FISMA RMF Module

Step-by-Step Tutorial

Document Version: 01.00.03 | April 2019

Contents

About Rsam Tutorials

The Rsam module step-by-step tutorials are designed to help you learn about a specific Rsam module and to gain basic familiarity with the user interface. The Rsam platform is highly configurable and is capable of handling both simple and comprehensive applications. The step-by-step tutorials and Rsam sandboxes, however, are specifically designed to quickly deliver a user experience without requiring further training. Each step-by-step tutorial walks you through common, out-of-the-box functionality within a given Rsam module, allowing you to get immediate hands-on familiarity with the module.

Rsam Sandbox Environment

Rsam module step-by-step tutorials are designed to work with the out-of-the-box Rsam configuration. You may follow this tutorial using an Rsam Sandbox environment or using your own instance of Rsam that you already own. If you are using this tutorial with an Rsam Sandbox environment, the URL to access your Rsam sandbox is delivered through an email. Otherwise, you may contact your Rsam Administrator for the URL to access your Rsam instance.

If you are using an Rsam sandbox environment, you should have provided Rsam with your organization's internet facing IP address. To find this information, open a browser and connect to an IP discovery site such as www.whatismyip.com, or contact your organization's Network Administrator for assistance. You may also contact your Rsam Customer Representative with any questions.

Sign-In Page

Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign-In page so that you can easily toggle between various sample accounts used throughout the tutorial.
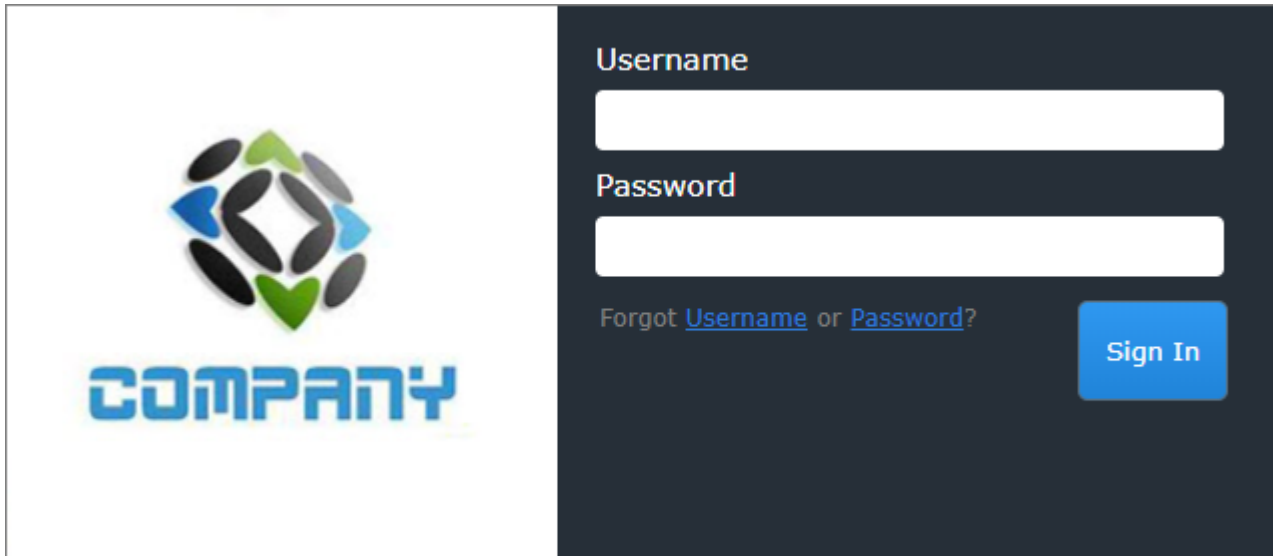
Like most elements in Rsam, the Sign-In page can be configured in a number of ways. Different authentication options such as user self-registration, integration with customer user directories (such as Active Directory), or integration with Single Sign-On products, such as Shibboleth, can be applied. You can also embed your own branding and logo on the Sign-In page.

Rsam FISMA RMF

Overview

The Rsam FISMA Risk Management Framework (RMF) module helps organizations automate the entire assessment lifecycle – from creation and initialization through assessment, remediation action, and ongoing risk and performance monitoring. It helps you evaluate risks on assets such as applications, databases, network devices, and computers, locations, business entities, and more. This tutorial provides a step-by-step procedure to walk you along one of many possible paths through the FISMA RMF workflow.

The Rsam FISMA RMF module provides the following capabilities and benefits:

- Identify, assess, and manage risk and compliance using various assessment criteria, such as business criticality and compliance requirements.

- Effective role-based access and user controls.

- Manage remediation efforts to address findings.

- Document remediation methods for risks after gaps have been identified, and track them on a continuing basis until they are resolved.

- Leverage leading industry content for standards and compliance.

Objects

Rsam Objects can be leveraged across all Rsam modules for storing and managing data. In the FISMA RMF module, objects are used to represent a specific topic or asset. While you do not need to understand the broader object concepts to complete this step-by-step guide, it is important to understand that this tutorial will leverage objects to represent NIST Information Systems that are being managed and assessed. You will see objects used in other ways across other tutorials.

RMF Workflows

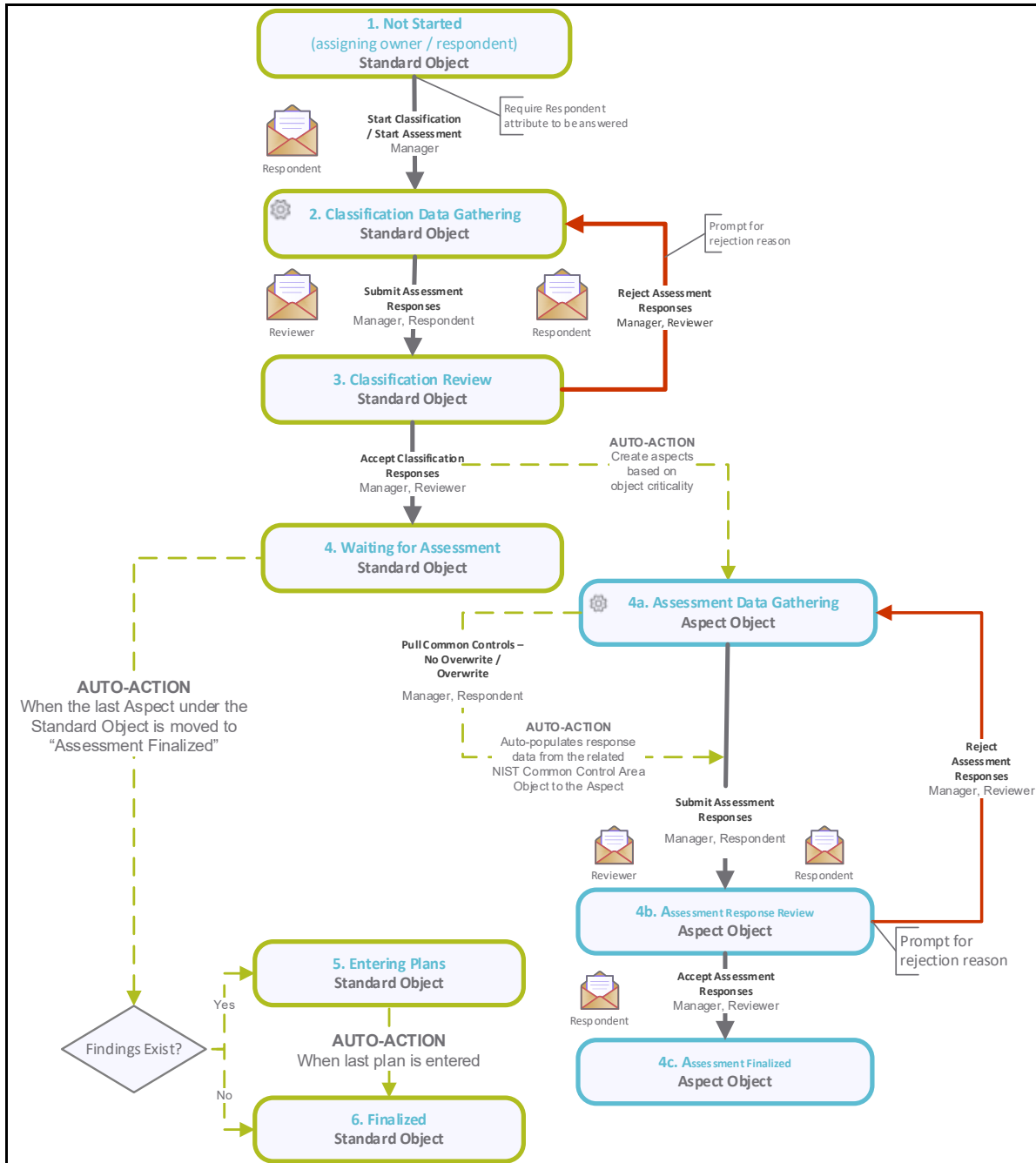This section covers the following workflows in the FISMA RMF module.

