FedRAMP Plan of Actions and Milestones (POA&M) Template Completion Guide

Version 2.1

February 21, 2018

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
02/18/2015	1.0	All	Publish Date	FedRAMP PMO
09/01/2015	1.1	All	Clarifications and format updates	FedRAMP PMO
10/21/2016	1.2	4-5	Instructions for the new Integrated Inventory Template Section 2.3; Operational Requirements – False Positive Updates to Table 2 – POA&M Items Column Information Description and Section 2.3	FedRAMP PMO
6/6/2017	1.2	Title	Updated Logo	FedRAMP PMO
1/31/2018	2.0	All	General changes to grammar and use of terminology to add clarity, as well as consistency with other FedRAMP documents.	FedRAMP PMO
1/31/2018	2.0	3	Corrected conflicting information in Sections 2 and 2.3 of the POA&M Template Completion Guide regarding the *FedRAMP Integrated Inventory Workbook Template*.	FedRAMP PMO
1/31/2018	2.0	6	Added text instructing CSPs to deliver the inventory workbook template **as part of their monthly ConMon package**, along with or included in their POA&M, in the same location as their POA&M.	FedRAMP PMO
1/31/2018	2.0	7	Updated guidance that findings from automated tools only need to be added to the POA&M once they are late.	FedRAMP PMO
1/31/2018	2.0	7	Automated tool findings identified as Low will be considered late after 180 calendar days.	FedRAMP PMO
2/21/2018	2.1	3	Revised guidance in the description for Column A – POA&M ID	FedRAMP PMO
2/21/2018	2.1	5	Added a description for Column AA – Auto-Approve	FedRAMP PMO
2/21/2018	2.1	6, 8	Updated links to resources resulting from new FedRAMP web site migration.	FedRAMP PMO
4/3/2018	2.1	7	Updated footnote.	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides guidance on completing the Federal Risk and Authorization Management Program (FedRAMP) Plan of Action and Milestones (POA&M) Template in support of achieving and maintaining a security authorization that meets 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.

The term *authorization* refers to either a FedRAMP JAB P-ATO or a FedRAMP Agency ATO.

The term *third-party assessment organization (3PAO)* refers to an accredited 3PAO. Use of an accredited 3PAO is required for systems with a FedRAMP JAB P-ATO; however, for systems with a FedRAMP Agency ATO this may refer to any assessment organization designated by the Agency AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Cloud Service Providers (CSPs), 3PAOs, government contractors working on FedRAMP projects, and government employees working on FedRAMP projects.

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

DOCUMENT REVISION HISTORY I

ABOUT THIS DOCUMENT II

WHO SHOULD USE THIS DOCUMENT? II

HOW TO CONTACT US II

1. INTRODUCTION 1
   - 1.1. POA&M Purpose 1
   - 1.2. Scope 2

2. POA&M TEMPLATE 2
   - 2.1. Worksheet 1: Open POA&M Items 2
   - 2.2. Worksheet 2: Closed POA&M Items 6
   - 2.3. Integrated Inventory Workbook 6

3. GENERAL REQUIREMENTS 7

APPENDIX A: FEDRAMP ACRONYMS 8

LIST OF TABLES

Table 1. POA&M Items Header Information Description 2

Table 2. POA&M Items Column Information Description 3

1. INTRODUCTION

This document provides guidance for completing and maintaining a FedRAMP-compliant POA&M using the *FedRAMP POA&M Template*. The POA&M is a key document in the security authorization package and monthly continuous monitoring activities. It identifies the system's known weaknesses and security deficiencies, and describes the specific activities the CSP will take to correct them.

A CSP applying for a FedRAMP JAB P-ATO, or a FedRAMP Agency ATO, must establish and maintain a POA&M for their system in accordance with this *POA&M Template Completion Guide* using the *FedRAMP POA&M Template*. The *FedRAMP POA&M Template* is available separately at: http://www.fedramp.gov/.

The *FedRAMP POA&M Template* provides the required information presentation format for preparing and maintaining a POA&M for the system. The CSP may add to the format, as necessary, to comply with its internal policies and FedRAMP requirements; however, CSPs are not permitted to alter or delete existing columns or headers.

1.1. POA&M PURPOSE

The purpose of the POA&M is to facilitate a disciplined and structured approach to tracking risk-mitigation activities in accordance with the CSP's priorities. The POA&M includes security findings for the system from periodic security assessments and ongoing continuous monitoring activities. The POA&M includes the CSP's intended corrective actions and current disposition for those findings.

FedRAMP uses the POA&M to monitor the CSP's progress in correcting these findings.

