StateRAMP

# STATERAMP CONTINUOUS MONITORING ESCALATION PROCESS

**VERSION:**
1.0

**DATE:**
August 2022

## DOCUMENT REVISION HISTORY

| Date | Description | Version | Governance Body |
|---|---|---|---|
| 7/22/2022 | Policy Approved | 1.0 | Standards & Technical Committee |
| 8/7/2022 | Policy Adopted | 1.0 | Board of Directors |
| | | | |
| | | | |

This document will be reviewed at the discretion of the StateRAMP 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 requirements.

To maintain a StateRAMP verified status of Ready, Provisional, 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 StateRAMP, visit the website at www.stateramp.org.

# 2. INTRODUCTION

This document explains the actions taken when an SP fails to maintain an adequate continuous monitoring program. StateRAMP 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 StateRAMP requirements.

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

SPs are expected to follow NIST SP 800-37, Revision 2, 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 StateRAMP Continuous Monitoring Guide requirements may result in escalating actions by StateRAMP outlined in subsequent sections of this document.

# 3. ESCALATION LEVELS AND PROCESS

As a condition to maintain a StateRAMP verified status, the SP agrees to participate in the StateRAMP ConMon process. If the SP fails to meet the requirements described in the *StateRAMP Continuous Monitoring Guide*, StateRAMP 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 StateRAMP Escalation Process*.

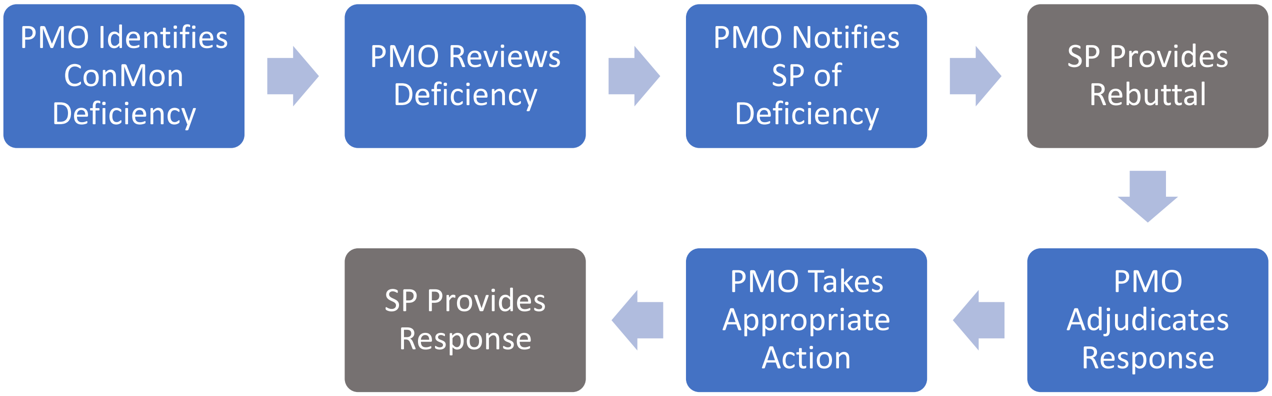
1. Detailed Finding Review: The StateRAMP PMO will request the SP's security Point of Contact (POC) to assess a deficiency and report the cause and remedy back to the StateRAMP PMO. If the SP does not resolve a Detailed Finding Review within the agreed-upon timeframe, StateRAMP PMO may escalate to a Corrective Action Plan.
2. Corrective Action Plan (CAP): A request from the StateRAMP 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 StateRAMP PMO Director may suspend or revoke the

system's StateRAMP 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 StateRAMP verified status until the identified deficiencies are resolved. If the SP does not resolve the deficiency within the agreed-upon timeframe and the StateRAMP PMO Director and the StateRAMP Approvals Committee (SAC) and/or SLED Authorizing Official (AO) determines the SP can no longer meet StateRAMP compliance requirements, StateRAMP PMO may revoke the system's StateRAMP 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 StateRAMP PMO Director and SAC or AO to revoke an information system's StateRAMP 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 StateRAMP Ready, Provisional, or Authorized status requirements. See section 3.1 for more details.

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

*Figure 1 StateRAMP Escalation Process*



PMO Identifies ConMon Deficiency

PMO Reviews Deficiency

PMO Notifies SP of Deficiency

SP Provides Rebuttal

PMO Adjudicates Response

PMO Takes Appropriate Action

SP Provides Response

## 3.1 THE ESCALATION PROCESS

1. **StateRAMP identifies a deficiency (refer to Table 1) with the SP's ConMon information.**

2. **The StateRAMP PMO reviews the deficiency and compares it to the SP's past ConMon performance.**
    a. StateRAMP 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, StateRAMP PMO takes one of the following actions:
        i. StateRAMP 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. StateRAMP may increase an SP's existing escalation level. For example, an SP on a CAP may face suspension of their StateRAMP verified status.
        iii. In rare cases, StateRAMP may determine the deficiency is severe enough to make the escalation effective immediately, in which case, steps 3 and 4 are skipped.