- Assessment Workflow

- Finding Workflow

Before proceeding to the workflow, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.
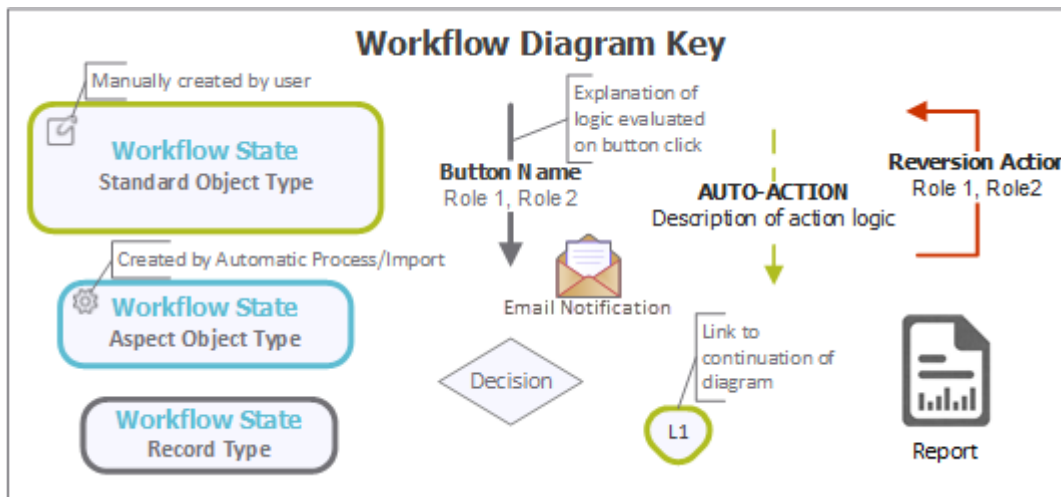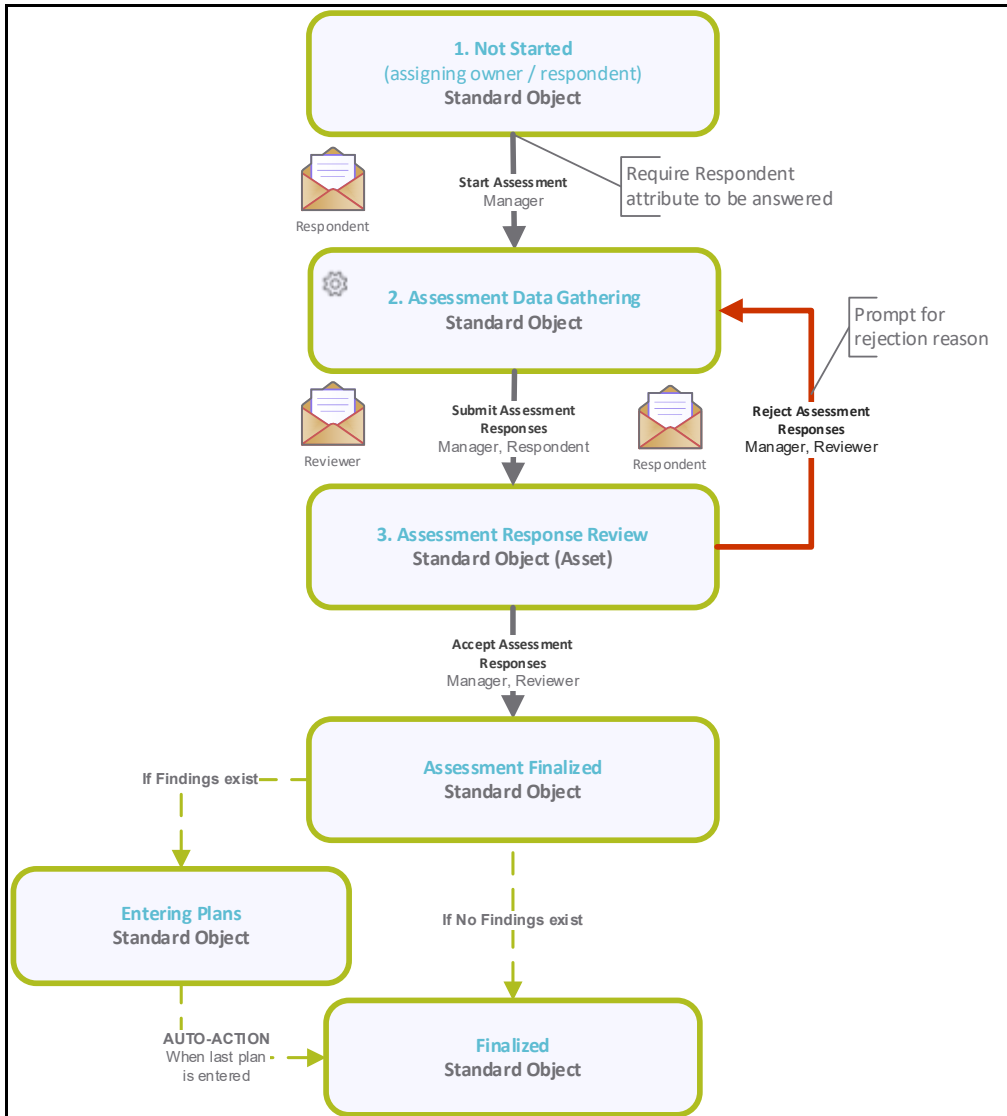
Assessment Workflow

