FedRAMP Continuous Monitoring Performance Management Guide

Version 2.0

January 31, 2018

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
07/22/2015	1.0	All	Initial document	FedRAMP PMO
01/06/2016	1.1	6	Added Formal CAP for second (or more) non-compliant delivery of scan results.	FedRAMP PMO
01/31/2018	2.0	All	Title change from *FedRAMP P-ATO Management and Revocation Guide* to *FedRAMP Continuous Monitoring Performance Management Guide*.	FedRAMP PMO
01/31/2018	2.0	All	General changes to grammar and use of terminology to add clarity, as well as consistency with other FedRAMP documents.	FedRAMP PMO
01/31/2018	2.0	2-5	Added the Escalation Process and clarified the Suspension and Revocation Escalation Actions.	FedRAMP PMO
01/31/2018	2.0	6-8	Clarified deficiency triggers.	FedRAMP PMO
01/31/2018	2.0	8	Added a Zero-day Attack notification trigger.	FedRAMP PMO
01/31/2018	2.0	9	Added Customer Demand threshold.	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides guidance on continuous monitoring and ongoing authorization in support of maintaining a security authorization that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term *authorizing official (AO)*. For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says *Agency AO*. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects. This document may also prove useful for other organizations that are developing a continuous monitoring program.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This document explains the actions FedRAMP takes when a CSP fails to maintain an adequate continuous monitoring capability. The FedRAMP continuous monitoring program 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 Organization*, and is governed by the *FedRAMP Continuous Monitoring Strategy Guide*.

The goal is to provide: (i) operational visibility; (ii) managed change control; and (iii) attendance to incident response duties. Security-related information collected during continuous monitoring is used to determine if the system security is operating as intended and in accordance with applicable Federal law, guidelines, and policies.

When a CSP receives a P-ATO letter for its cloud system, that letter comes with the following minimum requirements:

1. CSP satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP's Continuous Monitoring (ConMon) Strategy Guide and CSP's Continuous Monitoring Plan;
2. CSP mitigates all open Plan of Action and Milestones (POA&M) action items, agreed to in the Security Assessment Report (SAR), within the appropriate timeframe as defined in the agreed POA&M; and
3. CSP identifies and manages significant changes or critical vulnerabilities in accordance with applicable Federal law, guidelines, and policies.

Further, by accepting the P-ATO requirements, as outlined in the P-ATO letter[1], the CSP agrees to maintain Operational Visibility, Change Control, and Incident Response functions clearly defined in the *FedRAMP Continuous Monitoring Strategy Guide*. In addition, the CSP is expected to continue 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 the requirements of the P-ATO may result in escalation actions by FedRAMP, outlined in subsequent sections of this document, as well as additional actions as FedRAMP deems appropriate.

While this document specifically addresses FedRAMP P-ATOs maintained by the JAB, FedRAMP recommends agencies create similar guides and/or use this *FedRAMP Continuous Monitoring Performance Management Guide* when maintaining FedRAMP agency ATOs.

[1] Additional requirements may be included in the P-ATO letter to address system-specific security concerns identified during assessment.

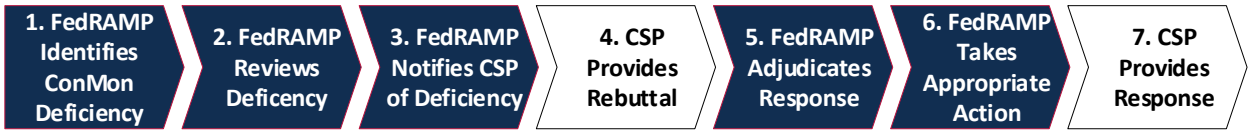
2. ESCALATION LEVELS AND PROCESS

As a condition of the P-ATO, the CSP is agreeing to participate in the FedRAMP ConMon process. If the CSP fails to meet the requirements described in the *FedRAMP Continuous Monitoring Strategy Guide*, FedRAMP initiates an escalation process, which may result in one of the following escalation levels:

- **Detailed Finding Review**: A request from the FedRAMP Point of Contact (POC) for the CSP's security POC to assess a deficiency, and report the cause and remedy back to FedRAMP. If the CSP does not resolve a detailed finding review within the agreed upon timeframe, FedRAMP may escalate to a corrective action plan.
- **Corrective Action Plan (CAP)**: A request from the FedRAMP Director for the CSP's system owner to perform a root-cause analysis and provide a formal plan for remediation. If the CSP does not resolve a CAP within the agreed upon timeframe, FedRAMP may suspend or revoke the system's P-ATO.
- **Suspension**: A decision by the JAB to temporarily suspend a system's P-ATO until identified deficiencies are resolved. If the CSP does not resolve a suspension within the agreed upon timeframe, or if the FedRAMP Director and JAB determine the CSP can no longer meet FedRAMP compliance requirements, FedRAMP may revoke the system's P-ATO.
- **Revocation**: A decision by the JAB to permanently revoke a system's P-ATO. If revoked, the only way the system can obtain a P-ATO is by re-entering the JAB authorization process as if the system were seeking a P-ATO for the first time.

