ITRMBond - Risk and Compliance Assessments

Step-by-Step Tutorial

Rsam Version: 10 | Document Version: 01.00.04

August 2020

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.

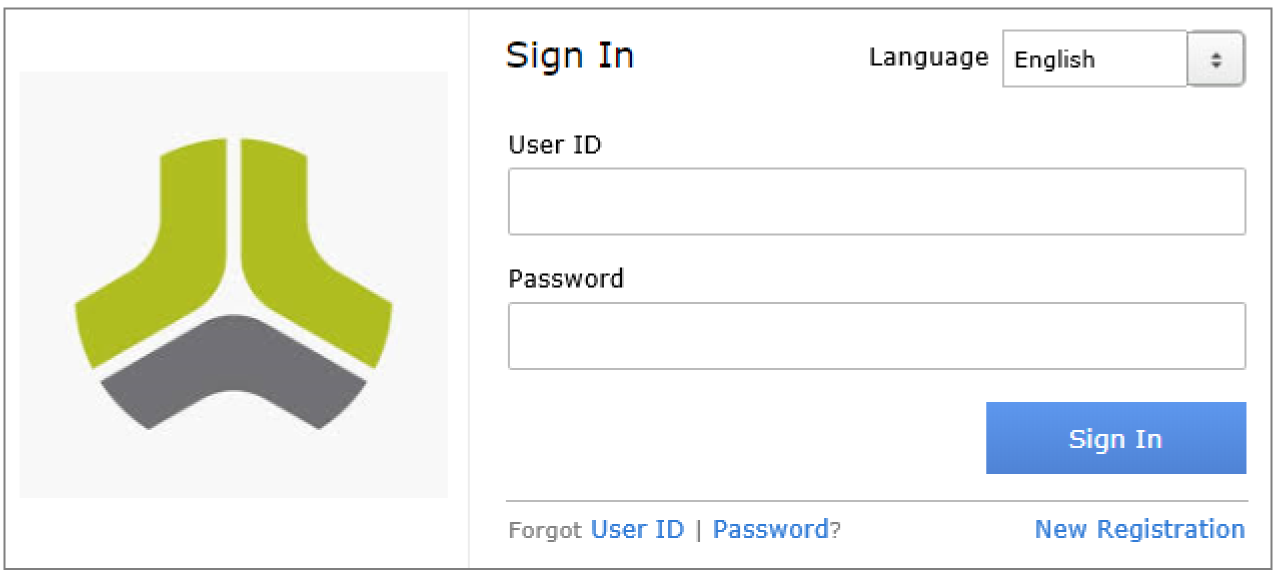
Rsam Sandbox Environment

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

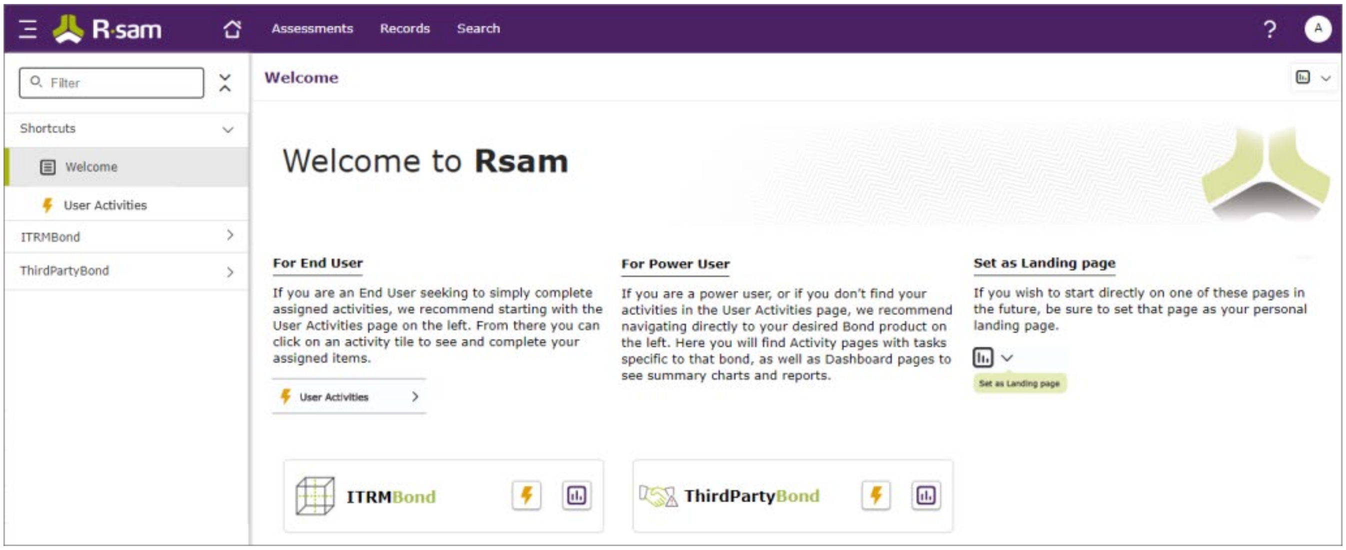
Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign In page so that you can easily toggle between various sample accounts used throughout 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.

