

Office of Information Security Cyber Security Policy & Compliance

Plan of Action and Milestone (POA&M) Standard Operating Procedure



**April 12, 2017
Version 2.1**

[illegible]

This page intentionally left blank

Table of Contents

REVISION HISTORY	I
1 INTRODUCTION.....	1
2 PURPOSE.....	1
2.1 GRC Tool	2
2.2 Terminology	2
2.3 Useful Tips	4
3 POA&M COMPONENTS.....	5
4 POA&M PROCESS.....	8
4.1 Process Step 1: Document the POA&M	9
4.2 Process Step 2: Review and Approve the POA&M.....	19
4.3 Process Step 3: Update and Monitor the POA&M.....	21
4.4 Process Step 4: Close POA&M.....	24
5 POA&M REPORTS.....	31
6 CONCLUSION	32
 Table 1. Guidance for Finding Components	5
Table 2. Guidance for Response Components.....	7
Table 3. Criteria for Approval.....	20
Table 4. Examples of Control Evidence.....	27
 Figure 1: Open Finding Workflow Screen	3
Figure 2. Create Finding from Control	10
Figure 3. Assessment Details General Tab	10
Figure 4. Creating a New Finding through the Findings Tab Screen	10
Figure 5: Create Finding Screen.....	11
Figure 6. Completed Finding Example.....	11
Figure 7. Accept (or Reject) Finding Screen	12
Figure 8. Accept Finding Comments Box	12
Figure 9. Workflow Stage 2 Respond	13
Figure 10. Navigating to New Response Screen	14
Figure 11. Assessment Details Findings Tab.....	14

Figure 12. Adding a Response	15
Figure 13. Add New Response Screen.....	15
Figure 14. Add New Response Additional Screens	15
Figure 15. Response Tab Screen.....	16
Figure 16. Edit Finding to include Financials Screen	16
Figure 17. Editing Financial Information Screen	17
Figure 18. Non-Funding Obstacles.....	17
Figure 19. Progress Finding/Response to Review Screen.....	18
Figure 20. Workflow Stage 3-Review.....	18
Figure 21. Review Finding/Response Screen.....	19
Figure 22. Approve/Reject /Response Screen.....	20
Figure 23. Workflow Stage 4-Pending	21
Figure 24. Example of New Response as a result of a Change in Plans	23
Figure 25. Quarterly Review Response Example	23
Figure 26. Submit Workflow for ISO Review and Approval Screen.....	23
Figure 27. Review Workflow Screen.....	24
Figure 28. Close Response	26
Figure 29. Response Tab Screen with All Completed Responses.....	26
Figure 30. Add Document Screen	28
Figure 31. Finding/Attachments Tab Screen with Closure Evidence	29
Figure 32. Submitting for Close Screen	29
Figure 33. Navigate to the Close Response	30
Figure 34. Accept and Close POA&M.....	30
Figure 35. Comments Box for Approving/Rejecting Screen	30
Figure 36. Workflow Stage 6-Closed	31

1 INTRODUCTION

On October 17, 2001 the Office of Management and Budget (OMB) issued Memoranda 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, outlining the minimum mandatory guidance and detail to be included in a Plan of Action and Milestones (POA&M). According to 38 U.S.C. § 5727, POA&Ms are defined as “A plan used as a basis for the quarterly reporting requirements of OMB that includes the following information: (i) A description of the security weakness; (ii) the identity of the office or organization responsible for resolving the weakness; (iii) an estimate of resources required to resolve the weakness by fiscal year; (iv) the scheduled completion date; (v) key milestones with estimated completion dates; (vi) any changes to the original key milestone date; (vii) the source that identified the weakness; (viii) the status of efforts to correct the weakness.”

The purpose of the POA&M is to assist the Department of Veterans Affairs (VA) in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. It is a tool that identifies weaknesses and delineates the tasks necessary to mitigate them; to include tasks that need to be accomplished, resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. Though the POA&M is expected to be a comprehensive plan, OMB assumes additional, more detailed project management plans exist for each corrective action item identified in the POA&M, and that the original source documents (e.g., Inspector General (IG) audit reports, risk assessments), in which weaknesses were first identified, are readily available. Thus, each POA&M weakness should be clearly traceable to its original source(s) and the documentation supporting the corrective actions should be maintained in the system security profile.

A standardized POA&M process will ensure VA's POA&Ms are managed appropriately and that remedial information security actions to mitigate risk to VA operations, assets, individuals, other organizations and the Nation are documented correctly. By reflecting the Enterprise security needs of an agency, a consolidated POA&M provides a roadmap for continuous agency security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool for agency officials, Inspectors General, and OMB.

Prior to the release of the “Revocation of All Risk-Based Decision Memo Processes”, Risk Based Decisions (RBD) were allowed to be used. It has always been the process to create a POA&M in conjunction with the RBD. After the release of the memo, new RBD memos will no longer be signed.

2 PURPOSE

This POA&M Management Guide provides the necessary information and step-by-step instruction for developing, maintaining, reporting and monitoring weaknesses as it relates to a specific system. Subsequently, it will provide instructions on the use of the Governance, Risk and Compliance (GRC) RiskVision tool to support the POA&M process.

The intended audience of this guide includes VA personnel responsible for the security of VA information systems and the management of the associated POA&Ms. VA Handbooks 6500, *Risk Management Framework for VA Information Systems – Tier 3*:

VA Information Security Program, and 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems*, document roles and responsibilities associated with these functions. It is specifically designed to assist Information Security Officers (ISOs) and System Stewards who enter and approve POA&Ms in RiskVision. This Standard Operating Procedure includes general guidance, specific instructions, and where applicable, examples to accomplish each procedure step. It also includes specific instructions for how to accomplish the procedure steps while navigating through RiskVision. Screen shots are included for ease of use.

This document was designed to align with the following documents:

- VA Handbook 6500
- VA Handbook 6500.3
- Accreditation Requirements Guide, Standard Operating Procedures October 2016
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- GRC training and documentation located on the Office of Information Security (OIS) Portal in the GRC Training and Brown Bag Materials section.

2.1 GRC Tool

VA uses a centralized and automated process through the use of a GRC tool called RiskVision. RiskVision supports the process to assess, authorize, and monitor the security posture of the Department's information technology (IT) systems, as well as provide reporting capabilities. RiskVision is the tool enabling VA to implement a continuous monitoring program where security issues will be addressed on an ongoing basis throughout the life cycle of a system.

2.2 Terminology

Plan of Action and Milestones (POA&M) is a tool that identifies weaknesses and delineates the tasks necessary to mitigate them; to include tasks that need to be accomplished, details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

In RiskVision a POA&M is tracked via Findings (weakness) and Responses (milestones which document the corrective action plan or remediation activities). Together they form the POA&M.

Findings are security weaknesses or vulnerabilities identified from audits (internal or external) or security control assessments. Findings are typically related to financial resources that are not available to allow for scan vulnerabilities or controls to be fully implemented.

Responses are a RiskVision term used to represent the milestone. These are created to document the plan to show the initial plan and the progress towards remediating the Finding. Over time, there can be multiple Responses for a single Finding.

Weakness refers to any program or system level information security vulnerability that poses a risk to the confidentiality, integrity, or availability of VA information system. Weaknesses represent the gaps between the current program or system status and the long-term program or system security objectives.

Remediation Activities are the corrective action activities or mitigation activities and associated milestones to correct the weakness. This document primarily uses this term. These are documented in the Response; specifically the Milestones with Completion Date field.

RiskVision Role determines which functions are performed by whom and at which Workflow Stage.

Traditional System Owner responsibilities are assigned the “System Steward” role in RiskVision. The System Steward is responsible for documenting the Finding and Response, documenting financials, transition of the Finding Workflow and upload closure evidence to both the POAM and the control. Traditional ISO responsibilities are assigned the “ISO” role in RiskVision. The ISO is responsible for reviewing, approving and validating the documentation in the Finding and Response, closure evidence, financials and transitioning the Finding Workflow.

Workflow is a function within RiskVision to perform a defined sequence of tasks assigned to specific roles. The Workflow Stage reflects which task the Workflow is in. The Workflow Stages must be progressed throughout the process to complete all tasks.

Finding Workflow is the function within RiskVision used to manage the POA&M process. Progression of the Workflow Stages changes the status of a Finding from open, review, pending or closed and defines the steps stakeholders perform at each Stage. Defined tasks must be completed within each Stage by certain roles. It is necessary to navigate to the Workflow tab of the Finding to progress the Workflow.



