

FedRAMP P-ATO Management and Revocation Guide



FedRAMP

Version 1.0

July 29, 2015

Revision History

Date	Version	Page(s)	Description	Author
07/22/2015	1.0	All	Initial version	FedRAMP PMO

How to Contact Us

For questions about FedRAMP or this document, email to info@fedramp.gov.

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

1. INTRODUCTION

This document explains the actions FedRAMP will take when a Cloud Service Provider (CSP) fails to maintain an adequate risk management program. When a CSP receives a Provisional Authority to Operate (P-ATO) for its cloud system, it comes with the following minimum requirements:

1. *The CSP satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP's continuous monitoring (ConMon) requirements and CSP's Continuous Monitoring Plan;*
2. *CSP mitigates all open low and moderate POA&M action items, agreed to in the Security Assessment Report (SAR); and*
3. *Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies.¹*

This document lays out the escalation processes and procedures as well as minimum mandatory escalation actions FedRAMP will take when a CSP fails to adhere to the requirements of the P-ATO.

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

2. ESCALATION PROCESS AND PROCEDURES

If a CSP fails to meet the FedRAMP ConMon requirements described in the *FedRAMP Continuous Monitoring Strategy Guide*, FedRAMP will initiate the escalation process defined in Table 1 below. This escalation process outlines actions that can be taken by FedRAMP, but is not necessarily linear. The severity and scope of the change in the cloud system's risk posture will define the escalation action taken by FedRAMP.

¹ As a note, there may be additional requirements included in the P-ATO that address cloud system specific security concerns that were identified.

Table 1. Escalation Process

Escalation Actions	FedRAMP Action
Internal Corrective Action	<p>If a CSP cannot meet the FedRAMP ConMon requirements for their cloud system:</p> <ul style="list-style-type: none"> • FedRAMP will notify the CSP of the specific failures to comply with FedRAMP ConMon. • The CSP will provide a Corrective Action Plan (CAP) to FedRAMP including a time period agreement to fix the specific failures noted by FedRAMP. <ul style="list-style-type: none"> ○ The CAP must be provided to FedRAMP within 1 week of notice of the failures to comply with FedRAMP ConMon. • FedRAMP will notify the JAB teams on issues and the CSP’s CAP and continued progress.
Formal Corrective Action Plan	<p>If a CSP cannot meet the stated requirements within FedRAMP ConMon for their cloud system:</p> <ul style="list-style-type: none"> • The FedRAMP Director will send a letter to the CSP notifying the CSP a CAP is required. The letter will outline the specific failures of the CSP’s ConMon activities. • The letter will be posted in the FedRAMP Secure Repository for leveraging agencies to see. • The CSP shall provide a CAP to FedRAMP including a time period agreement to fix the specific failures noted by FedRAMP. <ul style="list-style-type: none"> ○ The CAP must be provided to FedRAMP within 1 week of receipt of the letter from the FedRAMP Director. ○ The CAP must be signed by the System Owner. ○ The CAP must be agreed to by FedRAMP. • The CAP and updates will be posted to the FedRAMP Secure Repository. • Once the CAP is completed, the FedRAMP Director will post a letter to the FedRAMP Secure Repository detailing the successful completion of the CAP and the CSP’s adherence with FedRAMP ConMon requirements.
Suspension	<p>If a CSP cannot meet the stated requirements within FedRAMP ConMon for their cloud system:</p> <ul style="list-style-type: none"> • The FedRAMP Director will send a letter to the CSP notifying the CSP of possible P-ATO suspension. The letter will outline the specific failures of the CSP’s ConMon activities. • The FedRAMP Director will initiate a formal JAB P-ATO review to