Welcome Page

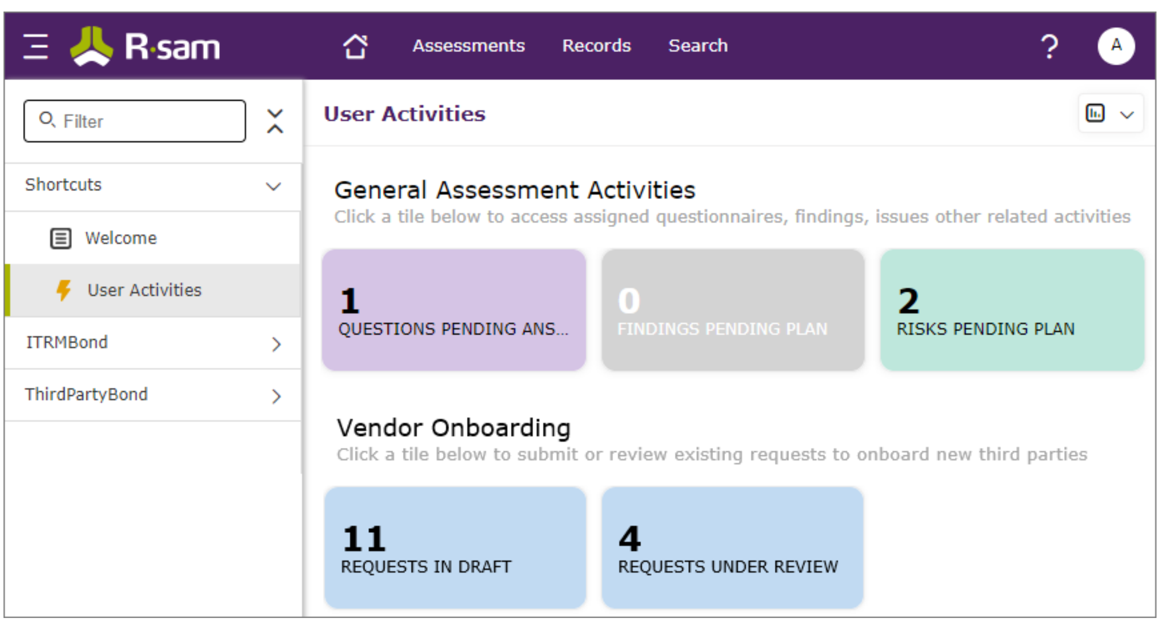
The Welcome Page is the first page that appears when you log in to Rsam for the first time. This page provides navigation instructions and shortcuts to access the most commonly used pages from the bonds you have access to.