Figure 1: Open Finding Workflow Screen

- Stage 1: Open – The Finding is created. The Finding must be accepted by the ISO in order to move the workflow to Stage 2: Respond
- Stage 2: Respond – The System Steward creates the milestone (Response) and must submit it for ISO review
- Stage 3: Review – the ISO must review the response and choose an option in RiskVision to progress the workflow
- Stage 4: Pending – This is the stage the POA&M should be in as remediation actions occur. The System Steward can create additional responses while in this stage
- Stage 5: Close – The ISO closes the POA&M

POA&M Status reflects the status of the Finding and associated Responses:

- Open: weakness continues to be remediated consistent with the associated scheduled completion date
- Overdue: the original and/or updated scheduled date of completion has been surpassed
- Closed: the weakness has been fully resolved and the closure evidence has been tested

2.3 Useful Tips

Below are some useful tips and reminders to assist System Stewards and ISOs in their POA&M activities:

- All controls identified as either “Planned” or “In-place and Planned” must have a Finding and Response created describing what the deficiency is (Finding) and how and when it is planned to be remediated (Response).
- Multiple Findings can be tied to a single control. However, in RiskVision only one Finding can be created at the control in Compliance Manager. If additional Findings need to be created this must be done in the Finding tab. Refer to [Procedure Step 1.1.1](#).
- When completing the New Finding or New Response Screens, fields marked with an asterisk (*) are mandatory fields in RiskVision that must be completed in order to leave the screen; however, all fields in [Table 1. Guidance for Finding Components \(New Finding Screen in RiskVision\)](#) and [Table 2. Guidance for Response Components \(New Response Screen in RiskVision\)](#) are required to be completed in order to have a properly documented POA&M. These tables provide instructions for how to document, and criteria to review/approve the fields.
- The requirement is that Findings and the initial Response is created within 15 days of the weakness being identified. Responses to SCA audit findings must have an initial response created within 15 days of the finding being entered.
- RiskVision does not provide automatic notifications outside the tool. There are notifications on the home page. However, it is good practice for the System Steward and ISO to collaborate and inform one another when a workflow is passed to them, so timely action can be taken.
- As workflows are progressed through the stages, provide specific comments for any rejection action so it can be corrected and returned to the appropriate workflow stage.
- Once a Finding is closed, remember to return to the Compliance Manager (CM) to mark the control “In Place”; update the control implementation details and upload evidence to show the control is fully tested and in place.
- An effective practice is for the System Steward and ISO to work collaboratively to document the Finding and Response prior to populating RiskVision. This minimizes issues that may arise during review and approval.
- Once created in RiskVision certain fields in the Finding cannot be changed or edited, caution should be taken to document correctly.
- Although RiskVision allows edits to the Response, VA direction is to create a new Response to document changes to milestones.
- POA&M closure evidence should be attached to the Attachments tab of the Finding

and at the control not within the Response tab.

- The workflow tab of the Finding identifies which workflow stage the finding is currently in. It also shows the history of the Finding as it progressed through the stages. This is helpful information; therefore a review of the history can be valuable.
- Workflow stage 5: Closed Pending Control (3-2) Update should not be used.
- The Force Transition button in RiskVision should not be used.
- Any deficiency identified within an accreditation boundary must have a POA&M created. This includes use of medical devices where they cannot meet security controls.

3 POA&M COMPONENTS

The two POA&M components in RiskVision are the Finding and the Response. [Table 1. Guidance for Finding Components](#) identifies the fields that must be properly documented in the New Finding screen in RiskVision. All fields in [Table 1](#) must be completed. Additionally, it includes more detailed guidance and/or examples that should be followed when creating and approving the Finding. [Table 2. Guidance for Response Components](#) identifies the fields that must be properly documented in the New Response screen in RiskVision.

Table 1. Guidance for Finding Components
(New Finding Screen in RiskVision)

New Finding in RiskVision	
(NOTE: The fields not listed in this table are not used at this time and should not be populated)	
Field	Purpose/Guidance/Instruction/Example
Name/Title (*) <i>This is a text field in RiskVision</i>	<p>Ensure the name of the Finding includes the control number and name. If more than one Finding exists for the same control, include more description or enhancement number since titles cannot be duplicated. Examples include:</p> <ul style="list-style-type: none"> • AC-2 Account Management • AC-2 Account Management – No Account Termination Process <p>If the Finding is a result of an audit, include the type of audit, date of audit and control number</p> <ul style="list-style-type: none"> • FY2015 FISMA SI-2.1.2
Type of Weakness <i>This is a text field in RiskVision</i>	<p>The type of weakness helps categorize and is used to identify where the weakness originated. If the source of the Finding was identified from an audit, include information detailing the type and date of the audit. Examples include:</p> <ul style="list-style-type: none"> • Self-Assessment • FY 2015 Deloitte site readiness • FY 2015 BAH site readiness • FY 2015 ERM SCA Audit • FY 2015 FISMA IG Audit • Medical Device
Resources Required <i>This is a drop down field with the following options: "None", "Minimal", "Moderate", or "High"</i>	<p>The cost of weakness remediation activities must be determined and included in POA&Ms. To ensure security is integrated into IT investments, OMB requires tying POA&Ms to the capital planning and budget process.</p> <p>When populating this field in the Finding Screen, choose the best of the 3 options, Because some level of resources will always be required, "None" should not be chosen.</p>
Financials <i>Finding must be edited to access the associated fields</i>	<p>When updating the Finding a more detailed estimate of resources, in man-hours or funds must be established. Refer to Procedure Step 1.3.2 Edit Finding to Include Financial Information. Also refer to Financial entry for Findings Training_ June 2014.ppt for specific instructions on how to complete this in RiskVision.</p>

New Finding in RiskVision	
(NOTE: The fields not listed in this table are not used at this time and should not be populated)	
Field	Purpose/Guidance/Instruction/Example
	<p>The resource estimate should be a realistic estimate in man-hours or funds, based on total resources required to complete all milestones associated with weakness remediation.</p> <p>As part of POA&M closure update (Procedure Step 4.2 Approve POA&M Closure), to reflect the actual man-hours or funds expended should be documented in the closed response.</p>
<p>Identified in CFO Audit or other review</p> <p>This is a drop down field with the following options: "Yes", "No"</p>	<p>If the Finding was identified as a result of an IG FISCAM Audit, chose "Yes". If the Finding was identified as a result of an IG FISMA Audit, SCA, ERM security control audit or other readiness audit chose "No". NOTE: RiskVision does not allow this field to be changed once populated and saved even if the Finding is rejected by the ISO for corrections</p>
<p>Scheduled Completion Date</p> <p>This is a calendar pop-up field</p>	<p>Estimate the completion date to resolve the weakness This is a best guess based on a realistic estimate of time to organize resources, develop a solution, implement remediation tasks, and test that weakness is fully remediated. The Scheduled Completion Date (SCD) cannot be changed and is what determines the status of a POA&M for tracking and monitoring. If remediation takes longer than the Scheduled Completion Date it is in overdue status. The scheduled completion date should never be a date prior to the date the POA&M is created.</p> <p>For remediation's that are known and resources are available, the timeline to be used as guidance is as follows:</p> <p>NIST 800-53 Priority 1 – 60 days</p> <p>NIST 800-53 Priority 2 – 90 days</p> <p>NIST 800-53 Priority 3 – 120 days</p> <p>Medical Device POA&Ms – expected end of life of device</p> <p>If the control deficiency has an unknown remediation the Scheduled Completion Date must be reasonable and achievable.</p> <p>NOTE: The tool does not allow this field to be changed once populated and saved even if the Finding is rejected by the ISO for corrections</p>
<p>Description - why control is not fully met or what is the identified weakness.</p> <p>Include:</p> <ol style="list-style-type: none"> The <i>criteria</i> for the failed control requirement. The <i>condition</i> for the failed control requirement. The <i>cause</i> for the failed control requirement. 	<p>The description for the Finding should be detailed enough clearly articulate the weakness and enable appropriate oversight and tracking. Do not restate the Finding Name, be more descriptive.</p> <p>**Provide a summary of the overall deficiency that was derived from the A&A, annual assessment or audit. Identify the VA Handbook 6500 requirement(s) or security control from VA Handbook 6500 that cannot be met. Clearly describe the security issue or problem to be addressed by the POA&M. Describe the business impact of this deficiency. Describe the technical reasons why the requirement cannot be met and the risk and impact.</p>
	<p>Document which portion of the applicable control Assessment Procedure was not met.</p> <p>Example: Failure of AC-2.1 Criteria: Examination of access control policies determined that the organization does not require appropriate approvals for requests to establish accounts, as required in AC-2 baseline requirement in VA Handbook 6500.</p>
	<p>Document the observed situation, as it existed at the time of the weakness was identified.</p> <p>Example: Failure of AC-2.1 Condition: Users are currently granted Admin-level access to the application with only Network-Admin review and authority. No management personnel approve access requests</p>
	<p>Document the probable reason for this condition existing.</p> <p>Example: Failure of AC-2.1 Cause: The application Business Owner has not developed a documented process for requesting and approving access to various defined user groups.</p>

Owner/Individual (*)	<i>This field will default to the person creating the Finding. Provide the name of the person who is best able to address questions pertaining to weakness remediation and who can address progress made. Click the + sign next to the Owner field that allows a user to specify the user role and make additional comments. The person chosen must have an</i>
----------------------	---

New Finding in RiskVision	
(NOTE: The fields not listed in this table are not used at this time and should not be populated)	
Field	Purpose/Guidance/Instruction/Example
	account in RiskVision. <u>Do not choose a team</u> as those are not used currently in RiskVision.
Impact (*) This is a drop down field with the following options: "High", "Medium", "Low"	Should be appropriate to the risk level for the system for the Finding. Apply the following definitions:
	[High]: Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
	[Medium]: Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
	[Low]: Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.
Likelihood (*) This is a drop down field with the following options: "Certain", "Almost Certain", "Likely", "Possible", "Unlikely"	Use best judgement to determine the likelihood that this weakness will occur. Apply the following definitions from NIST SP 800-30 Table G-3, page G-2:
	[Certain]: Error, accident, or act of nature is almost certain to occur (96%-100%) ; or occurs more than 100 times a year
	[Almost Certain]: Error, accident, or act of nature is highly likely to occur (80%-95%) ; or occurs between 10-100 times a year
	[Likely]: 21-79 5 Error, accident, or act of nature is somewhat likely to occur (21%-79%) ; or occurs between 1-10 times a year
	[Possible]: 5-20 2 Error, accident, or act of nature is unlikely to occur (5%-20%) ; or occurs less than once a year, but more than once every 10 years
	[Unlikely]: Error, accident, or act of nature is highly unlikely to occur (0%-4%) ; or occurs less than once every 10 years.