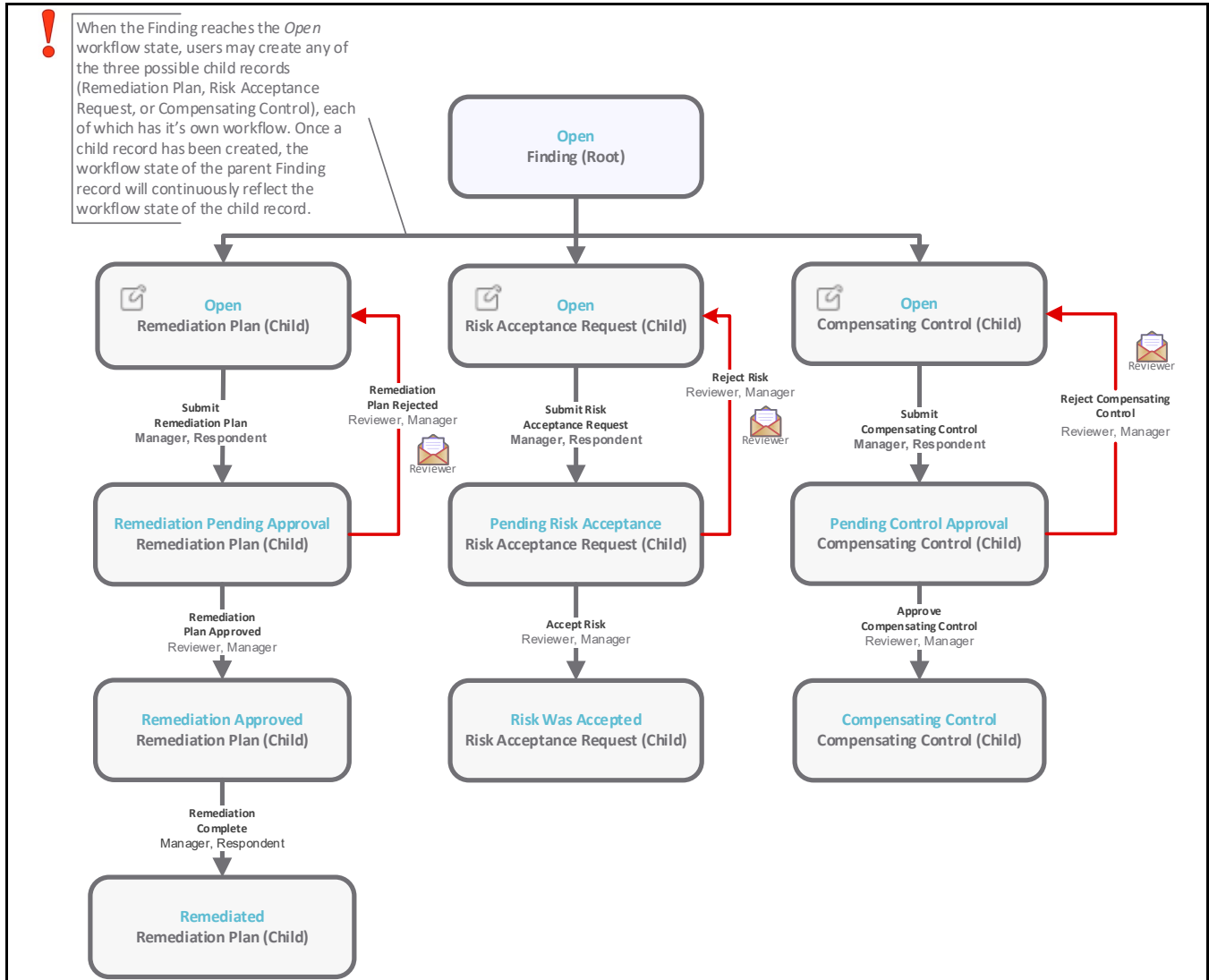The following diagram shows the classification questionnaire with aspects.

The following diagram shows the classification questionnaire without aspects.

Finding Workflow

The following diagram depicts the out-of-the-box Finding workflow.

When the Finding reaches the *Open* workflow state, users may create any of the three possible child records (Remediation Plan, Risk Acceptance Request, or Compensating Control), each of which has it's own workflow. Once a child record has been created, the workflow state of the parent Finding record will continuously reflect the workflow state of the child record.

Open
Finding (Root)

Open
Remediation Plan (Child)

Open
Risk Acceptance Request (Child)

Open
Compensating Control (Child)

Reviewer

Submit
Remediation Plan
Manager, Respondent

Remediation
Plan Rejected
Reviewer, Manager

Reviewer

Submit Risk
Acceptance Request
Manager, Respondent

Reject Risk
Reviewer, Manager

Reviewer

Submit
Compensating Control
Manager, Respondent

Reject Compensating
Control
Reviewer, Manager

Remediation Pending Approval
Remediation Plan (Child)

Pending Risk Acceptance
Risk Acceptance Request (Child)

Pending Control Approval
Compensating Control (Child)

Remediation
Plan Approved
Reviewer, Manager

Accept Risk
Reviewer, Manager

Approve
Compensating Control
Reviewer, Manager

Remediation Approved
Remediation Plan (Child)

Risk Was Accepted
Risk Acceptance Request (Child)

Compensating Control
Compensating Control (Child)

Remediation
Complete
Manager, Respondent

Remediated
Remediation Plan (Child)

Note: You may create as many variations to this pre-defined workflow configuration as desired by adding, deleting, or modifying steps in order to match your specific business processes.

User Accounts

User accounts are required for the individuals that are authorized to access a specific Rsam module. The Rsam sandbox for RMF comes with pre-populated sample accounts that include the following.

Note: Sample users for each of these roles are optionally provided with the baseline module installation package.

Account ID	User	Business Responsibilities
r_assessment _respondent	Assessment Respondent	This user is responsible for completing assessments.
r_assessment _reviewer	Assessment Reviewer	This user is responsible for reviewing and validating all the assessment responses submitted by the *Assessment Respondent* user.
r_assessment _manager	Assessment Manager	This user is responsible for the administration of all the Rsam assessments. This user can perform all the tasks that can be done with the *Assessment Respondent* and *Assessment Reviewer* user accounts.

The default password for all accounts in the Rsam FISMA RMF sandbox is *password*. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

High-Level Steps

The following is a high-level list of the steps described in this tutorial.

Step	User	Description
Step 1: Creating an Object	Assessment Manager	In this step, the *Assessment Manager* user creates a new object (NIST Information System), assigns an owner to the object, and begins the classification assessment.
Step 2: Answering Classification Assessment	Assessment Respondent	In this step, the *Assessment Respondent* user provides responses for the questions in the classification assessment, and submits the classification assessment responses for review.
Step 3: Reviewing Classification Responses	Assessment Reviewer	In this step, the *Assessment Reviewer* user reviews and accepts the classification assessment responses submitted by the Assessment Respondent user. After the responses are accepted, NIST Low Aspect Controls are generated automatically.
Step 4: Answering Control Assessment	Assessment Respondent	In this step, the *Assessment Respondent* user provides responses for the questions in NIST Low controls assessment that are created based on the classification assessment result, and then submits the control responses for review.

Step	User	Description
Step 5: Reviewing Control Assessment Responses	Assessment Reviewer	In this step, the *Assessment Reviewer* user reviews and accepts the responses for NIST Low controls assessment.
Step 6: Creating and Submitting a Remediation Plan	Assessment Respondent	In this step, the *Assessment Respondent* user creates a remediation plan for each questionnaire finding.
Step 7: Reviewing and Approving a Remediation Plan	Assessment Reviewer	In this step, the *Assessment Reviewer* user reviews and approves remediation plans.
Step 8: Flagging the Completion of a Remediation Plan	Assessment Manager	In this step, the *Assessment Manager* user flags the completion of remediation plans.

Step-by-Step Procedure

This section contains the workflow steps we will follow in this tutorial. The path followed in this tutorial walks you through a questionnaire-based assessment lifecycle. In this tutorial, you will learn how to create a new object (an NIST Information System), initialize an assessment for that object, answer and review the classification and control assessments, and remediate weak/failed controls. This path was chosen because it is the common path through the workflow, though you are welcome to explore the other paths as well.

Before you begin to execute the step-by-step procedure, consider following:

a. Practicing each step requires a different user account as mentioned in the High-Level Steps section. However, you may execute all the steps with the Assessment Manager user credentials in one session if desired.

b. Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your users receive the notifications while practicing the steps, please see the Setting up Email Addresses section later in this tutorial.

Note: This tutorial uses a subset of controls from the Rsam NIST control libraries to illustrate the concept of control assessment. You may also use other controls and survey types that are available, or create new ones.

Step 1: Creating and Initializing an Object

In this step, you will log in to Rsam as the *Assessment Manager* user to create a new object (NIST Information System), assign an owner that will answer the classification questionnaire, and then begin the classification assessment process.

1. Sign in as the *Assessment Manager* user. Enter **Username** as *r_assessment_manager* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management** > **Assessment Navigator**.
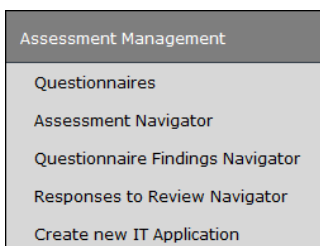
The assessment navigator appears.