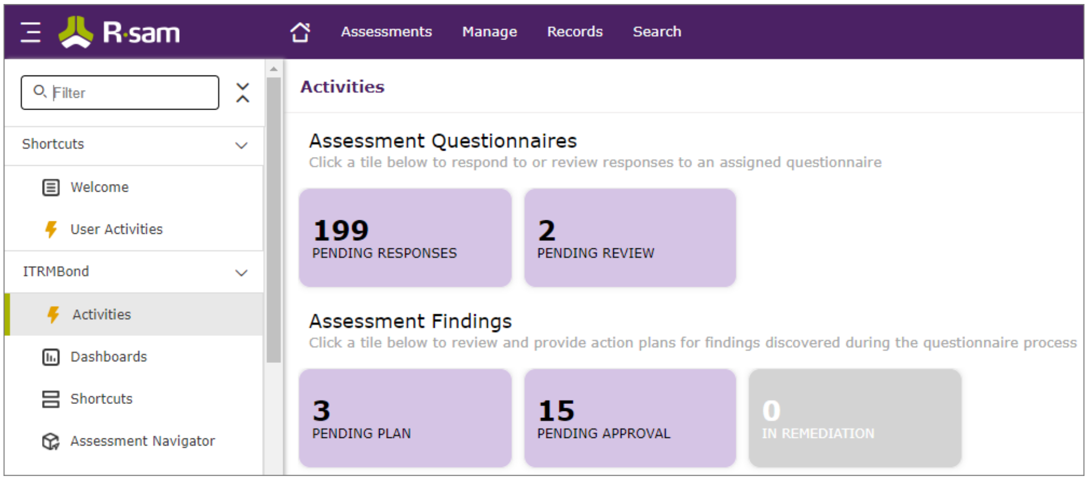
Note: The view of the Welcome Page may be different from the one shown in the image, based on the role of the logged in user.

Navigating to Tasks and Dashboards

If you are an end user and have logged in to complete assigned tasks, you can click User Activities available on the left navigation bar to view the most frequently used Activity Centers *across all bonds assigned for your role*. You can click the relevant activity tile to navigate to your tasks.



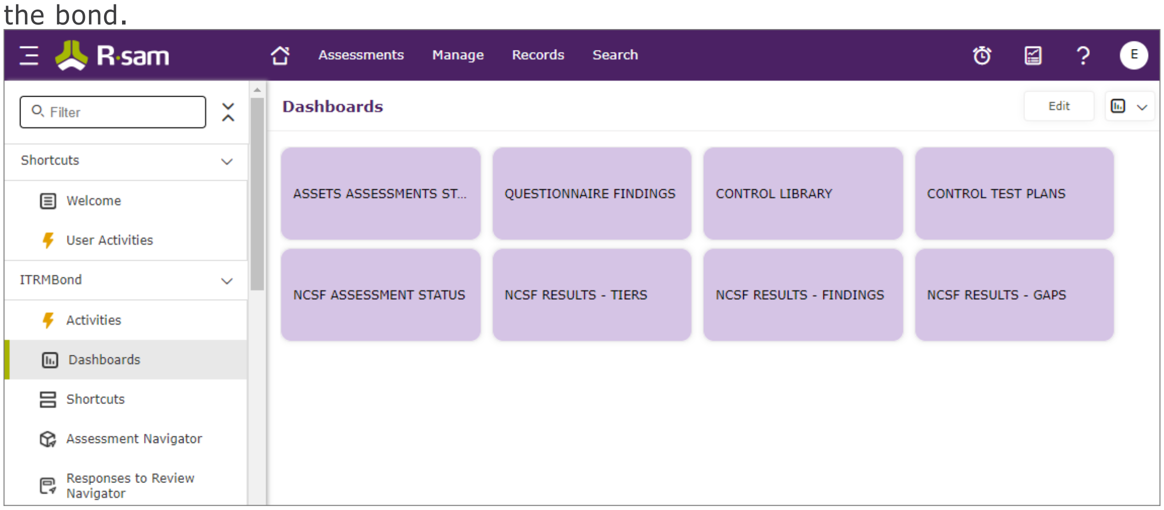
If you do not find the required activity tiles, you can either click corresponding to a bond on the Welcome Page or navigate directly to the bonds from the left navigation bar and select the **Activities** tab to view all related Activity Centers.



Click an Activity Center tile to view all related tasks.

Additionally, you can perform the following navigation actions:

- Click corresponding to a bond on the Welcome page to view all Dashboards configured for the bond.

  Alternatively, you can navigate to the required bond from the left navigation bar and select **Dashboards**.