Table 2. Guidance for Response Components
(New Response Screen in RiskVision)

New Response in RiskVision	
(NOTE: The fields not listed in this table are not used at this time and should not be populated nor should default information be changed.)	
Field	Guidance/Example
Title (*) This title is used to track weaknesses from quarter to quarter.	Use the naming scheme below to easily identify subsequent Responses [Enter Response sequence]
	Example: AC-2 Account Management Initial response
	Example: AC-2 Account Management Second response
	Example: AC-2 Account Management FY15 Q3 Quarterly Review
	Example: AC-2 Account Management Close response
Milestone w/Completion Dates	Document the specific activities needed to fully mitigate the weakness. If several tasks are identified include all tasks with an anticipated completion date for each. The milestone should address the objective the milestone will achieve as well as the criteria for determining when the milestone will be completed.

New Response in RiskVision	
(NOTE: The fields not listed in this table are not used at this time and should not be populated nor should default information be changed.)	
Field	Guidance/Example
	<p>The recommended action/remediation is [Include options with pros and cons for each option, if available. Include other pertinent information to assist in making a decision, such as, costs, etc. Justify why the POAM is being created instead of remediating the deficiency. Include cost analysis, as well as rejected requests for resources (financial, staff, etc).]</p> <p>For long term risk acceptance requires compensating controls that bring the risk down to an acceptable level. The compensating controls that will be put in place are [Identify and describe the controls from VA Handbook 6500 that will serve as compensating controls. Describe how implementing the compensating controls eliminate or reduce the risks associated with not implementing the baseline control. Describe how the compensating controls offer equivalent or comparable level of protection, or if not, describe the residual risk and the impact.]</p> <p>**A compensating control will not be necessary for a POAM that has a valid plan to be resolved.</p> <p>***Compensating controls will be provided at the point that due diligence has made it clear to request risk acceptance. At this time, the POAM will be closed and a "RISK" will be created in the ERM module of RiskVision. If you feel you have reached this point, email VARiskReviewWorkgroup@va.gov distribution group. This team will review the request and address the Risk as necessary. See mitigation status section below for additional process.</p>
	<p><i>Objective Example: Create user roles that properly identify each of the applications user roles and the necessary data access and restriction for each role. Estimated complete date is 12/15/2015</i></p> <p><i>Criteria Example: This milestone will have been reached when all of the functional requirements can be achieved within the identified and documented roles.</i></p> <p>Over time, if there are additional milestones, they must be documented by creating a New Response.</p>
Response Action	<p>Accept: Default</p> <p><i>Mitigate: Do not use</i></p> <p><i>Transfer: Do not use</i></p>
Start Date	Enter the date that this Response is created. This field serves as a time stamp to record all milestones associated with a Finding. It is important to include the date.
End Date	Enter the date that the RESPONSE task is expected to be completed. Example if you have a water pipe above your server room and you need to enter a request for money to move it, the response start date is the date you request the money and the end date is the expected reply if the money is granted. If the response is to provide an updated SCD, the start date and end date can be the same.

Mitigation Status	<i>Approved: Do not use</i> <i>Cancelled: Do not use</i> <i>Implemented/Completed: Do not use</i> <i>Verified: Do not use</i> <i>In Place: Use this status when you feel the finding needs to be reviewed by the FSS/SDE review team for a RISK to be created</i> <i>Suggested: Default</i>
Changes to Milestones	Do not use this field. New or changed milestones are documented by creating a new Response.
Comments	Enter the reason for the Response. Example: FY15 Q4 POA&M Review

4 POA&M PROCESS

The POA&M process includes the procedure steps outlined in this section. The POA&M process is initiated when a weaknesses is identified. Weaknesses can be at the program, national, or system level as identified through OIG audit reports and risk assessments to include:

- Non-Compliant Controls: Identified in control assessments performed by System Steward – Findings are created by the System Steward
- Weaknesses identified by the ISO during review of control implementation status descriptions – Findings are created by the ISO
- Weaknesses identified by Enterprise Risk Management (ERM) during the Security Control Assessment (SCA) and provided in the Risk Assessment and Security Assessment Report (SAR) – Report is uploaded to RiskVision, and POAMs are created by the system steward.
- Weaknesses identified in Nessus Scans – One POA&M is created by System Steward each month as a reminder to work vulnerabilities. This finding can be closed when all identified vulnerabilities are remediated for that month.

4.1 Process Step 1: Document the POA&M

The following steps are performed to open and document the POA&M.

Procedure Step	Responsibility
1.1 Create Finding 1.1.1 Populate RiskVision New Finding Screen	System Steward/ISO
1.2 Accept Finding 1.2.1 Review Finding 1.2.2 Accept Finding	ISO
1.3 Create Response 1.3.1 Populate RiskVision New Response Screen 1.3.2 Edit Finding to Include Financial Information 1.3.3 Progress Workflow to the ISO at Stage 3: Review	System Steward

[Procedure Step 1.1 Create Finding](#)

Findings are created as a result of weaknesses identified within a system or program. The components for a Finding must be properly documented to ensure compliance and consistency in order for VA to manage POA&MS. VA guidance states that once the Finding is created in RiskVision, certain fields cannot be edited or updated; including, Name, Description, Scheduled Completion Date, and Identified in CFO Audit. Therefore it is important to properly document all fields in the RiskVision Finding Screen. [Table 1. Guidance for Finding Components](#) provides guidance and instruction for completing these fields. Both the System Steward and ISO can create a Finding in RiskVision. All controls that are identified as either “Planned” or “In-place and Planned” in the control assessment must have a Finding created. In RiskVision, only one Finding can be tagged to each control and the Finding name cannot be duplicated.

ISOs are required to review and approve security control implementation descriptions to include control test evidence required to prove that a control is in place. During this review ISOs identify those controls that are deficient in either description or evidence. ISOs perform this function when new systems are coming on line and after the annual reviews performed by System Stewards. The ISOs have the option to make comments and send the workflow back to the System Steward to make corrections, however if the System Steward cannot fully remediate (i.e. add appropriate evidence or accurately describe the implementation) once the workflow is sent back to the ISO, they have the option of changing the control to ‘planned’ and creating a finding.

[Procedure Step 1.1.1 Populate RiskVision New Finding Screen](#)

Using the guidance in [Table 1. Guidance for Finding Components](#) populate the RiskVision New Finding Screen.

[RiskVision Navigation](#)

A new Finding is created in the Compliance Manager (CM) workflow in either the Task 1-1, 1-2, 3-2 stage by the system steward or the Task 1-3, 4-2 stage by the ISO. This is done by using the Finding tab under each control. If a control already has a finding attached to it, a new Finding can be created in the Finding workflow.

Method to create a finding from the control within Compliance Manager:

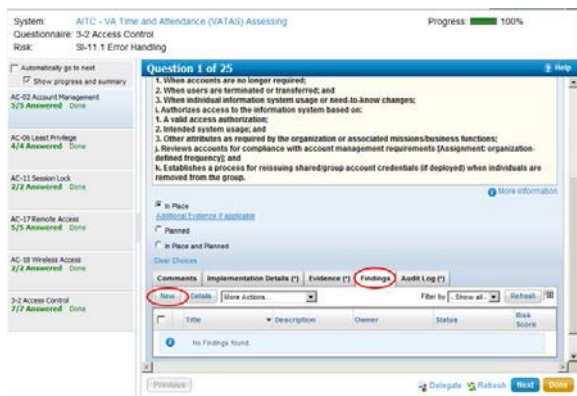


Figure 2. Create Finding from Control

From the Control Results tab of the Entity:

- 1 Click on the **Findings** Tab
2. Click the **New** button

Method to create a finding using the Finding Workflow (only to be used if a Finding for the specific control already exists).

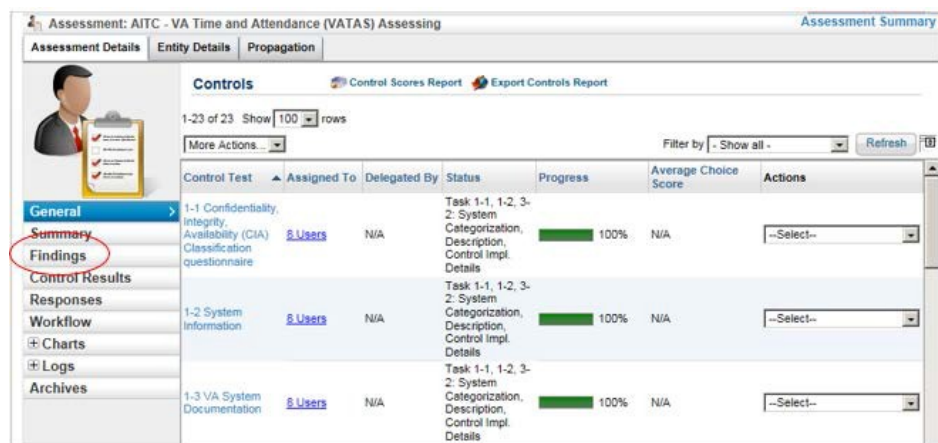


Figure 3. Assessment Details General Tab

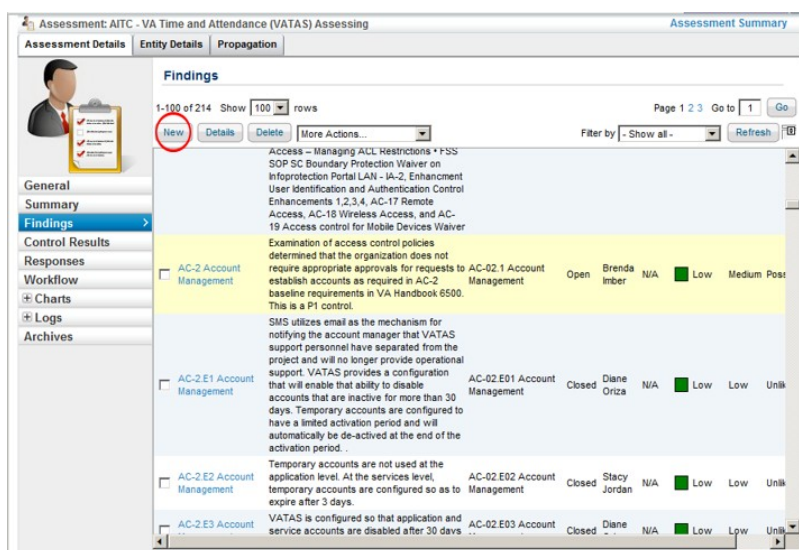


Figure 4. Creating a New Finding through the Findings Tab Screen

The screen to the left will appear. This workflow represents the Finding Workflow 1. Click the **New** button A new Finding Screen as shown below