3. In the assessment navigator view, click **Add** and then select **Object** from the options that appear.
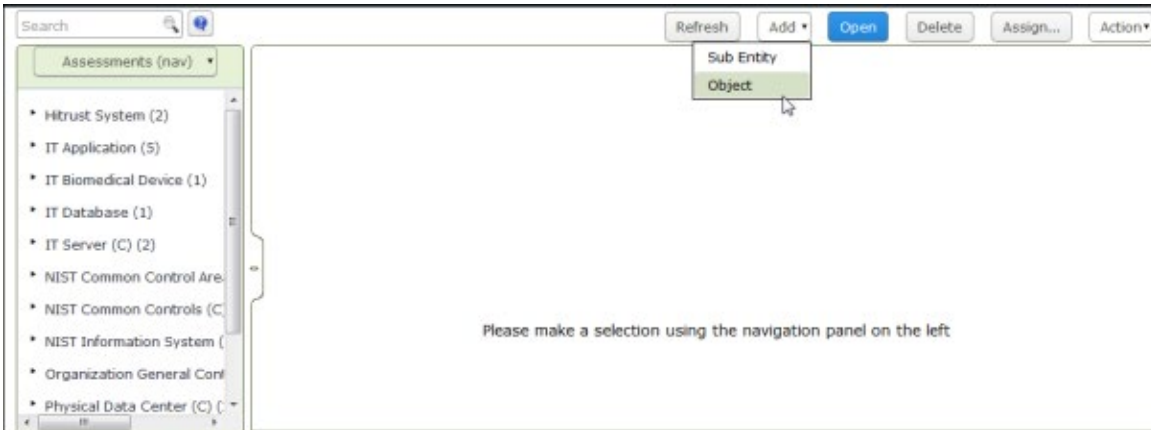
The **Create a new Object** dialog box appears.

4. Perform the following steps.

   a. Complete the following values for fields listed in the table below.

Field	Value
Object Name	RMF Example
Sub Entity	Assessments
Object Type	NIST Information System

   b. Click **Save**.
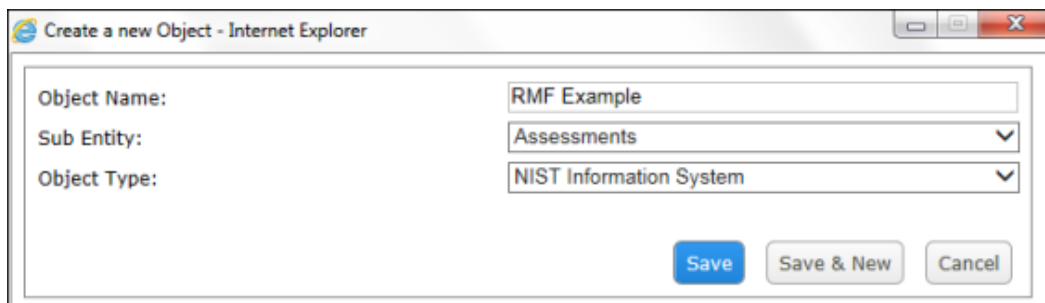
   The object is created.

5. From within the navigation panel with **Assessments (nav)** selected, expand **NIST Information System**, and then click **Not Started**.

   The assessments in the **Not Started** workflow state appear.

6. Locate the newly-created object **RMF Example**.

7. Use one of the following methods to open the newly-created *RMF Example* object:

    • Double-click the *RMF Example* object.

    • Select the *RMF Example* object, and then click **Open**.

    • Click the [icon] icon in the *RMF Example* object row.
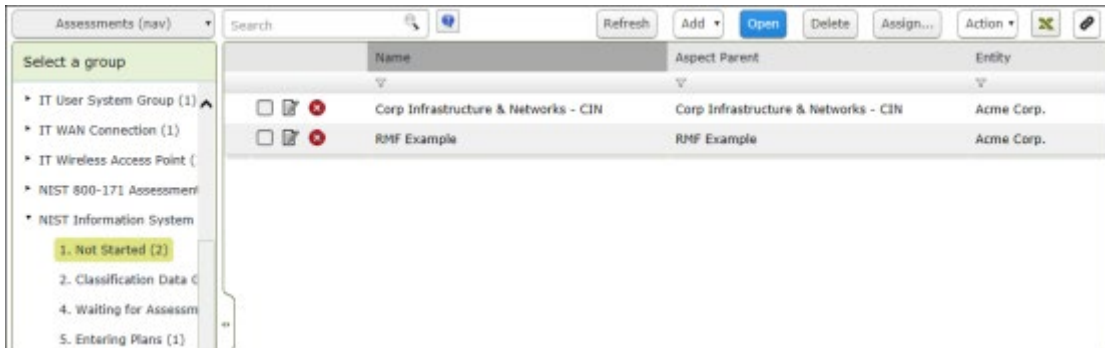
    The object details appear.

8. To open the classification questionnaire, under **Questionnaires**, click the [icon] icon.

    The questionnaire details appear.

9. In the questionnaire, locate the **Owner (this person will be assigned as the respondent)** attribute.

10. Assign the *r_assessment_respondent* user.

    a. Enter *r_assessment_respondent* in the Owner (this person will be assigned as the respondent) attribute. While typing, a list of users that match the string is shown.

    b. Select **r_assessment_respondent** from the user list.
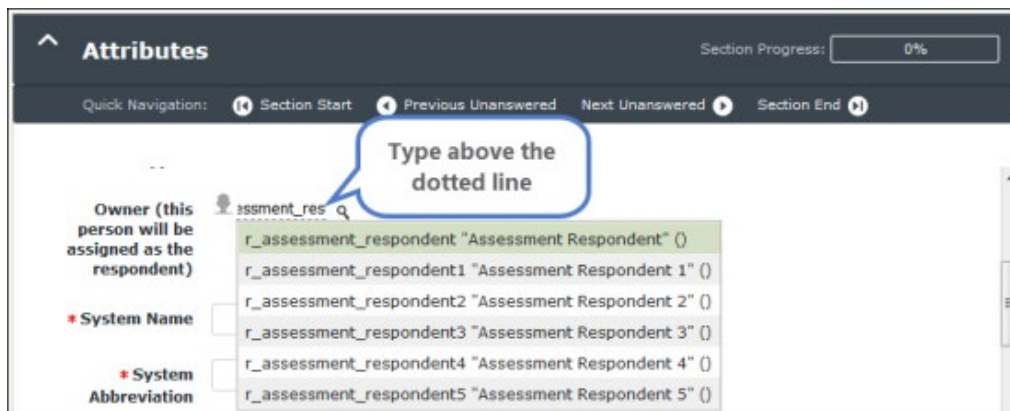
The *Assessment Respondent* user inherits the *Respondent* role and the permission to access the newly-created object.

11. Click **Start Classification**.
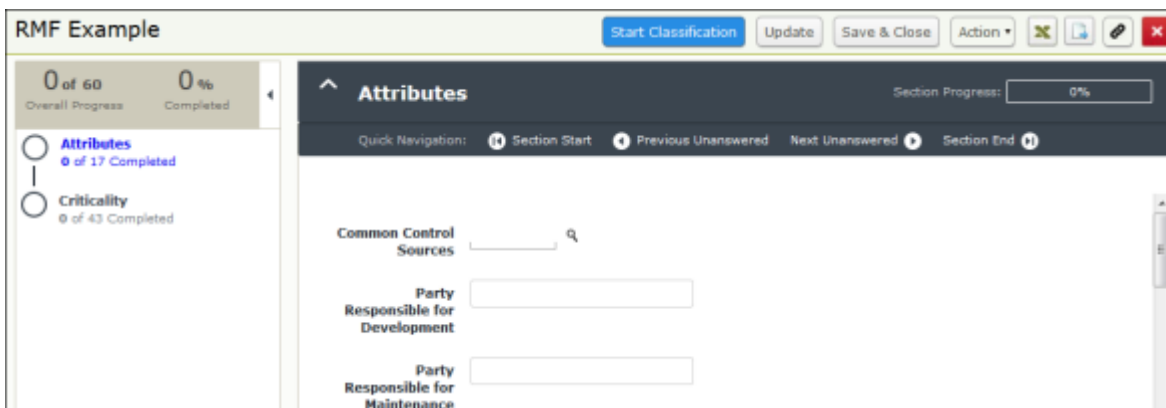
The *RMF Example* assessment enters the **2. Classification Data Gathering** state and an email notification is sent to the *Assessment Respondent* user.

12. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

    You have successfully logged out of Rsam.