- Click corresponding to a bond on the Welcome page to view all Dashboards configured for the bond.

  Alternatively, you can navigate to the required bond from the left navigation bar and select **Dashboards**.

- Expand the required bond from the left navigation bar and use the pages.

For information on using the home page features and configuring Activity Centers, see the *Rsam Administrator* and *End-User Help*.

Rsam Risk and Compliance Assessments

The Rsam Assessments module helps organizations to automate the entire assessment lifecycle – from creation and initialization through assessment, remediation action, and ongoing risk and performance monitoring. They help you evaluate assets such as applications, databases, network devices, computers, as well as locations, business entities, and more. This tutorial provides a step-by-step procedure to walk you through one path of an Assessment workflow within the module.

The Rsam Assessments 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

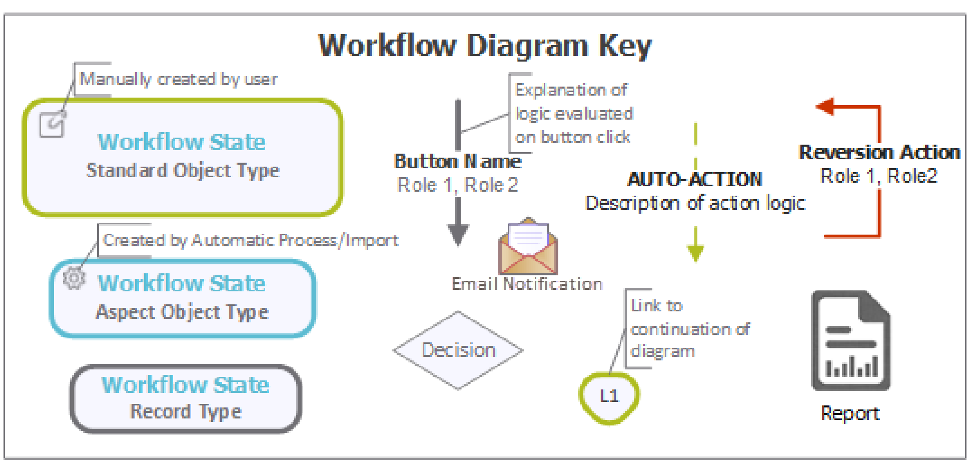
Objects in Rsam can be leveraged across all Rsam modules for storing and managing data and defining workflow and assignments for a specific topic or asset. While you do not need to understand the broader object concepts to complete this step-by-step guide, it is important to understand that this tutorial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

Assessments Workflows

This section covers the following diagrams that illustrate the workflows in the Assessments module:

