CyberTek™ - Plan of Action and Milestones (POA&M) Management

Create POA&M

Document Weakness
Identify source of weakness
Assign POC
Determine Severity

Prioritize POA&Ms

Risk Analysis of weaknesses and their impacts on the Confidentiality, Integrity, Availability, Privacy, etc.

Create Corrective Action Plan (CAP)

Identify corrective action options and perform a cost benefit analysis to select the most appropriate corrective action based on the risk

Create a CAP Schedule

Identify Resources Required
Identify Milestones
Set a completion date based on resource availability

Implement CAP

Execute and Monitor the corrective actions identified in the CAP according to the plan

Validate that POA&M is resolved

Test the implemented corrective action and verify that the weakness has been fully resolved

Retire POA&M

Mark POA&M as "Completed" upon validation.
Note completion date.

Quarterly POA&M Status Report

A quarterly report must contain at a minimum the following *five* metrics:

1) The total number of weaknesses identified on the original POA&Ms
2) The number of weaknesses for which corrective action was completed on time (including testing)
3) The number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled
4) The number of weaknesses for which corrective action has been delayed including a brief explanation for the delay
5) The number of new weaknesses discovered following the last POA&M or status update and a brief description of how they were identified.