The POA&M includes the:

- Security categorization of the cloud information system;
- Specific weaknesses or deficiencies in deployed security controls;
- Importance of the identified security control weaknesses or deficiencies;
- Scope of the weakness in components within the environment; and
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security control implementations (e.g., prioritization of risk mitigation actions and allocation of risk mitigation resources).

The POA&M identifies: (i) the tasks the CSP plans to accomplish, including a recommendation for completion either before or after information system implementation; (ii) any milestones the CSP has set in place for meeting the tasks; and (iii) the scheduled completion dates the CSP has set for each milestone.

1.2. SCOPE

The scope of the POA&M includes security control implementations, including all management, operational, and technical implementations, that have unacceptable weaknesses or deficiencies. The CSP is required to submit an updated POA&M to the AO in accordance with the *FedRAMP Continuous Monitoring Strategy & Guide.*

2. POA&M TEMPLATE

The *FedRAMP POA&M Template* is an Excel Workbook containing two worksheets:

- **Open POA&M Items**, which contains the unresolved entries; and
- **Closed POA&M Items**, which contains resolved entries.

2.1. WORKSHEET 1: OPEN POA&M ITEMS

The Open POA&M Items worksheet has two sections. The top section of the worksheet contains basic information about the system, which is described in *Table 1. POA&M Items Header Information Description*, below. The bottom section is a list that enumerates each open POA&M entry, which is described in *Table 2. POA&M Items Column Information Description*, below.

Table 1. POA&M Items Header Information Description

FEDRAMP SYSTEM CATEGORIZATION	IDENTITY ASSURANCE LEVEL (IAL)
CSP	The Vendor Name as supplied in the documents provided to the AO.
System Name	The Information System Name as supplied in the documents provided to the AO.
Impact Level	Cloud Service Offerings (CSOs) are categorized as **Low, Moderate, or High** based on a completed FIPS 199/800-60 evaluation. FedRAMP supports CSOs with High, Moderate, and Low security impact levels.
POA&M Date	The date the POA&M was last updated. For an initial authorization, this is the date to which the CSP committed in their continuous monitoring plan.

The bottom section of the *Open POA&M Items* worksheet includes the CSP's corrective action plan used to track IT security weaknesses. This section of the POA&M worksheet has similarities to the National Institute of Standards and Technology's (NIST) format requirements; however, it contains additional data and formatting as required by FedRAMP.

Table 2. POA&M Items Column Information Description

COLUMN	DETAILS
Column A – POA&M ID	Assign a unique identifier to each POA&M item. While this can be in any format or naming convention that produces uniqueness, FedRAMP recommends the convention V-<incremented number> (e.g., V-123). This identifier is assigned by the CSP to a unique vulnerability in the CSP system. Often, during annual assessment activities the 3PAO identifies a vulnerability that the CSP has already identified through continuous monitoring activities, or vice versa. If the same vulnerability is detected on the same assets, the same POA&M ID must be used by both parties. The earlier of the two detection dates applies. If the same vulnerability is discovered on additional assets at a later date, a new POA&M ID and detection date may be used for the new assets.
Column B – Controls	Specify the FedRAMP security control affected by the weakness identified during the security assessment process.
Column C – Weakness Name	Specify a name for the identified weakness that provides a general idea of the weakness. Use the Weakness Name provided by the security assessor, or taken from the vulnerability scanner that discovered the weakness.
Column D – Weakness Description	Describe the weakness identified during the assessment process. Use the Weakness Description provided by the security assessor or the vulnerability scanner that discovered the weakness. Provide sufficient data to facilitate oversight and tracking. This description must demonstrate awareness of the weakness and facilitate the creation of specific milestones to address the weakness. In cases where it is necessary to provide sensitive information to describe the weakness, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
Column E – Weakness Detector Source	Specify the name of the 3PAO, vulnerability scanner, or other entity that first identified the weakness. In cases where there are multiple 3PAOs, include each one on a new line.
Column F – Weakness Source Identifier	Often, the scanner/assessor will provide an identifier (ID/Reference #) that specifies the weakness in question. This allows further research of the weakness. Provide the identifier, or state that no identifier exists.
Column G – Asset Identifier	List the asset/platform on which the weakness was found. This must correspond to the Asset Identifier for the item provided in the system's *Integrated Inventory Workbook.* The inventory workbook must be maintained as part of the CSP's configuration management processes, and submitted as one of continuous monitoring deliverables each month. Include a complete Asset Identifier for each affected asset. Do not use an abbreviation or "shorthand." The CSP may obfuscate the asset information when it is