Figure 5: Create Finding Screen

The Create Finding Screen will appear

1. Document all fields except Residual Impact and Residual Likelihood per the guidance and standards identified in [Table 1. Guidance for Finding Components \(New Finding Screen in RiskVision\)](#)
2. Click **OK**

Pay very special attention when completing Name, description, Identified in CFO Audit and scheduled completion date fields. Once the OK button is clicked this information can never be edited/changed. If the SS is unsure of this information it is best to discuss with the approving ISO before entering.

The finding now exists and will be listed in the findings for the entity. It is in the Open Workflow stage.

Figure 6. Completed Finding Example

This is an example of a Finding once OK has been clicked

[Procedure Step 1.2 Accept Finding](#)

The ISO role must review and accept (in RiskVision) the Finding (even if the ISO created it).

[Procedure Step 1.2.1 Review Finding](#)

The ISO reviews the information for all the Finding fields to ensure they are in agreement, and it meets the criteria as described in ([Table 1. Guidance for Finding Components](#)). Pay special attention that the Finding Name and type of weakness is correct, the description has adequate detail to describe the weakness, and the

resources required field is reasonable. Review and ensure the Scheduled Completion Date is realistic.

[Procedure Step 1.2.2 Accept or Reject Finding](#)

The ISO reviews the Finding and either accepts it which moves the Finding to Stage 2. Respond in RiskVision, or rejects and the Finding goes to the Close Workflow Stage. The System Steward must then create a new Finding and submit for review.

[RiskVision Navigation](#)

The Finding must be accepted in RiskVision in order for the workflow to be progressed to the next stage.

Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2015-08-28 10:35:42	Start Workflow	Open	No	Brenda S Imber	Neil Cruz, Louise Lovett-Robinson, Stacy Jordan, Alice M Hanigan, Leigh Taylor	Finding workflow started	

The ISO

1. Navigates to the Workflow tab
2. Clicks "Accept" if the Finding is documented properly. NOTE: Acknowledge the Finding was reviewed and is valid in the comments box. The Workflow will then move to Stage 2: Respond; OR
3. Clicks "Reject" if the Finding is not documented properly. NOTE: Include the specific reasons why the Finding was deficient.

Figure 7. Accept (or Reject) Finding Screen

Finding Approved. No changes anticipated

Alice M Hanigan

OK Cancel

Figure 8. Accept Finding Comments Box

If the Finding is rejected, the workflow stage goes to stage 5: Closed. If the intent is to create a new POAM to properly document a deficiency due to a POAM being closed for improper documenting; the process goes back to [Procedure Step 1.1 Create Finding](#). Refer to [Figure 4: Creating a New Finding through the Findings Tab Screen](#).

Findings: AC-2 Account Management

Name: Default Finding Workflow

1 Open 2 Respond 3 Review 4 Pending

5 Closed - Pending Control (3-2) Update 6 Closed

Since: 2015-08-28 10:51:14

Current Owner (s): Roy Coles, Sandra Hedtke, Diane Oriza, David Bekele, Brenda S Imber, David P. Henkel, Quincy Pence, Oluamide Oloyede (Details)

Stage Actions: 1 of 8 needed for moving workflow to "Review"
1 of 8 needed for moving workflow to "Open"

☐ Force Transition
To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

Submit for Review Reject

Workflow History

1-2 of 2

Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2015-08-28 10:51:14	Open	Accept	Respond	No	Alice M Hanigan	David Bekele, Diane Oriza, Quincy Pence, Roy Coles, David P. Henkel, Oluamide Oloyede, Sandra Hedtke, Brenda S Imber	Finding Approved. No changes anticipated.
2015-08-28 10:35:42		Start Workflow	Open	No	Brenda S Imber	Neil Cruz, Louise Lovett-Robinson, Stacy Jordan, Alice M Hanigan, Leigh Taylor	Finding workflow started

Once the Finding has been accepted by the ISO, it is in stage 2: Respond

Figure 9. Workflow Stage 2 Respond

Procedure Step 1.3 Create Response

The milestone portion of the POA&M should be created as soon as possible once the mitigation activities to correct the weakness described in the Finding have been identified. In RiskVision, this is achieved by creating a new response. Over time, additional new Responses are created to address a change in the remediation plan and for quarterly reviews. The Response in RiskVision delineates the tasks necessary to mitigate the weakness; to include tasks that need to be accomplished, any milestones in meeting the task, and scheduled completion dates for the milestones. The description in the Response will vary depending if it is the initial milestone, a milestone documenting a change, or closure.

The terms "milestone" and "response" are used interchangeably in RiskVision training slides. For purposes of this document, the term "Response" refers to *all* fields contained in the New Response Screen. VA guidance states that once the Response is created in RiskVision it cannot be edited or updated. Therefore, it is important to properly document all fields in the RiskVision New Response Screen. Table 2. Guidance for Response Components includes more detailed guidance and/or examples that should be followed when creating and approving the Response.

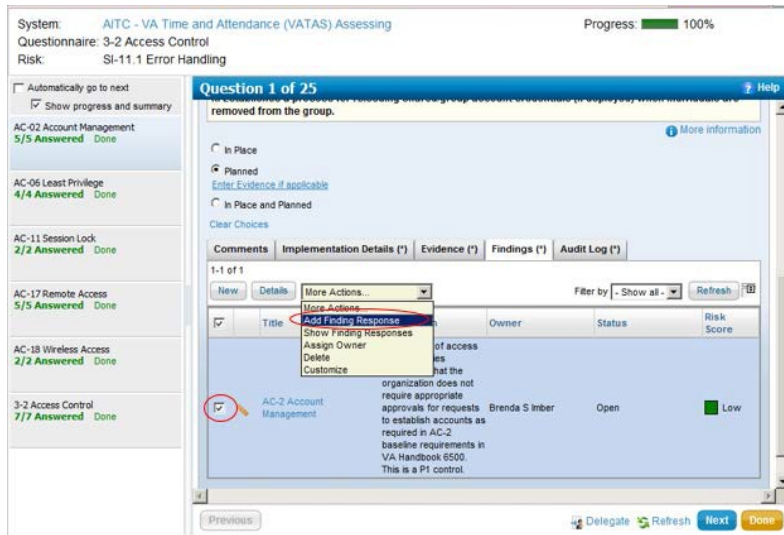
Procedure Step 1.3.1 Populate RiskVision New Response Screen

Using [Table 2.Guidance for Response Components](#) for reference, the System Steward creates the Response in RiskVision. Fields which are not included in [Table 2](#) should not be completed in RiskVision and defaults should not be changed. This procedure step can be, and often is completed prior to the ISO accepting the Finding in RiskVision ([Procedure Step 1.2.2](#)).

RiskVision Navigation

The Finding Workflow is either in Stage 1: Open (if the Finding has not been accepted by the ISO) or Stage 2: Respond if the Finding has been accepted. There are two ways to navigate to the new Response screen.

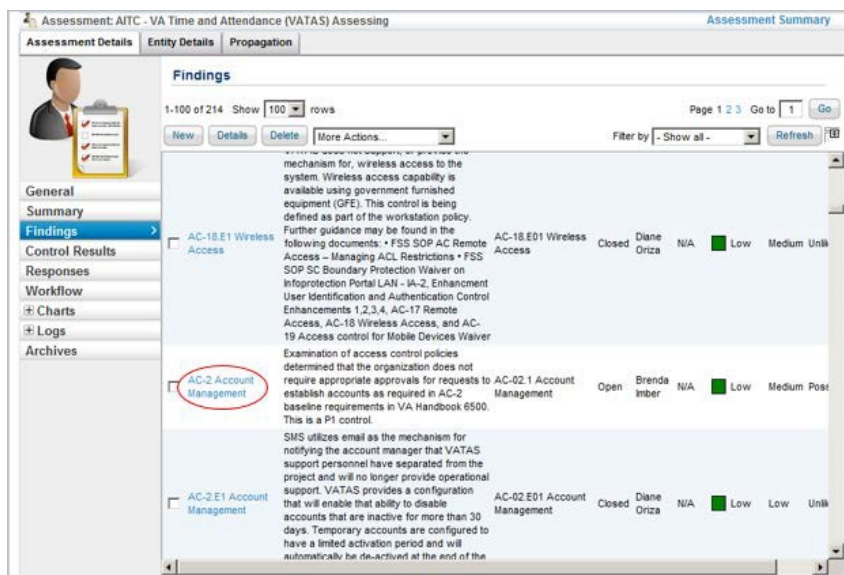
From the Control in Compliance Manager



1. Check the box next to the finding
2. Open the drop down box and choose "Add Finding Responses"

Figure 10. Navigating to New Response Screen

From the Finding Tab



1. Click on the Finding. (continue to next screen shot)

Figure 11. Assessment Details Findings Tab

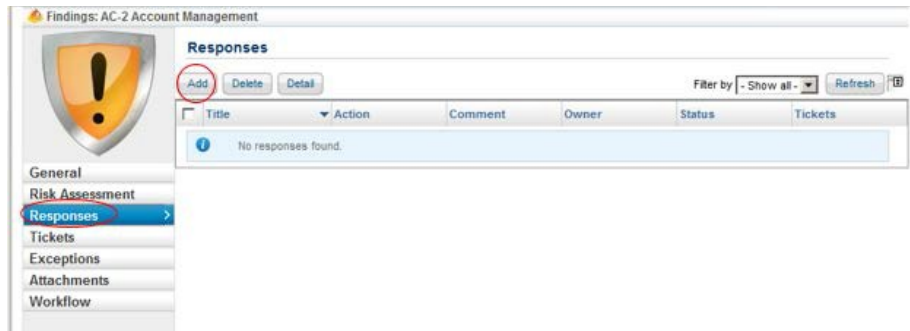


Figure 12. Adding a Response

Figure 13. Add New Response Screen

The New Response Screen appears.
1. Complete the fields in accordance with [Table 2. Guidance for Response Components](#). No need to complete fields which are not identified in [Table 2](#).
2. Click **OK**