Step 2: Answering Classification Assessment Questions

In this step, you will log in to Rsam as the *Assessment Respondent* user to answer the classification questionnaire. After answering all the questions, you will submit the classification questionnaire to the Assessment Reviewer user.

1. Sign in as the *Assessment Respondent* user. Enter **Username** as *r_assessment_respondent* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management > My Questionnaires Home**.

3. Under **My Questionnaires Home**, click the **Respondent** link.

The **My Assessments (Respondent)** grid appears.

4. Locate the **RMF Example** questionnaire and click **Open in the Action** column (as shown below).

The questionnaire details appear.

5. Complete all the required information available in the **Attributes** and **Criticality** sections. As part of this tutorial, we will generate the NIST Low Aspect Controls. To do this, under the **Criticality** section, select any answer (except N/A) for the **Mission Info Types: Natural Resources** criticality question, answer *Default* for the **FISMA: Minimum Security Categorization** criticality question, and answer **N/A** for the rest of the criticality questions.

Note: The default configuration requires responses to all Criticality questions, though administrators can change this requirement to match your organization's assessment process.

6. Fill out the sections on the left-hand-side of the questionnaire as follows:

    a. Click the desired section on the left-hand side.

    b. Use the following options to navigate within the section.

Option	Description
Section Start	This option takes you to the beginning of the section.
Previous Unanswered	This option takes you to the previous unanswered question from the current question.
Next Unanswered	This option takes you to the next unanswered question from the current question.
Section End	This option takes you to the end of the section.

Note: When all the responses are entered, the section header turns green.

7. Once you have entered all required answers, click **Submit Classification Responses**.

> **Note**: Information that you need to fill in the Attributes section are marked with asterisk (*). In case of unanswered Criticality questions, Rsam displays a message when trying to submit the incomplete assessment. Hence, be sure to complete all the required Criticality questions before submitting your responses.

8. In the message box that appears indicating that the responses have been submitted and the reviewer(s) will be notified, click **OK**.
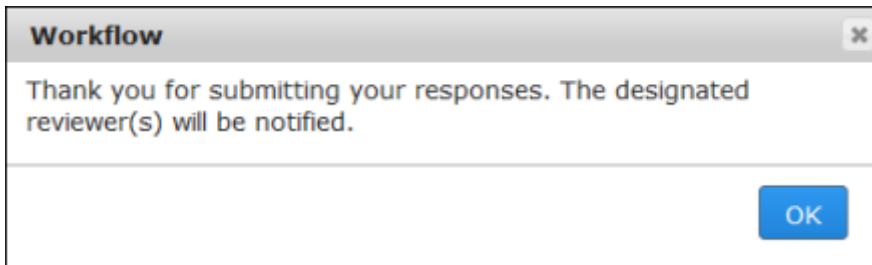
The *RMF Example* assessment enters the **Classification Review** state and an email notification is sent to the Assessment Reviewer user.

9. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

You have successfully logged out of Rsam.

Step 3: Reviewing Classification Assessment Responses

In this step, you will log in to Rsam as the *Assessment Reviewer* user to review the classification assessment responses submitted by the *Assessment Respondent* user. Here, you will accept all the responses.

1. Sign in as the *Assessment Reviewer* user. Enter **Username** as *r_assessment_reviewer* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management** > **Assessment Navigator**.

The assessment navigator appears.

3. From within the assessment navigator with **Assessments (nav)** selected, expand **NIST Information System**, and then click **3. Classification Review**.
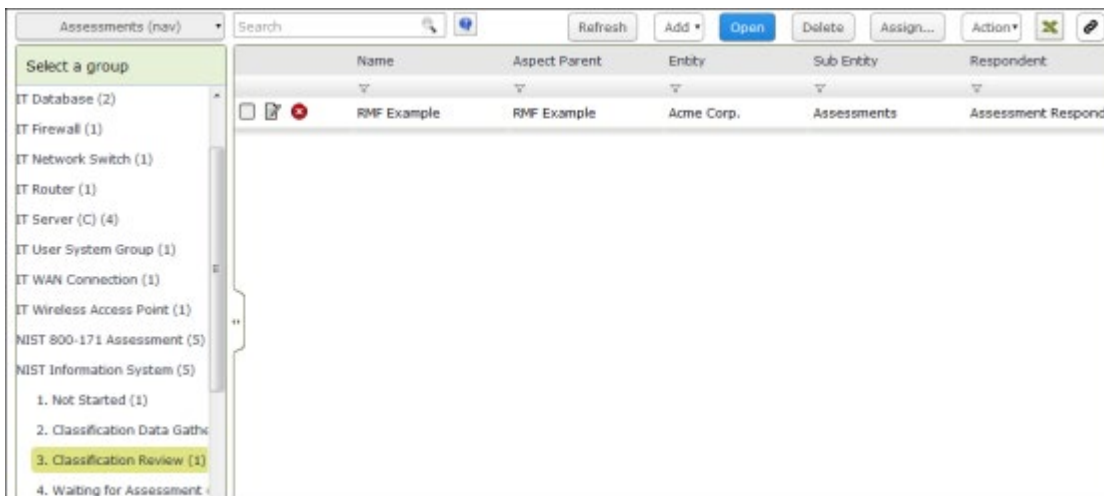
The objects in the **3. Classification Review** state appears.

4. Locate the classification assessment submitted by the *Assessment Respondent* user in Step 2: Answering Classification Assessment Questions.

5. Open the *RMF Example* object by using one of the following methods:

   - Double-click the *RMF Example* object.

   - Select the *RMF Example* object, and then click **Open**.

   - Click the ⬚ icon in the *RMF Example* row.

   The *RMF Example* object details appear.

6. Under **Questionnaires**, click the ⬚ icon.

The classification questionnaire appears.

7. Review the responses in each section.

8. Click **Accept Classification Responses**.
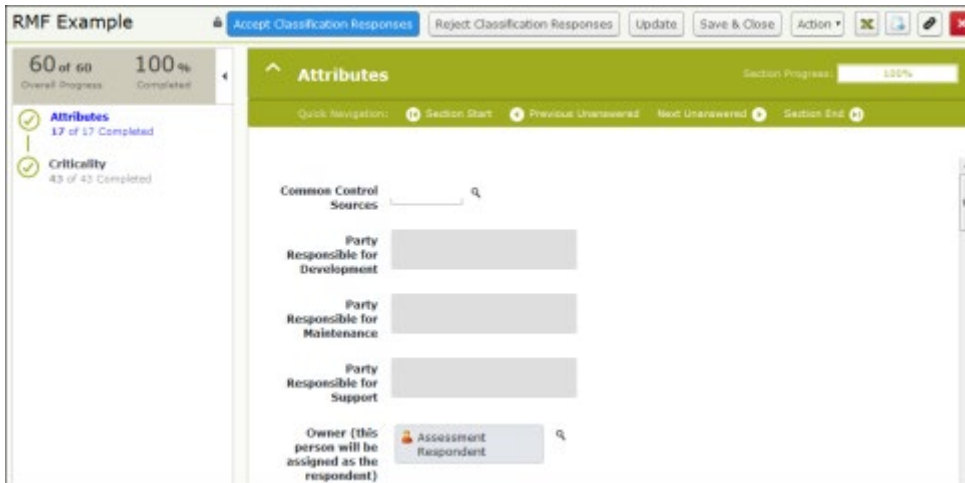
The classification data is evaluated, and then control assessments are generated automatically. The *RMF Example* assessment workflow enters the **4. Waiting for Assessment** state and an email notification is sent to the *Assessment Respondent* user. This also generates the *NIST Low Aspect Controls* automatically, and they are placed in the **4a. Assessment Data Gathering** workflow state.

9. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

You have successfully logged out of Rsam.

Step 4: Answering Control Questions

In this step, you will stay logged in to Rsam as the *Assessment Respondent* user to answer the control assessments and submit the responses to the *Assessment Reviewer* user.

1. In the **My Assessments (Respondent)** grid, click **Open** in the **Action** column of the **RMF Example – NIST 1. Low Controls** assessment row.

The questionnaire details appear.