COLUMN	DETAILS
	required by the internal policies of the CSP. The Asset Identifier must be unique and consistent across all POA&M documents, 3PAOs, and any vulnerability scanning tools.
Column H – Point of Contact	Identify the person/role that the AO holds responsible for resolving the weakness. The CSP must identify and document a Point of Contact (POC) for each reported weakness.
Column I – Resources Required	Identify resources required for resolving the weakness and when applicable, provide an estimated staff time in hours.
Column J – Overall Remediation Plan	Provide a high-level summary of the actions required to remediate the plan. In cases where it is necessary to provide sensitive information to describe the remediation plan, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
Column K – Original Detection Date	Provide the month, day, and year when the weakness was first detected. This must be consistent with the Security Assessment Report (SAR) and/or any continuous monitoring activities. The CSP may not change the Original Detection Date.
Column L – Scheduled Completion Date	The CSP must assign a completion date to every weakness that includes the month, day, and year. The Scheduled Completion Date column must not change once it is recorded. See Section 2.2 for guidance on closing a POA&M item.
Column M – Planned Milestones	Each weakness must have a milestone entered with it that identifies specific actions to correct the weakness with an associated completion date. Planned Milestone entries shall not change once they are recorded.
Column N – Milestone Changes	List any changes to existing milestones in Column M, Planned Milestones, in this column.
Column O – Status Date	This column must provide the latest date an action was taken to remediate the weakness or some change was made to the POA&M item.
Column P – Vendor Dependency	This column indicates the remediation of the weakness required by the action of a third party vendor (e.g., through the issuing of a patch that is not yet released). The CSP is required to check the status of the vendor's remedy at least every 30 days. As long as the fix is still pending from the vendor, and the CSP has checked-in within 30 days of POA&M submission, FedRAMP will not count the entry as late. Once the vendor makes the fix available, the CSP has 30 days to remediate high vulnerabilities, 90 days to remediate moderate vulnerabilities, and 180 days to remediate low vulnerabilities from the date the vendor makes the fix available. The CSP must provide the vendor's release date in column Z (comments). In this case, the CSP may overwrite the auto-calculated scheduled completion date found in column L.
Column Q – Last Vendor Check-in Date	This column is used to record the date the CSP most recently checked-in with a third party vendor regarding the availability of an un-released remedy for a known product vulnerability. If *Column P – Vendor Dependency* is "Yes," the CSP must check-in with the third-party vendor at least every 30 days and record the most recent date of check-in here. If *Column P – Vendor Dependency* is "No," the CSP may leave this column blank.

COLUMN	DETAILS
Column R – Vendor Dependent Product Name	If *Column P – Vendor Dependency* is "Yes," the CSP must provide the name of the product that the third-party vendor has responsibility. If *Column P – Vendor Dependency* is "No," the CSP may leave this column blank.
Column S – Original Risk Rating	Provide the original risk rating of the weakness at the time it was identified as part of an assessment and/or continuous monitoring activities.
Column T – Adjusted Risk Rating	Provide the adjusted risk rating after a *FedRAMP Deviation Request Form* is submitted. If no risk adjustment is made, state N/A. In the case that the scanner changes its risk rating from a lower to a higher risk rating, the CSP may update this column and set column U to "Yes." No deviation request form is necessary in this case.
Column U – Risk Adjustment	State the status of the deviation request for a risk adjustment request. If the CSP believes a risk adjustment is appropriate, they must set this column to "Pending" and immediately submit a deviation request to their AO using the *FedRAMP Deviation Request Form*, including mitigating factors. If the AO approves the deviation request, the CSP must change this to "Yes." If the AO denies the deviation request, or if the CSP does not intend to request a risk adjustment, the CSP must set this entry to "No." The CSP must set this column to "pending" if submitting a risk adjustment. The adjustment is finalized (setting the Risk Adjustment to "yes") if it is approved by the AO. Only AO-approved risk adjustments may alter the scheduled completion date.
Column V – False Positive	State the status of the deviation request for a false positive (FP). A FP occurs when a vulnerability is identified that does not actually exist on the system. This is known to happen from time-to-time with scanning tools. If the CSP believes a finding is an FP, they must set this column to "Pending" and immediately submit a deviation request to their AO using the *FedRAMP Deviation Request Form*, including evidence of the FP. If the AO approves the deviation request, the CSP must change this to "Yes." If the AO denies the deviation request, or if the CSP does not believe the finding is a FP, the CSP must set this entry to "No." AO-approved false positives can also be closed; see Section 2.2 for guidance on closing a POA&M item.
Column W – Operational Requirement	State the status of the deviation request for an operational requirement (OR). An OR means that there is a weakness in the system that will remain an open vulnerability that cannot be corrected without impacting the full operation of the system. An OR is also an open vulnerability that could be exploited, regardless of the limited opportunity for exploitation, such as a component that is installed but not enabled. A CSP determination of an operational requirement will cause this column to be set to "pending." The deviation is finalized, setting the status to "yes", if it is approved by the AO. Approved operational requirements must remain on the Open POA&M Items worksheet, and must be periodically reassessed by the CSP.