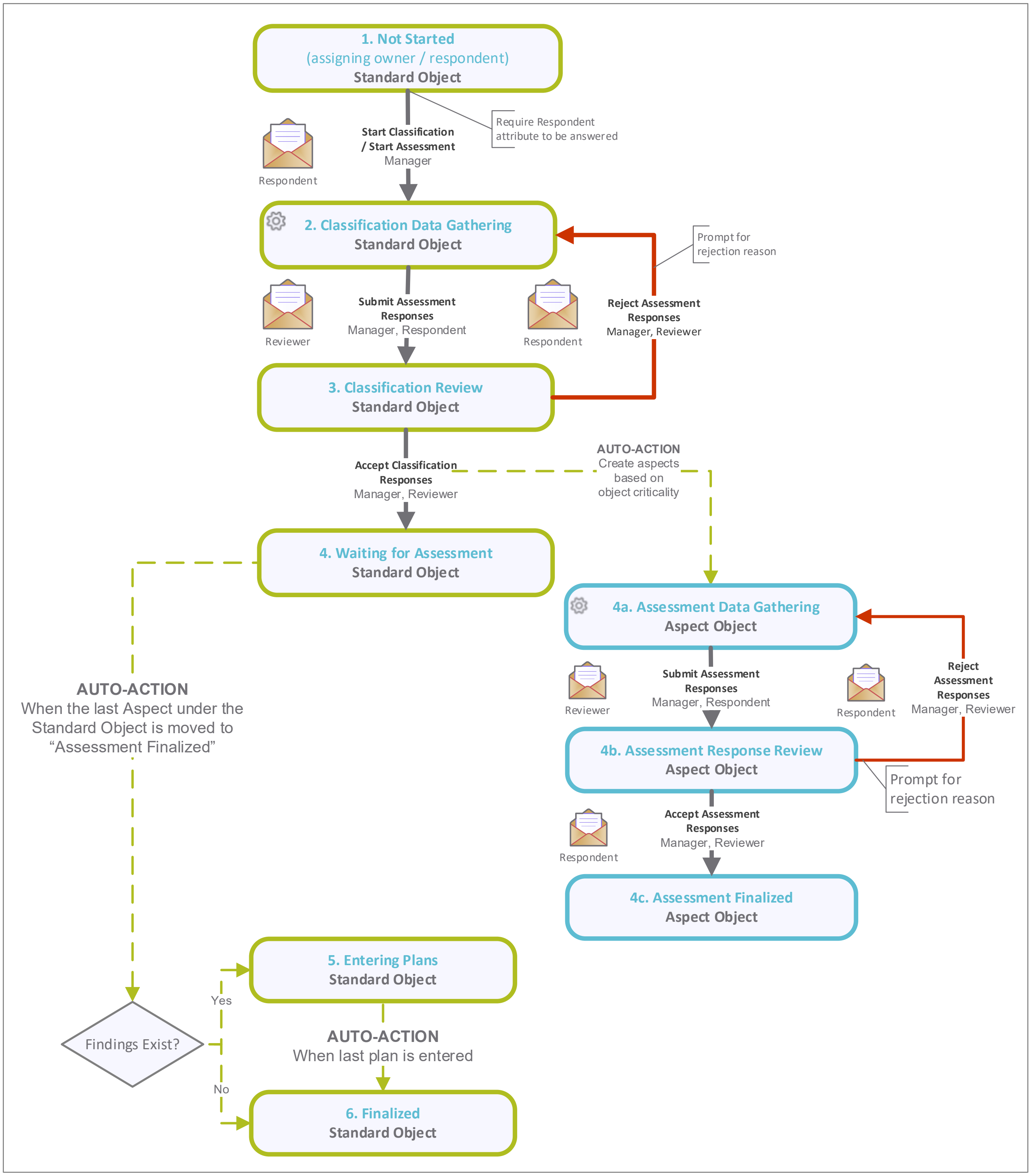
- Assessment
- Finding

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



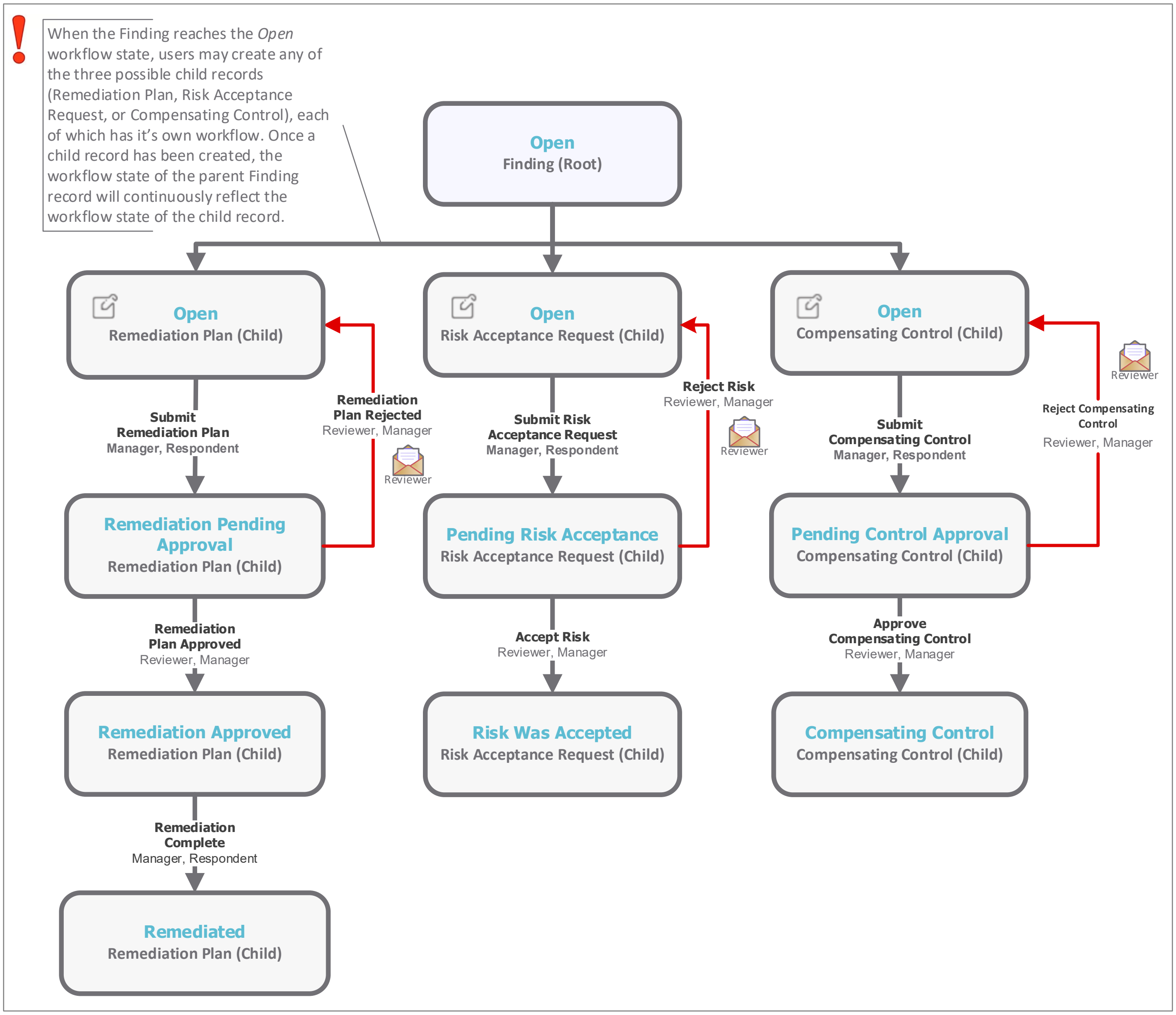
Assessment

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



Finding

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



Note: The Risk and Compliance Assessments module also provides additional roles that are specific to the questionnaire findings management process, but those roles have been omitted from the above diagram for the sake of simplicity. For more information about the QF-specific roles, refer the **Workflow Buttons** and **Workflow Roles** tables below.

User Accounts

User accounts are required for the individuals that are authorized to access a specific Rsam template. The Rsam sandbox for Assessments comes with pre-populated sample accounts as explained in the following table.

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

User 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. Typically, this user has the ability to perform all the tasks that can be done with the *Assessment Respondent* and *Assessment Reviewer* user accounts.

Users can contact *Rsam Administrator* to obtain passwords for assigned accounts. 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 IT Application	Assessment Manager	In this step, the *Assessment Manager* user creates a new object (IT Application), and then 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 then 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.
Step 4: Answering Control Assessment	Assessment Respondent	In this step, the *Assessment Respondent* user provides responses for the questions in control assessments that are created based on the classification assessment result, and then submits the control responses for review.
Step 5: Reviewing Control Assessment Responses	Assessment Reviewer	In this step, the *Assessment Reviewer* user reviews and accepts the control assessment responses.
Step 6: Creating and Submitting the Remediation Plan	Assessment Respondent	In this step, the *Assessment Respondent* user creates a remediation plan for each questionnaire finding.
Step 7: Reviewing and Approving the Remediation Plan	Assessment Reviewer	In this step, the *Assessment Reviewer* user reviews and approves remediation plans.
Step 8: Flagging 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 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 (IT Application), initialize an assessment for that object, answer and review the classification and control assessments, and remediate weak/failed controls. This path was chosen as it is a common path to follow, though you are welcome to explore the other paths as well.

From this point forward, we will provide the steps that are required to complete this tutorial. Before you begin to practice each step, consider following underlying capabilities:

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 PCI and Rsam Assessment 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.