When FedRAMP identifies a deficiency in the CSP's ConMon capabilities, it initiates the process depicted in *Figure 1. FedRAMP Escalation Process,* below.

Figure 1. FedRAMP Escalation Process



The Escalation Process occurs as follows:

1. **FedRAMP identifies a deficiency with the CSP's ConMon information.**
2. **FedRAMP reviews the deficiency and compares it to the CSP's past ConMon performance.** As a result of the review, FedRAMP decides on one of the following actions:
   - FedRAMP typically decides on an escalation level consistent with the guidance described in *Section 3, Common Requirements: Risk Management Deficiency Triggers.*
   - FedRAMP may elect to simply monitor the CSP more closely, but take no further action. If so, no notice is sent and the process stops here.
   - FedRAMP may increase a CSP's existing escalation level. For example, a CSP on a CAP may face Suspension.

- In rare cases, FedRAMP may determine the deficiency is severe enough to make the escalation effective immediately, in which case, steps #3 and 4 are skipped.

3. **FedRAMP notifies the CSP of the deficiency, and FedRAMP's intended escalation.** Depending on the intended escalation level, the notice comes from:
   - the FedRAMP POC for an intended detailed finding review; or
   - the FedRAMP Director for an intended CAP, Suspension, or Revocation.
4. **The CSP responds to the notification.** This CSP's response should include any information that may rebut the escalation decision. Depending on the intended escalation level, the CSP's response must come from:
   - the CSP's security POC for detailed finding review; or
   - the CSP's system owner for a CAP, Suspension, or Revocation.
5. **FedRAMP reviews and adjudicates the CSP's response, and renders a formal escalation decision.** Depending on the escalation level, the decision is made by:
   - the FedRAMP POC for a detailed finding review;
   - the FedRAMP Director for a CAP; or
   - the JAB for a Suspension or Revocation.
6. **FedRAMP notifies the CSP of its decision.** If FedRAMP decides to follow through with an escalation, this notice:
   - identifies the criteria for returning the system to a "Satisfactory" status. It may also include a deadline by which the CSP must fully satisfy the criteria or face more severe escalation; and
   - requires certain actions from the CSP. Typically FedRAMP requires the CSP to perform a root-cause analysis and develop a formal plan for addressing the deficiencies.
7. **CSP responds in accordance with the FedRAMP notification.** This response must include:
   - the results of the root cause analysis;
   - the CSP's plan for fully resolving the issues, with clearly established milestones and dates, including a date of full resolution. For a CAP or Suspension, the plan must be signed by the system owner. FedRAMP must approve the plan; and
   - any other items as specified by FedRAMP in its notification.

When a CSP is subject to escalation as described above, the following occurs:

- **Monthly ConMon Reporting to Leveraging Agencies:** FedRAMP updates the next monthly report to reflect the cited deficiencies, escalation level, and the CSP's identified resolution date.

  The system's status is changed to "Minor Concern" for a detailed finding review, or "Major Concern" for a CAP or Suspension. The status remains and the CSPs progress is reported each month until FedRAMP determines the issue is fully resolved.

  FedRAMP discontinues ConMon reporting when the system's P-ATO is suspended or revoked.

- **Other Postings and Notifications to Leveraging Agencies**: If there is a CAP, Suspension, or Revocation, a letter is posted to OMB MAX for review by leveraging agencies, as is the CSP's plan for resolution where appropriate. The information is retained indefinitely for historical reference.

  If a system's P-ATO is suspended or revoked, FedRAMP will directly notify each known leveraging agency, and will require the CSP to ensure the known leveraging agencies match the CSP's customer list for the impacted system.

  NOTE: P-ATO Revocation does not automatically result in revocation of each leveraging agency's ATO. Each leveraging agency's AO reviews the circumstances of P-ATO Revocation, and makes a determination regarding the status of the ATO they issued the system on behalf of their agency.
- **FedRAMP Marketplace:** FedRAMP updates the system's status on the FedRAMP Marketplace to reflect the escalation level for Suspension. FedRAMP removes the system from the Marketplace if the P-ATO is revoked. Detailed finding review and CAPs are not reflected on the Marketplace.
- **Further Escalation**: If the CSP fails to provide a plan acceptable to FedRAMP, or fails to meet the dates identified in the plan, FedRAMP may increase the escalation level. Further escalation repeats the same escalation process described above.
- **Extension**: If the CSP has made good-faith efforts to fully resolve the deficiency and address the plan, but requires more time, they may request an extension from FedRAMP.