Figure 14. Add New Response Additional Screens

These 2 screens will appear. There is no need to reference tickets or add attachments. All attachments will be added to the "Attachment" tab of the associated Finding. Click **Next** and **Finish**. A response is now completed.

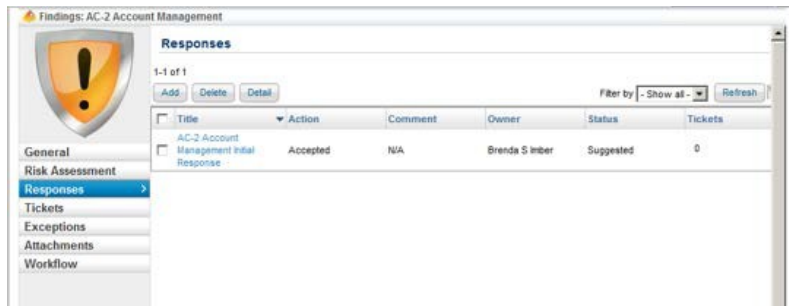


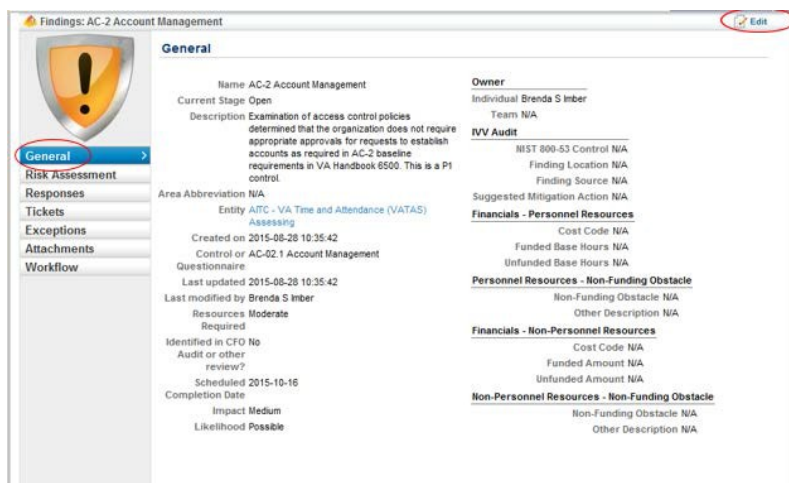
Figure 15. Response Tab Screen

[Procedure Step 1.3.2 Edit Finding to Include Financial Information](#)

OMB requires specific information for resources and financials to be reported for all FISMA systems. The Finding must be updated (using the edit function) to include estimated resources, both personnel hours and dollars associated with remediating the weakness (milestone). Apply a best realistic estimate in man-hours or dollars, based on total resources required to complete all milestones associated with weakness remediation. Refer to [Table 1 Guidance for Finding Components](#) and to the Financial entry for *Findings Training June 2014.ppt* in the GRC brown bag folder for specific instructions on how to complete this.

This step can also be done at the time the Finding is created ([Procedure Step 1.1 Create Finding](#)) if known. This procedure step should be repeated if the financial/resource changes.

[RiskVision Navigation](#)



1. Return to the General Tab of the Finding
2. Click "Edit" on the upper right corner

Figure 16. Edit Finding to include Financials Screen

Figure 17. Editing Financial Information Screen

Personnel Resources

1. Select Cost Code - Drop down to 1101, Personnel Resources
2. Enter total amount of funded hours (in .25 hour increments)
3. If applicable, enter total amount of unfunded hours (in .25 hour increments)
4. Select appropriate unfunded obstacle(s)
5. If selecting "other" enter short description in the "Other description" text box

Non-Personnel Resources

1. Select Cost Code(s)
2. Enter total amount of funded dollars in "Funded Amount" text box
3. If applicable, enter total amount of unfunded dollars in "Unfunded Amount" text box
4. Select appropriate non-funding obstacle(s)
5. If selecting "other" enter short description in "Other Description" text box
6. Click "Save" on upper right corner

Figure 18. Non-Funding Obstacles

Procedure Step 1.3.3 Progress Workflow to Stage 3: Review

Whenever a response is created it must be submitted for review and approval. If this is not done in RiskVision the workflow will not be progressed.

RiskVision Navigation

The System Steward will navigate to the Workflow tab and click the appropriate Response choice to submit the Finding for ISO review.

Findings: AC-2 Account Management

Name: Default Finding Workflow

1 Open 2 Respond 3 Review 4 Pending

5 Closed - Pending Control (3-2) Update 6 Closed

Since: 2015-08-28 10:51:14

Current Owner(s): Roy Coles, Sandra Hedtke, Diane Oriza, David Bekele, Brenda S Imber, David P. Henkel, Quincy Pence, Olumide Oloyede (Details)

Stage Actions: 1 of 5 needed for moving workflow to "Review"
1 of 5 needed for moving workflow to "Open"

☐ Force Transition
To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

Submit for Review Reject

Workflow History

1-2 of 2

Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2015-08-28 10:51:14	Open	Accept	Respond	No	Alice M Hanigan	David Bekele, Diane Oriza, Quincy Pence, Roy Coles, David P. Henkel, Olumide Oloyede, Sandra Hedtke, Brenda S Imber	Finding Approved. No changes anticipated.
2015-08-28 10:35:42		Start Workflow	Open	No	Brenda S Imber	Neil Cruz, Louise Lovett-Robinson, Stacy Jordan, Alice M Hanigan, Leigh Taylor	Finding workflow started

The System Steward navigates to the Workflow tab of the finding

1. Click Submit for Review

Figure 19. Progress Finding/Response to Review Screen

The Workflow is moved to Workflow Stage 3: Review and gives ownership to the ISO.

Findings: AC-2 Account Management

Name: Default Finding Workflow

1 Open 2 Respond 3 Review 4 Pending

5 Closed - Pending Control (3-2) Update 6 Closed

Since: 2015-08-28 11:03:25

Current Owner(s): Stacy Jordan, Neil Cruz, Leigh Taylor, Louise Lovett-Robinson, Alice M Hanigan (Details)

Stage Actions: 1 of 5 needed for moving workflow to "Pending"
1 of 5 needed for moving workflow to "Closed - Pending Control (3-2) Update"
1 of 5 needed for moving workflow to "Closed"
1 of 5 needed for moving workflow to "Respond"

☐ Force Transition
To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

Accept and Hold Accept and Close Pending Control (3-2) Update Accept and Close Reject

Workflow History

1-3 of 3

Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2015-08-28 11:03:25	Respond	Submit for Review	Review	No	Brenda S Imber	Neil Cruz, Louise Lovett-Robinson, Stacy Jordan, Alice M Hanigan, Leigh Taylor	Added initial response for ISO review and approval
						David Bekele, Diane Oriza, Quincy Pence	Finding

Figure 20. Workflow Stage 3-Review

4.2 Process Step 2: Review and Approve the POA&M

POA&Ms need to be approved in RiskVision. This is to ensure that the Findings are accurately identified, responses are adequate to resolve the Finding, and the responsibility for remediation is accurately defined.

Procedure Step	Responsible
2.1 Review Response	ISO
2.2 Approve Response	ISO

Procedure Step 2.1 Review Response

The ISO reviews the Finding/Response pair to ensure it is adequately documented in accordance with [Table 1. Guidance for Finding Components](#) and [Table 2. Guidance for Response Components](#), and that the mitigation actions (milestone with completion date field) are appropriate. Although the Finding had been reviewed previously ([Procedure Step 1.2](#)) it has been updated to include resource and financial information. In the review, pay special attention that the title, milestone and resource information and completion date are realistic and applicable. The ISO should review the Response as soon as possible so the POA&M progresses through the workflow.

RiskVision Navigation

The Finding workflow must be in Stage 3: Review as shown in [Figure 20](#).

Figure 21. Review Finding/Response Screen

The ISO navigates to the Finding Tab (refer to [Figure 15](#))

1. Click on the appropriate Finding
2. The screen to the left will appear. Click on the General Tab
3. Review the validity of all the fields. Ensure a start date was entered and nothing is entered in the changes to milestone field.

