Plan of Action and Milestones (POA&M)



<Vendor Name>

<Information System Name>

Version #

May 6, 2013

**Company Sensitive and Proprietary**

**For Authorized Use Only**

nistBlue

Table of Contents

ABOUT THIS DOCUMENT 4

Who should use this document? 4

Conventions used in this document 4

How to contact us 5

1. INTRODUCTION 6

1.1. Purpose 6

1.2. Scope 6

1.3. System Description 6

2. Methodology 7

Worksheet 1: System POA&M 7

Worksheets 2 - 4: FYXXQX POA&M Update 8

General Requirements 9

Embedded POA&M Spreadsheet (Click to open): 10

APPENDIX A.   ACRONYMS 11

APPENDIX B.   REFERENCES 12

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version | Author |
| 05/02/2012 | Document Publication | N/A | FedRAMP Office |
| 5/6/2013 | Updated to incorporate changes to worksheet | N/A | FedRAMP Office |

ABOUT THIS DOCUMENT

This document is released in template format. Once populated with content, this document will include detailed information about service provider information system deficiencies and plan of action and milestones for how the deficiencies will be mitigated.

Who should use this document?

This document is intended to be used by service providers who are applying for an Authorization to Operate (ATO) through the U.S. federal government FedRAMP program.

This template provides a sample format for preparing the Plan of Action and Milestones. The CSP may modify the format as necessary to comply with its internal policies and Federal Risk and Authorization Management Program (FedRAMP) requirements. Italicized text or comments should be replaced with appropriate CSP/Customer/System information.

Conventions used in this document

This document uses the following typographical conventions:

*Italic*

Italics are used for email addresses, and formal document names.

*Italic blue in a box*

Italic blue text in a blue box indicates instructions to the individual filling out the template.

*Instruction: This is an instruction to the individual filling out of the template.*

**Bold**

Bold text indicates a parameter or an additional requirement.

Constant width

Constant width text is used for text that is representative of characters that would show up on a computer screen.

<Brackets>

Text in brackets indicates a generic default name or word that should be replaced with a specific name. Once the text has been replaced, the brackets should be removed.

Notes

Notes are found between parallel lines and include additional information that may be helpful to the users of this template.

**Note:** This is a note.

Sans Serif

Sans Serif text is used for tables, table captions, figure captions, and table of contents.

Sans Serif Gray

Sans Serif gray text is used for examples.

How to contact us

If you have questions about something in this document, or how to fill it out, please write to:

*info@fedramp.gov*

For more information about the FedRAMP project, please see the website at:

<http://www.fedramp.gov>

1. INTRODUCTION

The plan of action and milestones (POA&M) is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system.

POA&Ms are used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment.

* 1. Purpose

The purpose of POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with Cloud Service Providers (CSP’s) priorities. POA&Ms are based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

POA&Ms are based on: (i) the security categorization of the cloud information system; (ii) the specific weaknesses or deficiencies in deployed security controls; (iii) the importance of the identified security control weaknesses or deficiencies; and (iv) CSP’s proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources).

The POA&M identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) any milestones in meeting the tasks; and (iii) the scheduled completion dates for the milestones.

* 1. Scope

The scope of the POA&M includes all management, operational, and technical FedRAMP security controls that are deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the control implementation). CSPs are required to submit updated POA&Ms to the FedRAMP PMO in accordance with the *FedRAMP Continuous Monitoring Strategy Guide.*

* 1. System Description

The ***<***Information System Name or Acronym***>***system has been determined to have a security categorization of <Moderate, or Low>.

*Instruction: Insert a brief high-level description of the system, business or purpose and system environment. Ensure this section is continuously updated with the latest description from the System Security Plan (SSP).*

1. Methodology

POA&Ms must include all known security weaknesses within the cloud information system. Weakness information is gathered and reported using the embedded FedRAMP POA&M workbook, which is comprised of five worksheets including the System POA&M worksheet, and four Quarterly POA&M Update worksheets, one for each quarter of the fiscal year.

### Worksheet 1: System POA&M

The System POA&M worksheet consists of two sections. The top portion of the POA&M provides basic system information as defined in the following table:

The top portion of the POA&M tracks the measures in the table below.

|  |  |
| --- | --- |
| **Measure** | **Details** |
| **FIPS 199 Risk 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. |
| **< Contractor or Federal CSP> <Information System Name>** | Systems are identified as either **Federal or Contractor.**    Contractor systems are identified as any system that processes or handles government--owned information on behalf of the government that are housed at non-government facilities including contractor, consultant, or other third party sites.  Federal systems are identified as any system that processes or handles government--owned information on behalf of the government that are housed at government facilities. |

The bottom portion of the POA&M worksheet is the corrective action plan used to track IT security weaknesses. This portion of the POA&M worksheet is based on OMBs format requirements.

**Column A – POAM ID**. – A unique identifier must be assigned to each POA&M item.

**Column B -- Weakness Description.** Describe weaknesses identified during the assessment process. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking, demonstrate awareness of the weakness, and facilitate the creation of specific milestones to address the weakness. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity.

