

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



FedRAMP

Version 1.1

September 3, 2015

Document Revision History

Date	Pages	Description	Author
02/18/2015		Publish Date	FedRAMP PMO
09/01/2015	All	Clarifications and Format Updates	FedRAMP PMO

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
How to Contact Us	i
1. Introduction	1
1.1. 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	5
2.3. Worksheet 3: Inventory	5
3. General Requirements	7
Appendix A – FedRAMP Acronyms	9

List of Tables

Table 1 – POA&M Items Header Information Description	2
Table 2 – POA&M Items Column Information Description.....	3
Table 3 – POA&M Template Inventory Information Description.....	6

1. INTRODUCTION

The Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO) prepared this document to provide guidance for completing the Plan of Action and Milestones (POA&M) Template. The POA&M is a key document in the security authorization package. It describes the specific tasks the Cloud Service Provider (CSP) has planned to correct any weaknesses or deficiencies in the security controls noted during the assessment and to address the residual vulnerabilities in their cloud system.

CSPs applying for a FedRAMP Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) should use this guide while completing the *POA&M Template*, which is available at: <http://www.fedramp.gov/resources/templates-3/>. CSPs develop the POA&M document in the *POA&M Template* according to the rules and requirements described in this guide to ensure consistency across providers. The POA&M Template provides the required format for preparing the Plan of Action and Milestones. The CSP may add to the format as necessary to comply with its internal policies and FedRAMP requirements; however, CSPs are restricted from altering columns or headers.

1.1. PURPOSE

The purpose of the POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with the CSP's priorities. The POA&Ms include the findings and recommendations of the Security Assessment Report (SAR) and the continual security assessments.

FedRAMP uses the POA&M to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment and throughout the continuous monitoring process.

The POA&Ms are based on 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 systems within the environment
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (for example, prioritization of risk mitigation actions, allocation of risk mitigation resources)

The POA&M identifies: (i) the tasks the CSP plans to accomplish with 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 the milestones.

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 POA&M also includes an up-to-date list of assets within the environment, based on the list provided in the Security Assessment Plan (SAP). CSPs are required to submit updated POA&Ms to the Authorizing Official (AO) in accordance with the *FedRAMP Continuous Monitoring Strategy & Guide*.

2. POA&M TEMPLATE

CSPs gather and report basic system and weakness information in the *POA&M Template*. The *POA&M Template* is an Excel Workbook containing three worksheets: The Open POA&M Items, Closed POA&M Items, and Inventory. CSPs should complete the System Inventory worksheet first because the Asset Identifier in the POA&M worksheet refers to the inventory items.

2.1. WORKSHEET 1: OPEN POA&M ITEMS

The Open POA&M Items worksheet has two sections. The top section of the worksheet documents basic system information and tracks the headers described in the table below:

Table 1 – POA&M Items Header Information Description

Headers	Details
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	Systems are categorized as Low, Moderate, or High based on a completed FIPS 199/800-60 evaluation. FedRAMP currently supports Moderate and Low risk impact level systems.
POA&M Date	The date the POA&M was created, which is the date the CSP committed to in their continuous monitoring plan.

The bottom section of the Open POA&M Items worksheet is the corrective action plan used to track IT security weaknesses. This section of the POA&M worksheet has some similarities to the National Institute of Standards and Technology’s (NIST) format requirements, but requires 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. This can be in any format or naming convention that produces uniqueness, but FedRAMP recommends the convention V-<incremented number>. (for example, V-123)
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 should 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 Third Party Assessment Organization (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 should correspond to the Asset Identifier for the item provided in Worksheet 3, Inventory List, as well as any applicable network ports and protocols. 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 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. See Section 2.3 for formatting requirements.
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 any cost associated with resolving the weakness and 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 should be consistent with the SAR and/or any continuous monitoring activities. The CSP may not change the Original Detection Date.

Column	Details
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 should 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 should specify whether the remediation of the weakness requires the action of a third party vendor. Should a weakness be vendor dependent, a monthly update with the third party vendor is required. In these cases, the weakness cannot be remediated, and the POA&M item cannot be closed, but the completion date may be extended if a monthly update is made. If the completion date is extended, provide an update in Column N, Milestone Changes. Once a patch is available, the CSP has 30 days to remediate high vulnerabilities and 90 days to remediate moderate vulnerabilities according to FedRAMP standards. This timeframe begins on the date that the patch is released. The CSP must include the patch 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	If the remediation of the weakness is dependent on a third party vendor's action, as specified in Column P, Vendor Dependency; a monthly update with the third party vendor is required. Provide the date that the latest update was made.
Column R – Vendor Dependent Product Name	If the remediation of the weakness is vendor dependent, provide the name of the product for which the third party vendor has responsibility.
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 when a 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 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 risk adjustment request. CSP determination of a risk adjustment will cause this column to be set to "pending." The adjustment is finalized (setting the Risk Adjustment to "yes") if it is approved by the AO. Approved risk adjustments may alter the scheduled completion date.
Column V – False Positive	State the status of the weakness deviation request for false positive. A false positive means the weakness is determined to be non-existent and is a false positive provided by the vulnerability scanner. A CSP determination of a false positive will cause this column to be set to "pending", the deviation is finalized (setting the status to "yes") if it is

Column	Details
	approved by the 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 weakness deviation request for operational requirement. An operational requirement means that the weakness cannot be remediated without affecting the operation of the system. 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 remain on Worksheet 1, <i>POA&M Template</i> , and are to be periodically reassessed by the CSP.
Column X – Deviation Rationale	Provide a rationale for the various weakness deviations requested for the item.
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.