2. Complete all the control questions.
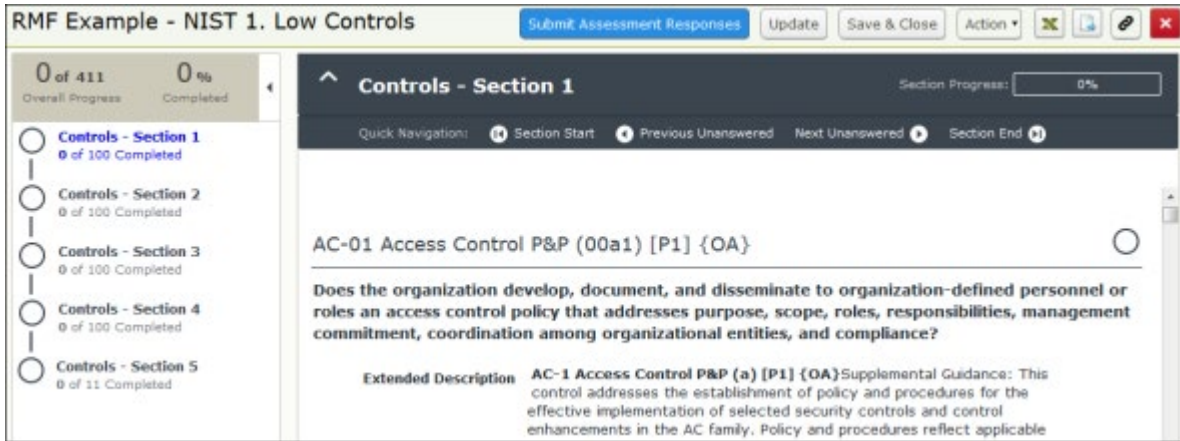
Note: To allow for quick and easy use of this tutorial, the default configuration of Rsam allows the questionnaire to be submitted without completing all required answers. Rsam can be easily configured to require answers for all questions before being submitted. The details about that configuration, however, are beyond the scope of this tutorial.
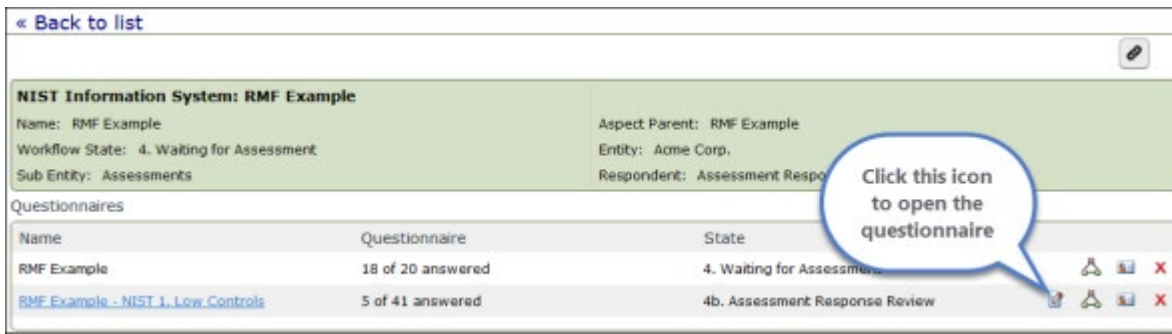
3. Click **Submit Assessment Responses**.

   The **NIST 1. Low Controls** assessment workflow enters the **4b. Assessment Response Review** state and sends an email notification to the *Assessment Reviewer* user.

4. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

   You have successfully logged out of Rsam.

Step 5: Reviewing Control Answers

In this step, you will log in to Rsam as the Assessment Reviewer user to review the control responses submitted by the *Assessment Respondent* user. Here, you will accept all the responses.

1. Sign in as the *Assessment Reviewer* user. Enter *Username* as *r_assessment_reviewer* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management** > **Assessment Navigator**.

   The assessment navigator appears.

3. From within the assessment navigator with **Assessments (nav)** selected, expand **NIST Information System** and click **4. Waiting for Assessment**.

   The objects in the **4. Waiting for Assessment** state appear.

4. Locate the *RMF Example* object in which the NIST low control answers were submitted by the *Assessment Respondent* user in Step 5: Answering Control Questions.

5. Open the *RMF Example* object by using one of the following methods:

   - Double-click the *RMF Example* object.

   - Select the *RMF Example* object, and then click **Open**.

   - Click the ![icon] icon in the *RMF Example* object row.
     The *RMF Example* object details appear.

6. Under **Questionnaires**, click the ![icon] icon in the **NIST 1. Low Controls** questionnaire row.

   The questionnaire details appear.

7. Review all the control responses.

8. Click **Accept Assessment Responses**.

   The control responses are evaluated against the standard determined by the assessment classification. A questionnaire finding record will be created for all the responses that do not meet the minimum standard requirements.

   The **NIST 1. Low Controls** assessment enters the **4c. Assessment Finalized** state. When all the control assessments enter the **4c. Assessment Finalized** workflow state, the parent assessment workflow for RMF Example object enters the **Entering Plans** state.

9. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

   You have successfully logged out of Rsam.

Step 6: Creating and Submitting a Remediation Plan

In this step, you will log in to Rsam as the *Assessment Respondent* user to review the questionnaire findings that were created automatically for all the controls that did not meet the assessment standards based on the defined classification. Here, you will propose remediation for the questionnaire findings.

Note: You can remediate a questionnaire finding by using the Remediation Plan (POAM), Risk Acceptance Request, or Compensating Control method. However, this tutorial will only walk you through the steps for the Remediation Plan (POAM) method in this tutorial. You may explore other remediation methods to enhance your learning, if desired.

1. Sign in as the *Assessment Respondent* user. Enter **Username** as *r_assessment_respondent* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management > Assessment Navigator**.

   The assessments navigator appears.

3. From within the navigator with **Assessments (nav)** selected, expand **NIST Information System**, and click **5. Entering Plans**.

   The objects in the **5. Entering Plans** state appear.

4. Locate the *RMF Example* object in which the control responses were reviewed by the Assessment Reviewer user in Step 5: Reviewing Control Answers.

5. Use one of the methods to open the *RMF Example* object:

   - Double-click the *RMF Example* object.

   - Select the *RMF Example* object, and then click Open.

   - Click the icon in the *RMF Example* object row.

   The *RMF Example* object details appear.

6. Under **Findings**, click the **Findings from Questionnaire** link.
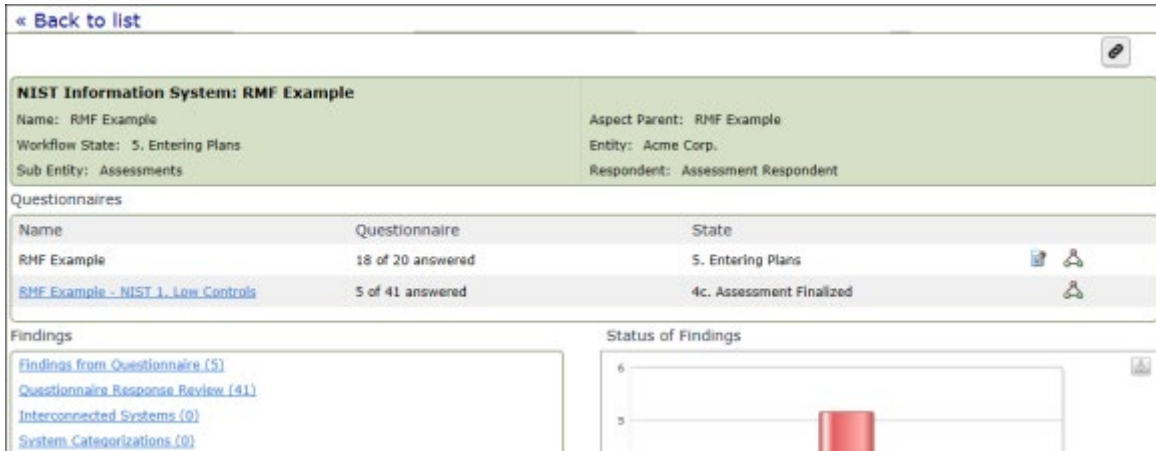
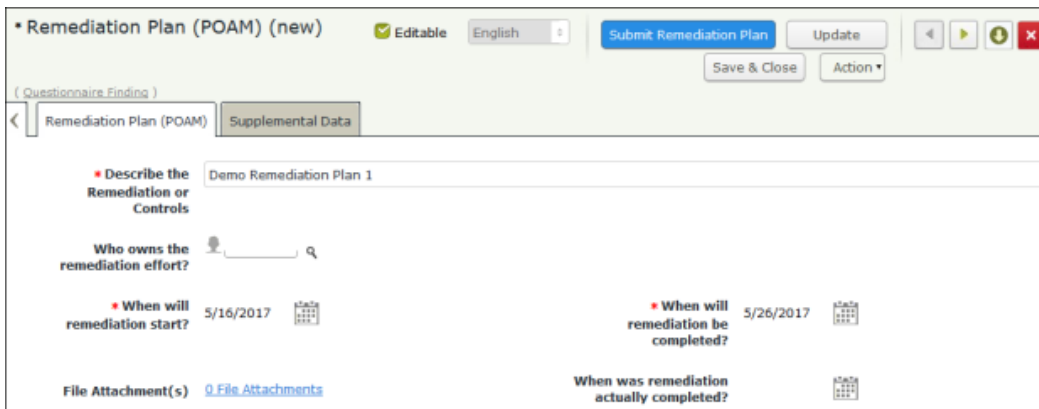The *RMF Example* object details open with the **Findings from Questionnaire** tab selected.