Procedure Step 2.2 Approve Response

RiskVision Navigation

If the Finding/Response pair is acceptable, the ISO approves it in RiskVision and it moves to Workflow [Stage 4: Pending](#). If it is not acceptable, the ISO documents deficiencies in the comments field and rejects it in RiskVision. If the POA&M is rejected, the Finding Workflow is sent back to [Stage 2: Respond](#). The System Steward must go back to [Procedure Step 1.3 Create Response](#) to revise. Ideally, the System Steward and ISO will work together ahead of time so that rejecting a POA&M is a rare

occurrence. In RiskVision there are actually four options to choose from in order to move the Workflow. This accommodates for additional responses associated with an open Finding to be reviewed and approved. The ISO should provide comments justifying reasons for each of the options selected in the comments box. Once approved, if the POA&M is still in progress, it should be in Stage 4: Pending.

Refer to Table 3: Criteria for Approval, below. In most cases the initial Response will result in using the "Accept and Hold" option. The ISO should add a comment

Figure 22. Approve/Reject /Response Screen

Table 3. Criteria for Approval

Option	When to Use
Accept and Hold	The ISO is in agreement with the documented Response and the finding cannot be closed at this time. This will move the Workflow to <u>Stage 4: Pending</u>
Accept and Close	This is applicable when approving the Finding for closure if all remediation tasks have been completed and evidence has been uploaded to the Finding (Attachment tab) and validated. Refer to <u>Process Step 4: Close POA&M</u> . <i>In most cases the Finding will not be ready to be closed at the point of processing the initial Response.</i>
Reject	Choose this if the response is insufficiently documented or does not provide current information. This will send the workflow back to stage 2: Respond and the SS will need to make changes as requested by the ISO.

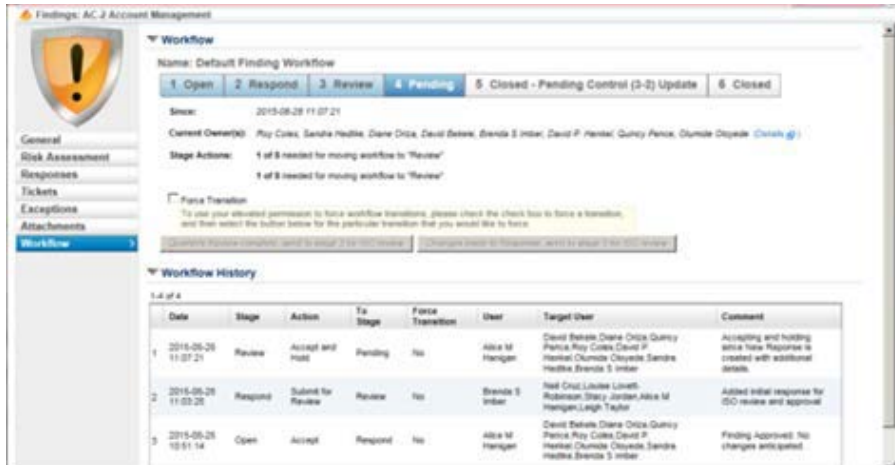


Figure 23. Workflow Stage 4-Pending

4.3 Process Step 3: Update and Monitor the POA&M

POA&Ms are monitored on a continuous basis. Reviews are performed to ensure POA&M remediation activities are on schedule, reflect updated and current information, and to track status and progress. Timely mitigation of weaknesses, combined with the identification and mitigation of new weaknesses indicate that a functional POA&M process is in place. In addition, POA&Ms are reviewed and prioritized for the enterprise. Prioritizing weaknesses reinforces the overall maturity of the process.

Procedure Step	Responsibility
3.1 Update POA&M if Remediation Plan Changes 3.1.1 Create New Response in RiskVision 3.1.2 Review and Accept in RiskVision	System Steward ISO
3.2 Update POA&M as a Result of Quarterly Reviews 3.2.1 Create New Response in RiskVision 3.2.2 Review and Accept in RiskVision	System Steward ISO
3.3 Monitor Status and Prioritize POA&Ms	All

Procedure Step 3.1 Update POA&M if Remediation Plan Changes

The information in the POA&M should be kept current as the remediation plan changes. If the plan is on track to meet the scheduled completion date and there have been no updates to document, the only requirement is the quarterly review. If changes occur due to fluctuations in resource availability, reprioritization of activities or unanticipated delays or funds, the POA&M must be updated to reflect revised milestones and/or revised anticipated date of completion. VA direction states that no edits or changes can be made to previous milestones therefore; this is accomplished by completing a new Response to the Finding in RiskVision ([Procedure step 1.3 Create Response](#)) in its entirety. In theory, if POA&M updates are completed as changes occur, continuous monitoring requirements would be fulfilled.

[Procedure Step 3.2 Update POA&M as a Result of Quarterly Reviews](#)

VA policy requires open POA&MS be reviewed quarterly, even if there has not been a change to the milestone requiring a new Response. This function is communicated via an Action item and ensures that proactive continuous monitoring occurs. Additional information pertaining to the quarterly review can be found in the RiskVision training folder on the OIS Portal. If a new Response was created as a result of [Procedure Step 3.1 Update POA&M if Remediation Plan Changes](#), within the quarter, the quarterly review requirement will be fulfilled and no further action is required.

Each quarter, both the System Steward and the ISO review the POA&M (both the Finding and all associated Responses) for the following:

- The scheduled completion date and financial information and are valid and remediation activities are still valid as documented in a Response. If this is the case, create a new Response to document the plan and scheduled completion date are on track.
- If the remediation plan has changed, create a new Response to document the change. Include a revised target completion date if applicable.

[Procedure Steps 3.1.1 and 3.2.1 Create New Response in RiskVision](#)

To make updates to POA&M information the System Steward will create a New Response ([Procedure Step 1.3 Create Response](#) in its entirety – See [Figure 10](#)). Refer back to [Table 2. Guidance for Response Components](#) which provides instructions on how to complete, as well as the review criteria for approval. Be sure to edit the Finding if the financial information has changed ([Procedure step 1.3.2](#)).

[RiskVision Navigation](#)

At the beginning of this procedure step the Finding Workflow should be in Stage 4: Pending which is the “ongoing” standing of a POA&M while it is process of being remediated. The workflow needs to be in either Stage 2: Respond or Stage 4: Pending for the SS to successfully process a new Response.

Refer to Procedure steps 1.3.1 Create a Response in RiskVision, and 1.3.2 and their associated RiskVision Navigation Screens with the below adjustments.

Figure 24. Example of New Response as a result of a Change in Plans

Figure 25. Quarterly Review Response Example

Figure 26. Submit Workflow for ISO Review and Approval Screen

1. Title – name the title according to the instructions (Table 2. Guidance for Response Components). The Title is used to sequence the Response or to identify a Quarterly Review
2. If the scheduled completion date is no longer valid, document a revised target completion date both in the Milestone w/ Completion Dates field of the Response
3. Update financial information (in the Finding) if applicable
4. Milestones w/Completion Dates - describe the current remediation status and document changes. If the Scheduled Completion Date has expired, or will not be met as documented in the Finding, provide an explanation
5. If the new Response is for a quarterly review and there are no changes, state "FYXX Quarter X Review completed". It is highly advisable to state something that has occurred in the past quarter towards remediation of this POAM.
6. Complete the Response through the 3 screens

1. From the Workflow tab submit the Response for ISO review (Procedure Step 1.3.3) choosing the appropriate option depending on whether the new Response was due to a quarterly review or due to changes in the plan
2. Use the Comment Box to state whether the new Response is a result of a change or a quarterly review

The Workflow will go to Stage 3: Review for ISO review and approval.

Procedure Steps 3.1.2 and 3.2.2 Review and Approve

The ISO will review and approve the subsequent Response as described in Procedure Steps 2.1 and 2.2 as well as criteria provided in [Figure 24](#). New Response Screen above. If the new Response reflects changes the ISO should ensure the reason for the update (delay, change in remediation plan) is adequately documented and the revised target completion date is reasonable.

RiskVision Navigation

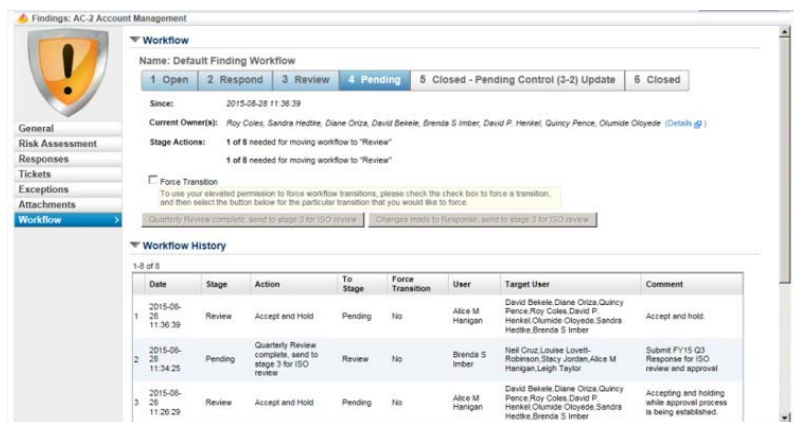


Figure 27. Review Workflow Screen

1. The ISO navigates to the Workflow tab of the Finding: If the ISO approves the New Response, the POA&M is accepted and moved to Pending Stage of the Finding Workflow by clicking "Accept and Hold". OR If the ISO does not agree with the documented Response reject by clicking "reject". The workflow is sent back to Stage 2: Respond. The SS must create a new response to address the deficiency.
2. If the New Response indicates that the POA&M should be closed, the ISO will review as per instructions in [Process Step 4: Close POA&M](#). If closure is approved click "Accept and Close". The workflow will move to Stage 6 Closed. "If a POAM is closed, the associated control must be updated with the evidence and the control marked as 'in place.'"
3. The ISO should provide appropriate comments in the comments field as to the justification for accept or reject.