When FedRAMP determines the CSP has fully resolved the cited deficiencies and satisfied the FedRAMP-identified criteria communicated in the notification, FedRAMP takes the following actions:

- **Notification to CSP**: The FedRAMP POC notifies the CSP's security POC when FedRAMP agrees a detailed finding review is fully satisfied. The FedRAMP Director notifies the system owner when FedRAMP agrees a CAP or Suspension is fully satisfied.
- **Monthly ConMon Reporting to Leveraging Agencies**: FedRAMP updates the next monthly report to reflect all cited deficiencies are resolved and the escalation level is no longer in effect. The status is returned to "Satisfactory."
- **Other Postings and Notifications to Leveraging Agencies**: The FedRAMP Director posts a letter to the secure repository indicating the CAP or Suspension is fully resolved to FedRAMP's satisfaction and the CSP is once again in good standing. As no letter is posted when a detailed finding review is initiated, no letter is posted when it is resolved.
- **FedRAMP Marketplace**: FedRAMP returns the system's status to its normal listing with no indication of an escalation level.

3. CONMON REQUIREMENTS: RISK MANAGEMENT DEFICIENCY TRIGGERS

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

Table 1. Risk Management Deficiency Triggers

CONMON PROCESS AREA	RISK MANAGEMENT DEFICIENCY TRIGGER	MINIMUM ESCALATION LEVEL
Operational Visibility	**Unique Vulnerability Count Increase** **20% from P-ATO 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 FedRAMP and may be approved on a case by case basis.*	Detailed Finding Review
	Non Compliance with scanning requirements outlined in the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide (available on FedRAMP.gov) **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 CSP being placed on a Detailed Finding Review. This applies only to a first CSP submission that is non-compliant with authenticated scan requirements.	Detailed Finding Review
	Non-Compliance with scanning requirements outlined in the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide (available on FedRAMP.gov) **Each subsequent incident beyond the first within 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 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 120 days	CAP
	Late Delivery of Annual Assessment Delivery of Annual Assessment SAP less than 60 days before annual P-ATO date	CAP
	Late Delivery of Annual Assessment Delivery of full Annual Assessment P-ATO Package after P-ATO anniversary date	CAP

CONMON PROCESS AREA	RISK MANAGEMENT DEFICIENCY TRIGGER	MINIMUM ESCALATION LEVEL
Operational Visibility (Continued)	**Poor Quality of Deliverables** Untimely or inaccurate submission of any deliverable, including (but not limited to) monthly ConMon documents, Deviation Requests, or Significant Change Requests	Detailed Finding Review
	Lack of Transparency Failure to report known issues to FedRAMP or purposely manipulating scans to avoid Risk Management Triggers	CAP
	Multiple Recurrences Any trigger that is realized multiple times within a 6-month timeframe	CAP
	Insufficient Notice of Planned Change Notification received less than 30 days before the planned change or insufficient documentation of the Security Impact Analysis	CAP
Change Control	**Late Notice of Emergency Change** Notification received longer than five days after the change	CAP
	Undocumented/Unreported Change No notification	CAP
	Degradation of the Change Management and Change Control Processes Insufficient adherence to the provided Configuration Management Plan as determined by FedRAMP	Detailed Finding Review
Incident Response	**Late Incident Notification** Late notification of incident not in accordance with the FedRAMP Incident Communications Procedure and United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines *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
	Incident Frequency Four or more incidents within six months	Detailed Finding Review
	Timely and Ongoing Notification of Zero Day Attack Failure to provide to FedRAMP daily updated progress in addressing Zero Day Attacks	CAP

4. CUSTOMER DEMAND

To remain eligible for a JAB P-ATO, FedRAMP requires a minimum of six unique agency customers with authorizations[2] that leverage the system's JAB P-ATO. FedRAMP evaluates CSP demand on a quarterly basis to ensure CSPs with P-ATOs are meeting and maintaining program demand thresholds.

A CSP that has fewer than six unique Federal Information Security Management Act (FISMA) System ATOs posted on the FedRAMP Secure Repository will be placed on a CAP at the discretion of the FedRAMP Program Management Office (PMO) and JAB. A CSP that cannot meet or maintain this demand threshold has the opportunity to pursue FedRAMP Agency Authorizations, in lieu of the P-ATO, with the support of the FedRAMP PMO.

FedRAMP established this threshold based on JAB resources, to ensure JAB continuous monitoring resources are focused on systems that result in broader impact across the Federal Government. FedRAMP may adjust this threshold at its discretion due to changes in available resources and overall demand across the Federal Government for cloud services.

[2] The FedRAMP PMO does not count the Defense Information Systems Agency (DISA) P-ATO as part of the unique agency customer total because it does not represent a true unique agency customer authorized to use a CSO.

APPENDIX A: FEDRAMP ACRONYMS

The *FedRAMP Master Acronyms & Glossary* contains definitions for all FedRAMP publications, and is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.