7. Select the desired finding, and then click **Add** and select **Remediation Plan (POAM)** from the options that appear.
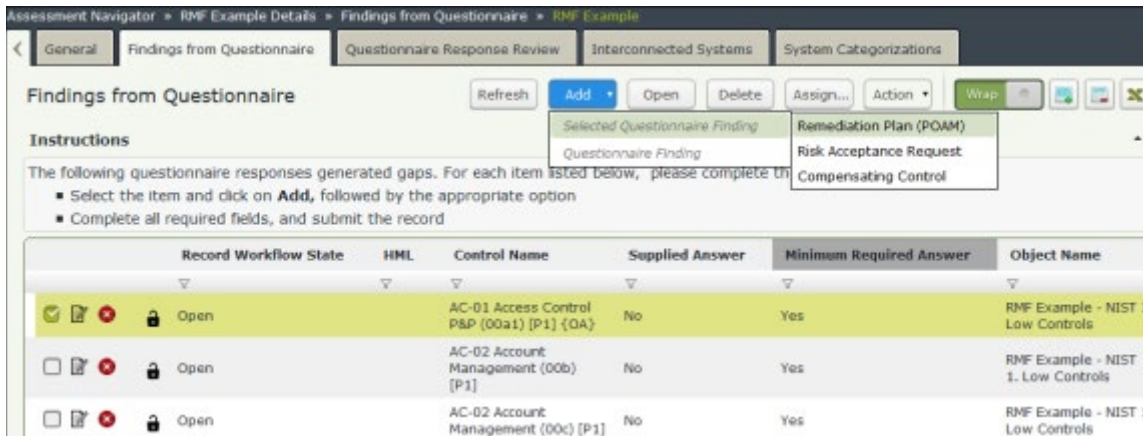
The **Remediation Plan (POAM) (new)** record opens with the **Remediation Plan (POAM)** tab selected.

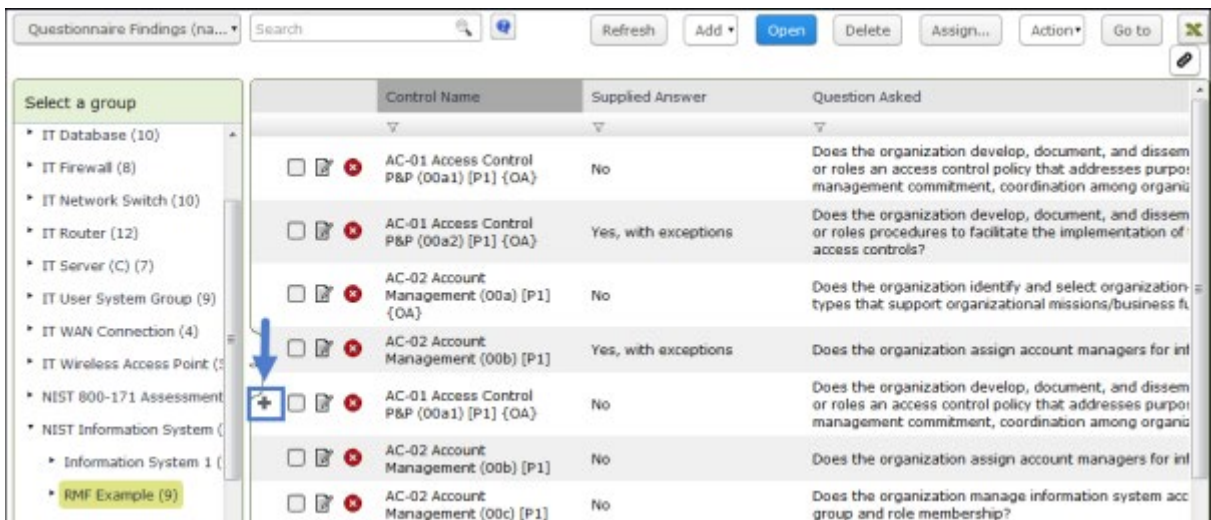8. On the **Remediation Plan (POAM)** tab, complete the values for fields listed in the following table.

Field	Value
Describe the Remediation or Controls	Demo Remediation Plan 1
When will remediation start	Select the desired start date
When will remediation be completed	Select the desired end date

9. Skip the **Supplemental Data** tab.

10. Click **Submit Remediation Plan**.

    The remediation plan (POAM) record is created, and the questionnaire finding workflow and the remediation plan (POAM) workflow enters the **Remediation Pending Approval** state.

11. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

    You have successfully logged out of Rsam.

Note: While this tutorial navigates to the findings by opening our specific object, there are other navigators that show all findings across all objects in a single, consolidated list. Users will use such navigators when documenting plans across multiple objects.

Step 7: Reviewing and Approving a Remediation Plan

In this step, you will log in to Rsam as the *Assessment Reviewer* user to review and approve the **Demo Remediation Plan 1.**

1. Sign in as the *Assessment Reviewer* user. Enter **Username** as *r_assessment_reviewer* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management > Questionnaire Findings Navigator**.

   The questionnaire findings navigator appears.

3. From within the navigation panel with **Questionnaire Findings (nav)** selected, expand **NIST Information System**, and then click **RMF Example**.

   The questionnaire findings appear.

4. Locate the questionnaire finding for which the *Assessment Respondent* user created the **Demo Remediation Plan 1** record in Step 6: Creating and Submitting a Remediation Plan.

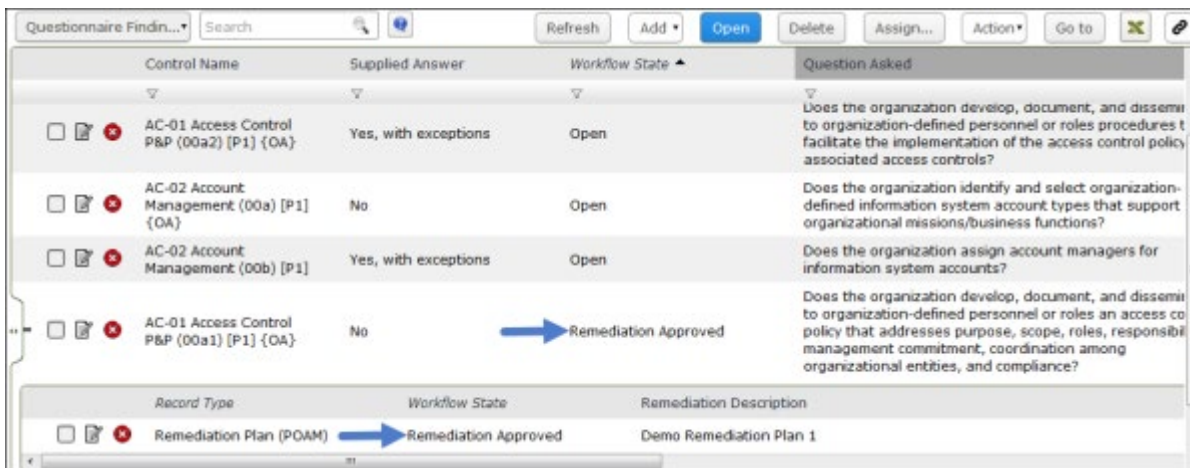5. Click **+** in the questionnaire finding record row.