3. **The StateRAMP PMO notifies the SP of the deficiency and StateRAMP's intended escalation.**
    a. Depending on the intended escalation level, the notice may come from:
        i. The StateRAMP PMO Staff for an intended Detailed Finding Review.
        ii. The StateRAMP 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 StateRAMP 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 StateRAMP PMO Staff for a Detailed Finding Review.
        ii. The StateRAMP PMO Director for a CAP.
        iii. The StateRAMP PMO Director for a suspension or revocation of Ready status.
        iv. The StateRAMP PMO Executive Director and the StateRAMP Approvals Committee or the SLED AO for a suspension or revocation of Authorized status.

6. **The StateRAMP PMO notifies the SP of its decision.**
    a. If StateRAMP 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 StateRAMP PMO requires the SP to perform a root-cause analysis and develop a formal plan for addressing the deficiencies.

7. **SP responds in accordance with the StateRAMP 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. StateRAMP must approve the plan.
        iii. Any other items as specified by StateRAMP 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 StateRAMP PMO may increase the escalation level. Further escalation repeats the same escalation process described in section 3.1.

**Monthly ConMon Reporting:**

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

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

**StateRAMP Authorized Product List (APL):**

StateRAMP updates the security status on the APL to reflect the escalation level for suspension. StateRAMP 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 StateRAMP PMO.

### 3.1.2 RESOLUTION ACTIVITIES:

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

**Provider notification**:

The provider's security POC will be notified when the StateRAMP PMO agrees a Detailed Finding Review is fully satisfied. The StateRAMP PMO Executive Director notifies the System Owner when the

StateRAMP PMO agrees a CAP is fully satisfied. The StateRAMP PMO Executive Director notifies the System Owner when StateRAMP PMO and SAC or AO agrees a suspension is fully satisfied.

**Monthly ConMon Reporting:**

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

**Other Postings and Notifications:**

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

**StateRAMP Authorized Vendor List**:

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

## 4. CONMON REQUIREMENTS: DEFICIENCY TRIGGERS

To ensure consistent expectations and enforcement, StateRAMP 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*, StateRAMP 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**<br>**20% from the annual vulnerability baseline (or 10 unique vulnerabilities whichever is greater)**<br>*Note: A request for rebaseline of a unique vulnerability count, accompanied with proper justification, can be submitted to the StateRAMP PMO, and may be approved on a case-by-case basis.* | Detailed Finding Review |
| **Non-compliance with scanning requirements outlined in the StateRAMP Vulnerability Scan Requirements Guide)**<br>**First incident in the previous six months.**<br>*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.* | Detailed Finding Review |
| **Non-Compliance with scanning requirements outlined in the StateRAMP Vulnerability Scan Requirements Guide Each subsequent incident beyond the first within the previous six months.**<br>*Unauthenticated scan results delivered as part of the initial SAR submission, as* | CAP |

| | |
|---|---|
| *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.* | |
| **Late Remediation High Impact Vulnerabilities**<br>*Five or more unique vulnerabilities or POA&Ms aged greater than 30 days.* | Detailed Finding Review |
| **Late Remediation High Impact Vulnerabilities**<br>*Five or more unique vulnerabilities or POA&Ms aged greater than 60 days.* | CAP |
| **Late Remediation Moderate Impact Vulnerabilities**<br>*Ten or more unique vulnerabilities or POA&Ms aged greater than 90 days.* | Detailed Finding Review |
| **Late Remediation Moderate Impact Vulnerabilities**<br>*Ten or more unique vulnerabilities or POA&Ms aged greater than 180 days.* | CAP |
| **Late Delivery of Annual Assessment Package**<br>*Delivery of full Annual Assessment Package after 30 days from the StateRAMP Ready or Authorized anniversary letter date.* | CAP |
| **Poor Quality of Deliverables**<br>*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**<br>*Willful failure to report known issues to StateRAMP or purposely manipulating scans to avoid risk management deficiency triggers.* | CAP |
| **Multiple Recurrences**<br>*Any trigger that is realized multiple times within a six-month timeframe.* | CAP |
| **Insufficient Notice of Significant Change**<br>*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**<br>*Notification received longer than five days after the change.* | CAP |
| **Undocumented /Unreported Significant Change**<br>*No notification of a change.* | CAP |
| **CONMON AREA – INCIDENT RESPONSE** | |
| **DEFICIENCY TRIGGERS** | ESCALATION LEVEL |
| **Late Incident Notification**<br>*Late notification of incident not in accordance with the StateRAMP Incident Communications Procedure.*<br>Note: An incident is a violation of computer security policies, acceptable use | CAP |

| | |
|---|---|
| policies, or standard computer security practices, according to NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 2. | |
| **Incident Frequency of Recurring Type**<br>*Any incident with recurring type and/or cause* | CAP |