Escalation Actions	FedRAMP Action
	<p>determine if the risk level requires suspension of the JAB P-ATO.</p> <ul style="list-style-type: none"> • The CSP shall provide a CAP to FedRAMP including a time period agreement to fix the specific failures noted by FedRAMP. <ul style="list-style-type: none"> ○ The CAP must be provided to FedRAMP within 1 week of the letter from the FedRAMP Director. ○ The CAP must be signed by the System Owner. • The JAB will review the CAP and either grant the CSP more time to mitigate the issue(s) or suspend the P-ATO for a specific period of time. • The JAB’s decision and necessary actions will be documented and a letter will be posted in the FedRAMP Secure Repository and all known agencies leveraging the CSP’s cloud system will be notified. • Once the CAP is completed, the FedRAMP Director will post a letter to the FedRAMP Secure Repository detailing the successful completion of the CAP and the CSP’s adherence with FedRAMP ConMon requirements.
Revocation	<p>If a CSP cannot meet the stated requirements within FedRAMP ConMon for their cloud system:</p> <ul style="list-style-type: none"> • The FedRAMP Director will send a letter to the CSP notifying the CSP of possible P-ATO revocation. The letter will outline the specific failures of the CSP’s ConMon activities. • The JAB may decide to have a formal P-ATO review initiated by the FedRAMP Director to determine if the risk level requires revocation of the JAB P-ATO. • The CSP shall provide a CAP to FedRAMP including a time period agreement to fix the specific failures noted by FedRAMP. <ul style="list-style-type: none"> ○ The CAP must be provided to FedRAMP within 1 week of the letter from the FedRAMP Director. ○ The CAP must be signed by the System Owner. • The JAB will review the CAP and either grant the CSP more time to mitigate the issue(s), or revoke the P-ATO. • The JAB’s decision and necessary actions will be documented, a letter will be posted in the FedRAMP Secure Repository, and all known agencies leveraging the CSP’s cloud system will be notified.

3. COMMON REQUIREMENTS: MEASUREMENTS, ACTIONS, AND RESPONSES

Each section below explains a ConMon requirement, associated risk factor, what action the FedRAMP PMO will take in response to that risk factor, and what action the organization must then take to maintain its P-ATO. Although each of the categories is identified as a separate risk factor, together they represent a system-based approach to risk management. For example, a risk factor of “increased vulnerabilities” and “past due” Plan of Action and Milestones (POA&M) items may actually be the result of poor configuration/change management process and procedures.

Any past due vulnerabilities can lead to an escalation action by FedRAMP based on the number and severity of the vulnerabilities. The table below includes the minimum escalation actions that will be taken by FedRAMP based on a CSP’s vulnerability management deficiency, however more severe escalation actions can be taken by FedRAMP and will be determined on a case by case basis.

Table 2. Risk Management Deficiencies

ConMon Process Area	Risk Management Deficiency	Mandatory Minimum Escalation Action
Operational Visibility	Unique Vulnerability Count Increase <i>20% or more from P-ATO</i>	Internal CAP
	Non Adherence to scanning requirements outlined in the <i>FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide</i> (available on FedRAMP.gov) <i>First non-compliant delivery of scan results and/or evidence to FedRAMP</i>	Internal CAP
	Late Remediation High Impact Vulnerabilities <i>5 or more unique vulnerabilities or POA&Ms aged greater than 30 days</i>	Internal CAP
	Late Remediation High Impact Vulnerabilities <i>5 or more unique vulnerabilities or POA&Ms aged greater than 60 days</i>	Formal CAP
	Late Remediation Moderate Impact Vulnerabilities <i>10 or more unique vulnerabilities or POA&Ms aged greater than 90 days</i>	Internal CAP
	Late Remediation Moderate Impact Vulnerabilities	Formal CAP

FedRAMP P-ATO Management and Revocation Guide

ConMon Process Area	Risk Management Deficiency	Mandatory Minimum Escalation Action
	<i>10 or more unique vulnerabilities or POA&Ms past due 120 days or longer</i>	
	Late Delivery of Annual Assessment <i>Delivery of Annual Assessment SSP less than 60 days before annual P-ATO date</i>	Formal CAP
	Late Delivery of Annual Assessment <i>Delivery of Annual Assessment SAR after P-ATO anniversary date</i>	Formal CAP
Significant Changes	Insufficient Notice of Planned Change <i>Notification received less than 30 days</i>	Formal CAP
	Late Notice of Emergency Change <i>Notification received longer than 5 days after the change</i>	Formal CAP
	Undocumented/Unreported Change <i>No notification</i>	Formal CAP
Incident Response	Incident Notification <i>Late notification of incident in accordance with US CERT reporting guidelines</i>	Formal CAP
	Incident Frequency of Re-Occurring Type <i>Any incident with re-occurring type and/or cause</i>	Formal CAP
	Incident Frequency <i>4 or more incidents within 6 months</i>	Internal CAP

APPENDIX A: TABLE OF ACRONYMS

Acronym	Meaning
AO	Authorizing Official
CAP	Corrective Action Plan
ConMon	Continuous Monitoring
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
JAB	Joint Authorization Board
P-ATO	Provisional Authority to Operate
PMO	Program Management Office
POA&M	Plan of Action and Milestones
SAR	Security Assessment Report
TR	Technical Representative