**Column C – Platform.** List the IP Platform(s) the weaknesses were found on and/or other applicable information.

**Column D – Point of Contact (POC).** Identify the person/role that FedRAMP can hold responsible for resolving the weakness. A POC must be identified and documented for each weakness reported.

**Column E -- Scheduled Completion Date.** A completion date must be assigned to every weakness, to include the month, day, and year.   If a weakness is resolved before or after the originally scheduled completion date, enter the actual completion date in Column J, *Status*. Also, if the time to correct the weakness extends beyond the original scheduled date of completion, the reasons for the delay must be noted in Column H, *Milestone Changes,* together with a revised scheduled date of completion. The *Scheduled Completion Date* column must not change once it is recorded. .

**Column F – Scheduled Completion Date Changes.** If there are changes to scheduled completion date(s) that are based on extension requests that have been accepted by FedRAMP, note them in this column.

**Column G – Milestones (e.g., remediation actions) with Completion Dates.** A milestone will identify specific requirements to correct an identified weakness. Each weakness must have a milestone documented that identifies specific actions to correct the weakness with an associated completion date.  *Milestones with Completion Dates* entries shall not change once they are recorded.

**Column H – Milestones Changes.** List any changes to existing milestones in Column G, *Milestones with Completion Dates*in this column***.***

**Column I – Source of Discovery.** Identify sources for all weaknesses. Ensure this is consistent with the SAR and/or any continuous monitoring activities (e.g., Security Assessment Report, xx/xx/xx, XQXX Quarterly Scans).

**Column J -- Status.** A status of *Completed or Ongoing* must be assigned to each weakness.

* *Completed* — This status is assigned when all corrective actions have been applied to a weakness such that the weakness is successfully mitigated.  The *Date of Completion* shall be recorded for a completed weakness.
* *Ongoing* — This status is assigned to all current weaknesses that have not been completed, regardless of source of discovery.

**Column K - 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 L –** **Adjusted Risk Rating.** Provide the adjusted risk rating as approved by FedRAMP.

**Column M –** **Rationale.** Provide the rationale for the adjusted risk rating.

**Column N –** **Comments.**  Provide additional comments as may be required

### 

### Worksheets 2 - 4: FYXXQX POA&M Update

Currently, POA&Ms are updated on a quarterly basis. Each POA&M update worksheet requires the following information:

* Column A
  + Row 6 - Explanation for Delayed Weaknesses: (Provide brief explanation of why weaknesses were delayed). List each delayed weakness by the Unique Identifier from Worksheet 1 and the reason for the delay.
  + Row 7 - Description of New Weaknesses: (Provide brief explanation for source of new weaknesses). List each new weakness by the Unique Identifier from Worksheet 1 and the source of the new weakness. If the source of the identification of the weakness is the same for several weaknesses, they can be grouped with a single explanation.
* Column B
  + Row 3 List of Actions 90 to 120 days overdue
  + Row 4 - Total # of actions delayed:
* Column C
  + Row 3 List of Actions Over 120 days overdue
  + Row 4 - Total # of actions delayed:

### General Requirements

Plan of Action & Milestone (POA&M) must comply with the following:

* Use the POA&M template embedded in this document to track and manage POA&Ms.
* If a finding in the Security Assessment Report (SAR) exists, the finding must be represented 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 clearly identified in the SAR (Appendices C, D, and E), along with supporting evidence (e.g., clean scan report) do not have to be identified 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

### Embedded POA&M Spreadsheet (Click to open):



APPENDIX A.   ACRONYMS

 [NOTE: Update the acronym list based on the acronyms used in this document]

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AC | Authentication Category |
| AP  API | Assurance Profile  Application Programming Interface |
| ATO | Authorization to Operate |
| C&A | Certification & Accreditation |
| COTS | Commercial Off the Shelf |
| AO  FedRAMP | Authorizing Official  Federal Risk and Authorization Management Program |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| GSS  IaaS | General Support System  Infrastructure as a Service (Model) |
| IATO | Interim Authorization to Operate |
| ID | Identification |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| RA  Rev. | Risk Assessment  Revision |
| SA | Security Assessment |
| SAR | Security Assessment Report |
| SDLC | System Development Life Cycle |
| SP | Special Publication |
| SSP  VLAN | System Security Plan  Virtual Local Area Network |

APPENDIX B.   REFERENCES

[NOTE: Update references as needed to reflect current guidance]

Laws and Regulations:

* Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
* Consolidated Appropriations Act of 2005, Section 522.
* USA PATRIOT Act (P.L. 107-56), October 2001.

OMB Circulars:

* OMB Circular A-130, Management of Federal Information Resources, November 2000.
* OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
* OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS Publications:

* FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
* FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
* FIPS PUB 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST Publications:

* NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
* NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
* NIST 800-30, Risk Management Guide for Information Technology Systems
* NIST 800-34, Contingency Planning Guide for Information Technology Systems
* NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
* NIST 800-47, Security Guide for Interconnecting Information Technology Systems
* NIST 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
* NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
* NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
* NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
* NIST 800-64, Security Considerations in the Information System Development Life Cycle