COLUMN	DETAILS
Column X – Deviation Rationale	Provide a rationale for any deviation request submitted to the AO. For operational requirements and risk adjustments, include mitigating factors and compensating controls that address the specific risk to the system. For false positives, include information about evidence/artifacts that support the result.
Column Y – Supporting Documents	List any additional documents that are associated with the POA&M item.
Column Z – Comments	Provide any additional comments that have not been provided in any of the other columns.
Column AA – Auto-Approve	Indicates an automatic risk adjustment. This field is only for use by CSPs with prior JAB approval to automatically downgrade risks based on established criteria.

2.2. WORKSHEET 2: CLOSED POA&M ITEMS

The top of the *Closed POA&M Items* worksheet contains the system information as the top of the *Open POA&M Items* worksheet. The remainder of the worksheet contains the POA&M items that are completed. The details should reflect almost all of the information provided in the *Open POA&M Items* worksheet; however, the CSP must update *Column O – Status Date*, with the date of completion.

To "close" a POA&M item, update the date in *Column O – Status Date*, and move the POA&M item to Worksheet 2, *Closed POA&M Items*.

A POA&M item can be moved to the Closed POA&M Items worksheet when either of the following occurs:

- All corrective actions have been applied and evidence of mitigation is collected by the CSP available for inspection. Evidence of mitigation must then be verified by a 3PAO during initial and periodic assessments, and may be requested by the AO at any time.
- A false positive deviation request was approved by the AO.

2.3. INTEGRATED INVENTORY WORKBOOK

The CSP must continuously maintain an inventory workbook using the *FedRAMP Integrated Inventory Workbook Template*, available separately on the FedRAMP website Templates page. In accordance with the *FedRAMP Continuous Monitoring Strategy & Guide*, the CSP must submit their up-to-date inventory workbook each month with their POA&M and other continuous monitoring deliverables.

The CSP may insert their inventory workbook as an additional worksheet in the POA&M, or retain it as a separate document. If retained separately, the inventory workbook and POA&M must be submitted together and placed in the same OMB MAX container each month. Please see the *Integrated Inventory Workbook Template* for instructions on completing and updating the inventory of system assets.

3. GENERAL REQUIREMENTS

The CSP must include the following in the *Open POA&M Items* worksheet:

- All security vulnerabilities identified through vulnerability scanning tools, where the CSP is late remediating the vulnerability[1];
- All known security vulnerabilities and deficiencies identified through means other than vulnerability scanning tools (e.g., interviews and penetration testing); and
- All security vulnerabilities for which the CSP is submitting a Deviation Request.

A security vulnerability remediation is late if it is not remediated within the time requirements detailed in the *FedRAMP Continuous Monitoring Strategy & Guide*, and summarized in the bullets below.

The CSP must comply with the following:

- Use the *FedRAMP POA&M Template* to track and manage POA&M items.
- If a finding is identified in the SAR, or as a result of continuous monitoring activities, it must be included as an item on the POA&M.
- All POA&M entries must map back to a finding in the SAR and/or continuous monitoring activities.
- False positives identified in the SAR (Appendices C, D, and E), along with supporting evidence (e.g., clean scan report) do not have to be included in the POA&M.
- Each finding in the POA&M must have a unique identifier. This unique identifier must pair with a respective SAR finding and continuous monitoring activities.
- All high and critical risk findings must be remediated prior to receiving a JAB P-ATO.
- High and critical risk findings identified through continuous monitoring activities must be remediated within 30 days after identification.
- Moderate findings must be remediated within 90 days following the P-ATO date, or 90 days following identification.
- Low findings must be remediated within 180 days following the P-ATO date, or 180 days following identification.

Note: *The POA&M Spreadsheet has problems with data validation in the Mac version of Microsoft Office. Disabling macros typically resolves this issue.*

[1] Previously, FedRAMP required the CSP to enter all scanner-identified findings into the POA&M. Now only late scanner-identified findings are required. This only applies to findings identified by a scanning tool. All other findings must still be entered into the POA&M, whether they are late or not. This includes deficiencies identified through assessment interviews and penetration testing activities. CSP's must provide raw scan data to their AO in order to satisfy this requirement. Additionally, CSP's must comply with any SLA's or AO preference in meeting this requirement (e.g. potentially including all open risks in the POA&M). It is the JAB's requirement to have CSP's comply with this by providing raw scan data.

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/documents/)

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