POA&M - Plan of Action and Milestones

The process to mitigate risks and weaknesses is called a Plan of Action and Milestones (POA&M). A POA&M is created whenever audits reveal an area of weakness in security controls. This is an opportunity to strengthen or "harden" your system through carefully planned improvements.

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.

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 up

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.

What is the POA&M process

1. Receive audit reports
2. Find opportunities to improve security
3. Analyze risks and options
4. Develop a corrective action plan
5. Put the plan into action
6. Report on progress
7. Confirm POA&M completion
8. POA&Ms and continuous monitoring

Components of Plan of Action and Milestones

A POA&M typically includes a set of action items with specific deadlines, responsible individuals, and milestones to track progress toward achieving a specific outcome. The key components of a POA&M are the

- Objectives:
  - A POA&M's objectives are the outcomes an organization aims to achieve within a specific time frame
  - The objectives should be specific, measurable, achievable, relevant, and time-bound.
- Goals
  - Goals provide direction for the objectives and guide the decision-making process toward the overall outcome.
- Tasks
  - POA&M tasks are specific activities that are necessary for achieving the goals and objectives. The tasks should be identified according to their priority, and the timelines for each should be established.
- Milestones
  - POA&M milestones are essential components of POA&Ms, as they provide the means for measuring progress toward achieving the overall objective.
- Metrics
- Resources
- items

- These are a list of tasks and milestones that need to be completed in order to achieve a specific goal or objective. These action items can include activities like completing a training program, implementing new software, or resolving security vulnerabilities. POA&M items are used in project management to ensure that all necessary tasks are identified, assigned, and tracked to ensure progress toward the project goal. A list of POA&M items include:

POA&M Identifier	A unique identifier assigned to each POA&M item for tracking purposes
Name of the Control	The specific control or action that needs to be implemented to address the weakness or deficiency
Name of the Weakness/Deficiency	A concise description of the weakness or deficiency that needs to be addressed
Weakness/Deficiency Description	A more detailed explanation of the weakness or deficiency, including its impact on the organization
How the Weakness Was Identified	A brief description of the process or method used to identify the weakness or deficiency
Asset Identifier	The identifier of the asset or system that the weakness or deficiency pertains to
Date of Identification	The date that the weakness or deficiency was first identified
Resources Required to Address the Issue	An estimate of the resources (time, money, personnel, etc.) needed to address the weakness or deficiency
Planned Milestones	Specific milestones or targets for addressing the weakness or deficiency
Planned Resolution Date	The date by which the weakness or deficiency is planned to be fully addressed
Milestone Changes	Any changes to the planned milestones or targets
Vendor Dependencies	Any dependencies on vendors or third-party providers that may impact the resolution of the weakness or deficiency
Risk Rating	A quantitative assessment of the level of risk posed by the weakness or deficiency
Adjusted Risk Rating	Any adjustments made to the risk rating based on new information or changed circumstances
Operational Requirement Assessment	An assessment of whether addressing the weakness or deficiency is necessary to meet the organization's operational requirements
Supporting Documents	Any documents or evidence that support the identification or resolution of the weakness or deficiency

How to Measure the Success of Plan of Action and Milestones

One of the best ways to measure the success of a POA&M is to analyze the results achieved against the key performance indicators (KPIs) set. Organizations should collect data and evaluate progress frequently. Analyzing data against the set KPIs can provide insights into the effectiveness of the plan and highlight areas that require improvements. Organizations should also listen to feedback from employees, customers, and other stakeholders to evaluate the effectiveness of the POA&M.

KPIs Used in Measuring the Success of POA&Ms

KPIs are critical in measuring the success of the POA&M. Some of the most commonly used KPIs include financial metrics such as ROI, operational metrics such as cycle time and quality, customer satisfaction metrics, and employee satisfaction metrics. KPIs should be specific, measurable, achievable, relevant, and time-bound (SMART).

Common Challenges in Developing Plan of Action and Milestones

Developing a POA&M can be challenging, especially if the organization lacks experience in strategic planning. Some common challenges include lack of clarity on objectives, poor communication with stakeholders, inadequate resources, and resistance to change. Additionally, a POA&M can be challenging to develop in a rapidly changing environment where priorities shift quickly.