ms aged greater than 90 days or 5% of inventory.*	Detailed Finding Review
Late Remediation Moderate Impact Vulnerabilities *The greater of ten (10) or more unique vulnerabilities or POA&Ms aged greater than 180 days or 5% of inventory.*	*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 3.	*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*
CONMON AREA – DATA CALL	
DEFICIENCY TRIGGERS	***ESCALATION LEVEL***
Failure to Comply with Data Call Requirements A vulnerability shall trigger a continuous monitoring deficiency when a detected weakness remains open beyond the allowable remediation window, involves products or technologies with widespread organizational use, and presents the potential to impact national security interests. Determinations of such high risk exposure are made at the sole discretion of the PMO Director.	*CAP*