Procedure Step 3.3 Monitor Status and Prioritize POA&Ms

Ongoing monitoring for an individual POA&M is performed by the System Steward and ISO to which it is assigned. VA should also prioritize and monitor POA&Ms at the enterprise, region, system, and facility level. Ongoing monitoring ensures that POA&Ms are prioritized such that the most critical weaknesses with the greatest potential to impact VA's mission are addressed first, and in a timely fashion. Using the reports described in Section 5, data can be extracted from RiskVision and manipulated in a consistent fashion to provide visibility of issues and a method to prioritize.

Focus POA&M activities to address:

- Open POA&Ms which are not started (no associated milestone)
- Open POA&Ms coming due in the next 30, 60, 90, etc. days
- Process open POA&Ms in the Open, Respond and Review workflow stages through to the Pending stage
- Review Open POA&Ms for instances where closure is appropriate
- Review validity of closure evidence and documentation for Closed POA&Ms
- Focus on training the field to properly test and approve closure evidence

Focus on better estimating, tracking and realizing completion dates

4.4 Process Step 4: Close POA&M

OMB's FISMA reporting guidance recommends that weaknesses should be considered "completed" only when they have been fully resolved and all remediation activities (documented in Responses to the Finding) have been tested and validated. Only

through testing can it be demonstrated that the vulnerability has been adequately addressed *and proven effective*. This step must occur and be thoroughly documented.

A mature POA&M process includes steps to validate the mitigation of weaknesses and ensures the accuracy of reported information. Throughout the process this document addresses this aspect - criteria to properly document and approve the Finding and Initial Response in [Process Step 1: Document the POA&M](#) and [Process Step 2: Review and Approve the POA&M](#); criteria and timeframes to properly update, document and approve changes in [Process Step 3: Update and Monitor the POA&M](#); and in [Process Step 4: Close POA&M](#), criteria to properly validate and document a weakness is fully addressed.

In this step, not only is it important to demonstrate the weakness has been resolved (adequate closure evidence) but also to verify and update the associated documentation to reflect what actually occurred (actual vs. planned). Over time, information collected for actual POA&Ms will be used to advance overall weakness mitigation effectiveness, apply lessons learned, and improve efficiency of procedures resulting in the avoidance of future potential weaknesses.

Before any Finding can be closed all remediation tasks identified must be completed. Once remediation tasks have been completed, the System Steward performs a new assessment of the control and updates the associated control implementation details and marks the control as in Place in RiskVision. (During certain times, for instance, if the Compliance Manager is in Stage 4: OCS Review and Approve, the System Steward is locked out from making updates).

Procedure Step	Responsible
4.1 Document POA&M Closure and Upload Evidence 4.1.1 Create a Close Response 4.1.2 Upload Evidence 4.1.3 Update Control	System Steward
4.2 Approve POA&M Closure 4.2.1 Validate POA&M 4.2.2 Accept or Reject POA&M Closure	ISO

[Procedure Step 4.1 Document POA&M Closure and Upload Evidence](#)

At this point in the process, the Finding Workflow is still in [Stage 4: Pending](#).

[RiskVision Navigation](#)

[Procedure Step 4.1.1 Create Close Response](#)

The System Steward will create a new Response in accordance with [Procedure Step 1.3 Create Response](#) (refer to [Figure 10](#)). However, this response must reflect what actually occurred versus prior responses which reflected planned actions. The following exceptions apply to the close response.

Figure 28. Close Response

Title	Action	Comment	Owner	Status	Tickets
AC-2 Account Management Second Response	Accepted	Submitting 2nd Response with more detail for SO review and approval	Brenda S Inber	Suggested	0
AC-2 Account Management Initial Response	Accepted	N/A	Brenda S Inber	Suggested	0
AC-2 Account Management FY15 Q2 Review Response	Accepted	FY15 Q2 Review complete. Changes are documented in the response	Brenda S Inber	Suggested	0
AC-2 Account Management Close Response	Accepted	Closing POA&M, all milestones have been completed. Original SCD was met.	Brenda S Inber	Suggested	0

Figure 29. Response Tab Screen with All Completed Responses

Procedure Step 4.1.2 Upload Evidence

POA&M closure evidence must be proof that the weakness has been remedied. Evidence must clearly show that a control is in place or that a weakness has been remediated. POA&M closure evidence is not necessarily the same as implementation control evidence. The evidence needs to demonstrate (“prove”) all deficiencies identified in the Finding have been mitigated or resolved. Different types of controls require different types of evidence. In general, evidence other than for -1 controls should not be documented procedures. The evidence must be succinct evidence that is reliable, dated, and specific. Evidence must be uploaded to RiskVision. It is not acceptable to point to SharePoint sites or other repositories outside of RiskVision. The table below provides an evidence description for specific management, operational and technical controls.

- Title: be sure to use Close in the title (refer to [Table 2. Guidance for Response Components](#))
- Document the Milestone with Completion Date Field:
 - Include whether the control has been reassessed, or will need to be reassessed in this field
 - Use this field to document tasks and events that actually occurred versus what the plan (prior Responses) had documented
 - Identify and include justification for submitted evidence, attach in “Attachments” Tab of finding
 - Document the actual completion date
 - Include the actual completion date the final milestone was completed
- Comments Field – Closing POA&M. All milestones have been completed. Note whether or not Original Scheduled Completion Date was met.
- End Date – the date the POAM is closed.

Table 4. Examples of POA&M Closure Evidence

Types of controls	Examples
<p>AC-1, AT-1, AU-1, etc.</p> <p>All -1 controls are policy and procedures controls</p>	<p>Evidence of policy is normally the enterprise signed policy or the regional policies.</p> <p>Evidence may be as minimal as signed cover page with date plus revision history page or one or the other. The entire document is not necessary and may cause VA more money in storage and back up of the portal, archive or storage location.</p>
<p>Management Controls: CA, PL, RA, SA</p> <p>Typically describe the steps or procedures of how to accomplish the management control</p>	<p>Plans, SOPs, Test results</p> <ul style="list-style-type: none"> • Individual Procedure Documents • Security Assessment Report • System Security Plan • Risk Assessment • VA SDLC management procedures <p>Evidence may be as minimal as signed cover page with date since these documents are often sensitive.</p> <p>Minutes of planning meetings may also be evidence where necessary to show or demonstrate the policy and plans are complete and the work is being done.</p>
<p>Operational Controls: AT, CM, CP, IR, MA, MP, PE, PS, SI</p>	<p>Sample training plans, screen shots from applications that show how a control is implemented. Example:</p> <ul style="list-style-type: none"> • Role Based Security Training plan (approved plan date and version) • Screen shot of online security awareness training tracking tool • Screen shots of baseline configurations for operating systems, databases, applications • Screen shot of results from change management auditing tool such as Tripwire. • Contingency Plan test results or after action report • Incident response lessons learned • Incident reporting procedures document • Screen shot of incident tracking tool • Maintenance tracking system screen shot or picture of paper log • Documented process for approving maintenance personnel; redacted approval of an application of real maintenance personnel. • Picture of locked media cases for offsite physical storage • Media Sanitation record(s) • Data Center Visitor logs

Types of controls	Examples
	<ul style="list-style-type: none"> • Pictures of keycard access panels • Picture of emergency shutoff switch • Procedures and records of personnel background checks • Screen capture of Nessus scan data report with date and time shown • Patch management accomplishments such as screen capture of patching being tested or applied with date and time.
Technical Controls: AC, AU, IA, SC	<p>Screen shots of configuration files that show how a control is implemented. Example:</p> <ul style="list-style-type: none"> • Account roles screen shots from Active Directory • Screen shot of audit record that shows content that matches VA Handbook 6500 requirement from Attachment 3 • Screen shot showing the log on screen requiring a PIV card or RSA token pin that clearly identifies multi-factor authentication use. • Screen shot showing the configuration requirements for password complexity • Screen shot showing separation of user from management privileges, i.e. users not being able to access system management activities.

RiskVision Navigation

The close Response has already been created in [Procedure Step 4.1.1](#). Navigate to the Finding to attach the evidence in the attachments tab.

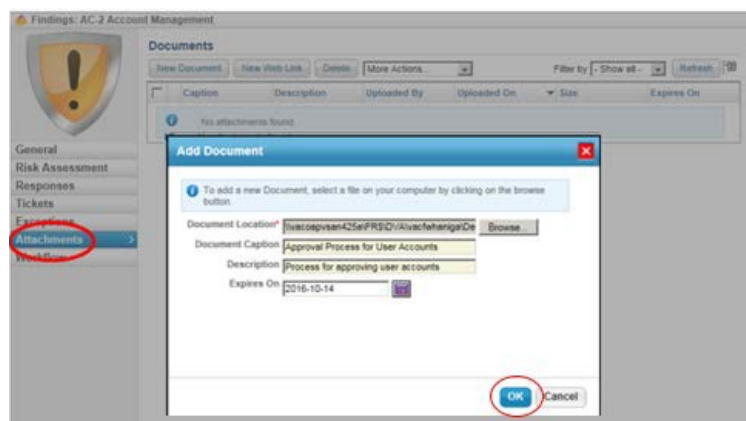


Figure 30. Add Document Screen

While in the specific Finding:

1. Click the **Attachments** Tab

A pop-up window to upload the document(s) will appear.