6. Use one of the following methods to open the **Demo Remediation Plan 1** record:

   - Double-click the **Demo Remediation Plan 1** record.

   - Select the **Demo Remediation Plan 1** record, and then click **Open**.

   - Click the [icon] icon in the **Demo Remediation Plan 1** record row.

   The **Remediation Plan (POAM)** record opens with the **Remediation Plan (POAM)** tab selected.

Step-by-Step Tutorial

7. Review the information on the **Remediation Plan (POAM)** and **Supplemental Data** tabs, and then click **Remediation Plan Approved**.

The remediation plan workflow and the questionnaire finding workflow enters the **Remediation Approved** state.

8. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

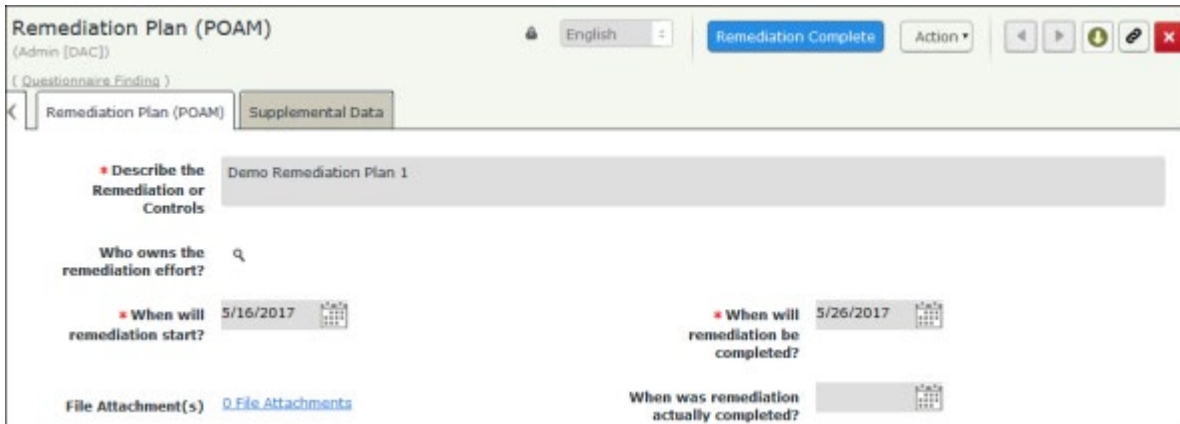You have successfully logged out of Rsam.

Step 8: Flagging the Completion of a Remediation Plan

In this step, you will log in to Rsam as the *Assessment Manager* user to flag the completion of the **Demo Remediation Plan 1** record approved by the *Assessment Reviewer* user.

1. Sign in as the *Assessment Manager* user. Enter the **Username** as *r_assessment_manager* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **Assessment Management > Questionnaire Findings Navigator**.

   The questionnaire findings navigator appears.

3. From within the navigation panel with **Questionnaire Findings (nav)** selected, expand **NIST Information System** and click **RMF Example**.

   The questionnaire findings appear.

4. Locate the questionnaire finding for which the Assessment Reviewer had approved the remediation plan in Step 7: Reviewing and Approving a Remediation Plan.

5. Click **+** in the questionnaire finding record row.

6. Use one of the following methods to open the **Demo Remediation Plan 1** record:

   - Double-click the **Demo Remediation Plan 1** record.

   - Select the **Demo Remediation Plan 1** record, and then click Open.

   - Click the icon in the **Demo Remediation Plan 1** record row.

   The **Remediation Plan (POAM)** record with the **Remediation Plan (POAM)** tab selected appears.

8. Review the information on the **Remediation Plan (POAM)** and **Supplemental Data** tabs, and then click **Remediation Complete**.

The remediation plan workflow and the questionnaire finding workflow enters the **Remediated** state.

9. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

You have successfully logged out of Rsam.

Appendix 1: Email Notifications and Offline Decision Making

Setting up Email Addresses

This module is configured to send automated email notifications at specific points in the workflow. In a production system, email addresses are usually gathered automatically using an LDAP server or a directory service. However, the email addresses in your Rsam instance can be manually provided for testing purposes.

To manually provide the email addresses, perform the following steps:

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the FISMA RMF module.

2. Sign in as *r_admin* user. Enter **Username** as *r_admin* and **Password** as *password*.

3. Navigate to **Manage** > **Users/Groups**.

4. Double-click a user row to open the details.

5. Provide an email address in the **eMail ID** attribute.

6. Click **OK**.

   The email address of the user account is saved.

Offline Decision Making

Rsam email notifications are configurable including what notification should be sent, what users or roles will receive the notifications, and the content in the notifications.

Offline Decision Making is a powerful and popular feature of Rsam. It provides the Rsam platform directly to the users to perform workflow actions without connecting to the Rsam module. The following image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.
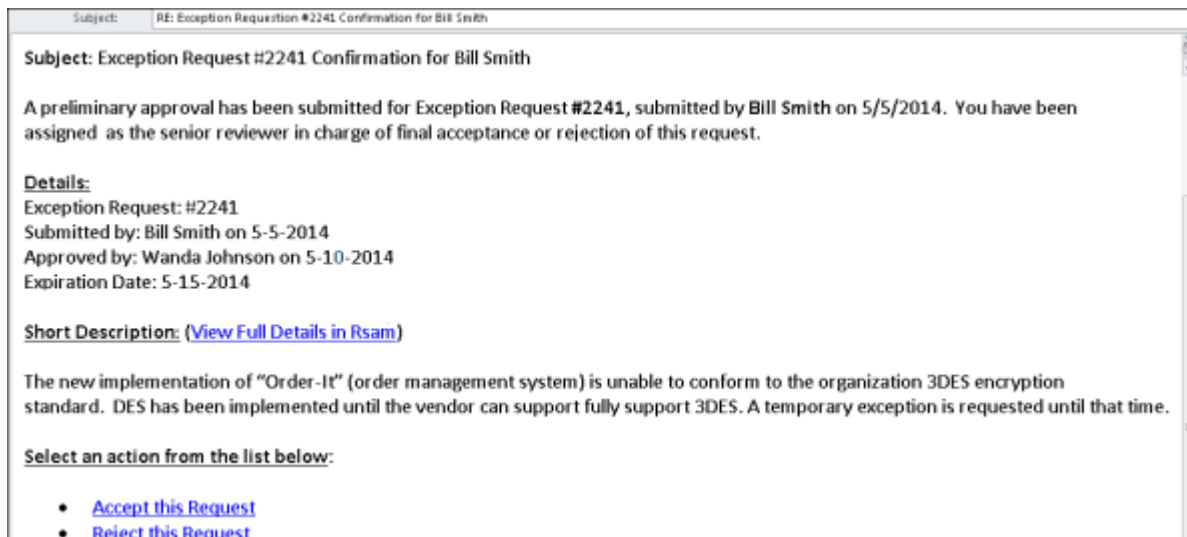
Appendix 2: Rsam Documentation

FISMA RMF Module Baseline Configuration Guide

To learn more about the pre-configurations in the FISMA RMF Module, refer the *FISMA RMF Module Baseline Configuration Guide*. You should have received the *FISMA RMF Module Baseline Configuration Guide* along with the FISMA RMF Module sandbox. If not, please contact your Rsam Customer Representative to obtain an electronic copy of the *FISMA RMF Module Baseline Configuration Guide*.

Online Help

This tutorial provides the step-by-step instructions for the Rsam FISMA RMF Module module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **Username** as *r_admin* and **Password** as *password*.

2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

   The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.