2.2. WORKSHEET 2: CLOSED POA&M ITEMS

The Closed POA&M Items worksheet contains similar basic system information as the top of Worksheet 1, Open POA&M Items. The remainder of the document should contain the POA&M items that are completed. The details will reflect almost all of the information provided in the Open POA&M Items worksheet; however, Column O, Status Date, needs to be updated to 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 when either of the following occurs:

- All corrective actions have been applied and evidence of mitigation has been provided. Evidence of mitigation can be verification by a 3PAO, a targeted vulnerability scan that covers the weakness domain, the following continuous monitoring scans, etc.
- A false positive request was submitted and approved by the AO.

2.3. WORKSHEET 3: INVENTORY

The Inventory worksheet is an up to date list of known assets within the system, and is similar to the inventory provided in the SAR.

Table 3 – POA&M Template Inventory Information Description

Column	Details
Column A – Unique Asset Identifier	Include a complete Asset Identifier for each inventory item. This can be in any format or naming convention that produces uniqueness, but FedRAMP suggests the convention used in the CSP internal network, be it IP address, or Domain Name. Do not use an abbreviation or “shorthand.” The CSP may obfuscate the asset information when it is 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. Use the IP address or DNS name as an identifier if obfuscation is not required.
Column B – IPv4	If available, state the IPv4 address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column C – IPv6	If available, state the IPv6 address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column D – DNS Name	If available, state the DNS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column E – NetBIOS Name	If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column F – MAC Address	If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column G – Asset Weight	Estimate the criticality of the item within the network as a number from 1-10; where 10 means that the item can cause a catastrophic effect on the environment, and 1 means that the item can cause only a limited effect on the environment.
Column H – Authenticated Scan	State whether or not (Yes or No) the inventory item will be authenticated during the vulnerability scan.
Column I – Baseline Configuration Name	If available, provide the name of the configuration template used within the CSP configuration management.
Column J – OS Name	Provide the name of the operating system running on the asset.
Column K – OS Version	Provide the version number of the operating system running on the asset.
Column L – Location	Provide the general location of the asset if the information is available.
Column M – Asset Type	Provide a general overview of the function of the asset.
Column N – Virtual	State whether the asset is a virtualized device.
Column O – Public	State whether the asset has any public facing ports.

Column	Details
Column A – Unique Asset Identifier	Include a complete Asset Identifier for each inventory item. This can be in any format or naming convention that produces uniqueness, but FedRAMP suggests the convention used in the CSP internal network, be it IP address, or Domain Name. Do not use an abbreviation or “shorthand.” The CSP may obfuscate the asset information when it is 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. Use the IP address or DNS name as an identifier if obfuscation is not required.
Column B – IPv4	If available, state the IPv4 address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field. However, if it is used as an identifier in vulnerability scans or security assessments, the field must be present.
Column P – In Latest Scan	Determine whether or not (Yes or No) the asset should appear in the network scans and can be probed by the scans creating the current POA&M.
Column Q – Comments	Provide any additional comments about the inventory item that have not been provided in any of the other columns.

3. GENERAL REQUIREMENTS

POA&Ms must include all known security weaknesses within the cloud information system.

POA&Ms must comply with the following:

- Use the *POA&M Template* to track and manage POA&Ms.
- If a finding is reported in the SAR and/or in the continuous monitoring activities, the finding must be included as an item on the POA&M.
- All findings must map back to a finding in the SAR and/or any continuous monitoring activities.
- False positives identified in the SAR (Appendices C, D, and E), along with supporting evidence (for example, clean scan report) do not have to be included in the POA&M.
- Each line item on the POA&M must have a unique identifier. This unique identifier should pair with a respective SAR finding and/or any continuous monitoring activities.
- All high and critical risk findings must be remediated prior to receiving a Provisional Authorization.
- High and critical risk findings identified following Provisional Authorization through continuous monitoring activities must be mitigated within 30 days after identification.
- Moderate findings shall have a mitigation date within 90 days of Provisional Authorization date or within 90 days of identification as part of continuous monitoring activities.

- The POA&M must be submitted in an appropriate format for the FedRAMP automated processes. See the example row in the *POA&M Template*.

Note: The POA&M Spreadsheet has problems with data validation in the Mac version of Microsoft Office. Disabling macros should prove to be a sufficient work-around.

Appendix A – FedRAMP Acronyms

Acronym	Description
3PAO	Third Party Assessment Organization
AO	Authorizing Official
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
P-ATO	Provisional Authorization to Operate
PMO	Program Management Office
POC	Point of Contact
POA&M	Plan of Action and Milestones
SAP	Security Assessment Plan
SAR	Security Assessment Report