2. Browse for and attach the appropriate closure evidence.

3. Enter the Document Caption, Description, Expires On date and click OK.

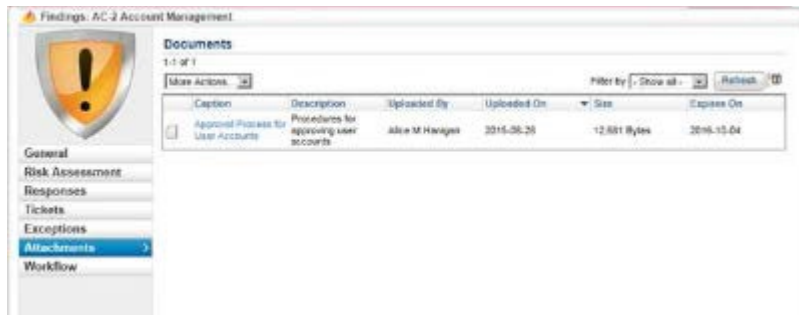


Figure 31. Finding/Attachments Tab Screen with Closure Evidence

Submit the workflow for ISO to Stage 3: Review

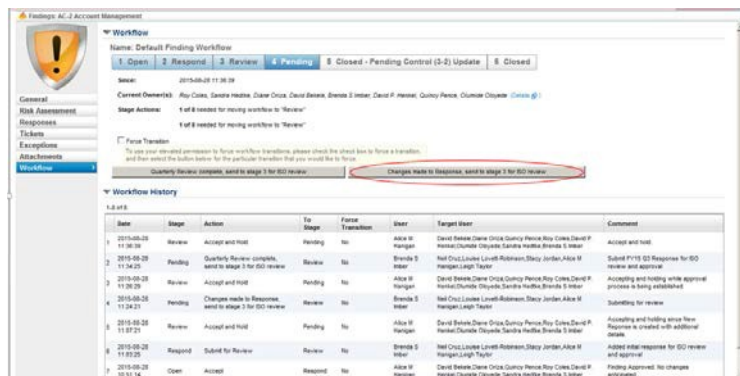


Figure 32. Submit Close Response Screen

Procedure Step 4.1.3 Update Control

The System Steward goes to the control in RiskVision and marks it as In Place, updates the control implementation details, and updates the control implementation evidence.

Procedure Step 4.2 Approve POA&M Closure

The ISO must review and validate the POA&M documentation and evidence to ensure that all tasks have been completed, the Close Response is accurately documented, and that evidence is sufficient to warrant closing the POA&M. The ISO validates closed Findings to determine if they have met the requirement. This is done by either re-testing or accepting the submitted documentation as proof of closure (refer to [Table 4. Examples of POA&M Closure Evidence](#)). All closed Findings must be supported by its associated documentation which is maintained in RiskVision

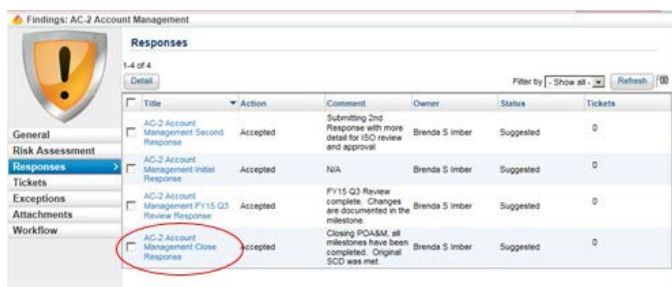
Procedure Step 4.2.1 Validate POA&M

The Close Response and Closure evidence and control information documentation must be reviewed, validated and tested.

1. Navigate to the workflow tab and click "Changes Made to Response" to move the Workflow to Stage 3: Review, for ISO review and approval. The System Steward should notify the ISO alerting there is a POA&M waiting for review and closure.
2. Enter Comments to alert the ISO the Finding is ready for review to be closed.

The Workflow will go to Stage 3: Review for ISO review and approval.

RiskVision Navigation

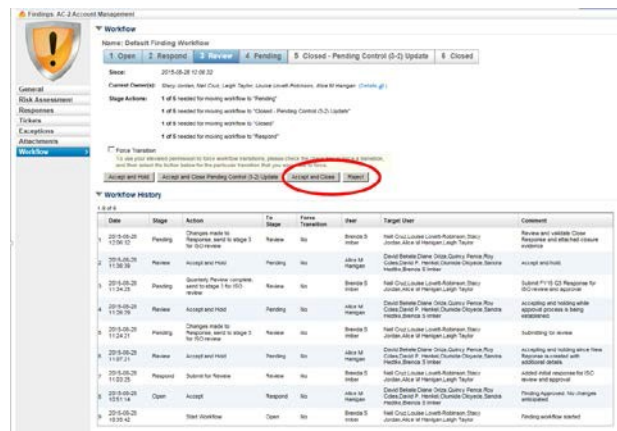


1. Navigate to the Finding
2. Click on the Responses Tab
3. Click on the **Close Response**
4. Review the information in the Close Response (Figure 28)
5. Review/validate/test closure evidence (Figure 31)

Figure 33. Navigate to the Close Response

The ISO should go to the control to verify that the control is now marked as In Place, the implementation details have been updated, and the evidence has been uploaded to the control.

Procedure Step 4.2.2 Accept or Reject POA&M Closure RiskVision Navigation



1. The ISO navigates to the Workflow tab of the Finding and chooses:
Accept and Close if all remediation actions have been completed, the evidence is sufficient, and the Close Response is properly documented as described in Figure 28. The ISO should document their concurrence in the comments box. The Workflow moves to Stage 6 Closed; or

Reject if the evidence or documentation is not sufficient, or all tasks were not completed. Include specific reasons for rejecting in the comments box. The Workflow is moved to Stage 2 Respond. The SS must create a new response to address the deficiency.

Figure 34. Accept and Close POA&M



Figure 35. Comments Box for Approving/Rejecting Screen

After clicking Accept and Close or Reject, a Comments pop-up box will appear. The ISO should acknowledge by documenting their approval in the comments box. In the case it is rejected, document the reasons and required corrections in the comments box and notify System Steward.

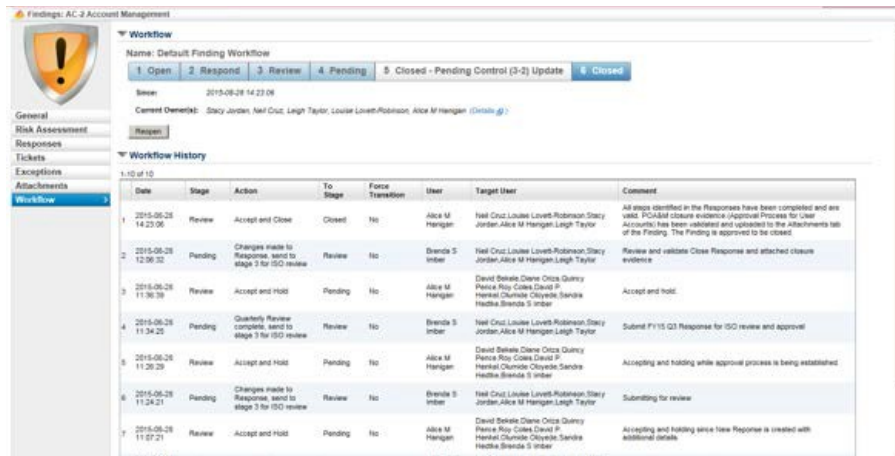


Figure 36. Workflow Stage 6-Closed

5 POA&M REPORTS

RiskVision provides reports that can assist in monitoring POA&M statuses among other things. Continuous monitoring POA&M statuses is essential and may lead to a more mature information security program. The following are two reports that you may find useful:

POA&M Details

This report provides details regarding the Findings, the milestones, and the additional milestones as well as additional information as listed below. NOTE: The additional milestones will show up on this report as individual line items. Because of this, the additional milestones should not be confused as an actual Finding.

This report includes the following data fields:

- Region
- Entity Type
- Control
- Description (of Finding)
- POC
- Scheduled Completion Date
- Created Date
- Current Status Date (date moved to the Current Status)
- Changes to Milestones
- Impact
- Entity Name
- Title (of Finding)
- Control Priority
- Type of Weakness
- Resources Required
- Identified in CFO Audit or other review
- Current Status (Workflow Stage)
- Milestones
- Milestone Added Date
- Likelihood

POA&M Details - Findings

This report is similar to the POA&M Details report; however, it does not provide details regarding the additional milestones.

This report includes the following data fields:

- Region
- Entity Type
- Control
- Description (of Finding)
- POC
- Scheduled Completion Date
- Created Date
- Current Status Date (date moved to the Current Status)
- Entity Name
- Title (of Finding)
- Control Priority
- Type of Weakness
- Resources Required
- Identified in CFO Audit or other review
- Current Status (Workflow Stage)

[RiskVision Navigation for both reports](#)

To generate this report in RiskVision:

- Step 1: Go to Analytics
- Step 2: Go to R6 Charts
- Step 3: Click on Shared Charts
- Step 4: Click on Public
- Step 5: Click on the appropriate report
- Step 6: Click on the Filter By drop down and choose Entity Name
- Step 7: Enter the Entity Name you are searching for and click Refresh

NOTE 1: Each of these reports can be exported into an Excel spreadsheet, as well as other formats, where the necessary information can be sorted and filtered accordingly.

NOTE 2: System Stewards and ISOs manage POA&Ms in the RiskVision Compliance Manager Module. The drill down menu allows users to view and modify the details of individual Findings and Responses. The Findings tab of an Assessment Tab for a given entity will show a table of all Findings for a given assessment.

6 CONCLUSION

A comprehensive POA&M process creates a repeatable cycle that effectively and efficiently corrects weaknesses. The standard approach prescribed in this Standard Operating Procedure ensures consistent application and accountability. Through this process, specific roles and responsibilities have been established. Continuous monitoring and prioritizing will further ensure that weaknesses are corrected within the specified time frame and resources are assigned consistent with the weakness risk.