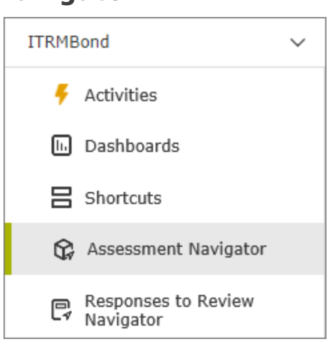
Step 1: Creating and Initializing an Object

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

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Assessments module.

2. Sign in as the *Assessment Manager* user. Enter **Username** as *r_assessment_manager* and provide the **Password**.

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

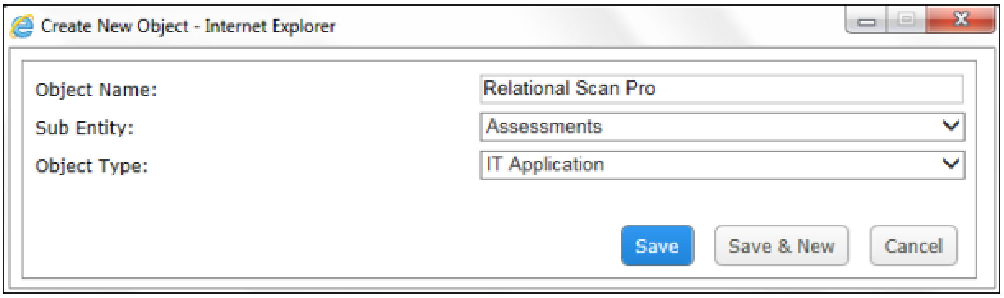


The Assessment Navigator is displayed.

4. In the Assessment Navigator, click **Add** and select **Object** from the options that appear.

   The **Create a new Object** window appears.

5. Enter an application name in the **Object Name** attribute, select **Assessments** from the **Sub Entity** list box attribute, select **IT Application** from the **Object Type** list box attribute, and then click **Save**.



   The object is created.

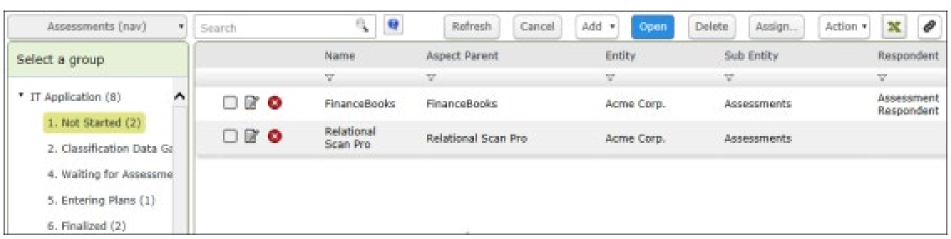
6. From within the navigation panel with **Assessments (nav)** selected, expand **IT Application** and click **Not Started**.

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

7. Locate the newly-created object.

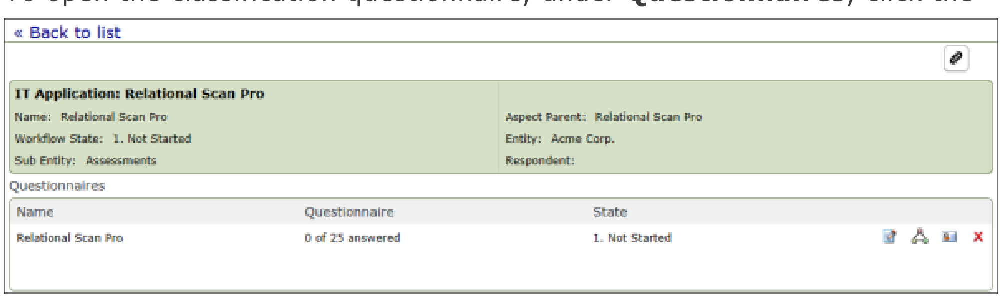
8. Use one of the following methods to open the newly-created object:

   - Double-click the object.
   - Select the object, and then click **Open**.
   - Click the icon in the object row.



   The object details are displayed.

9. To open the classification questionnaire, under **Questionnaires**, click the icon.



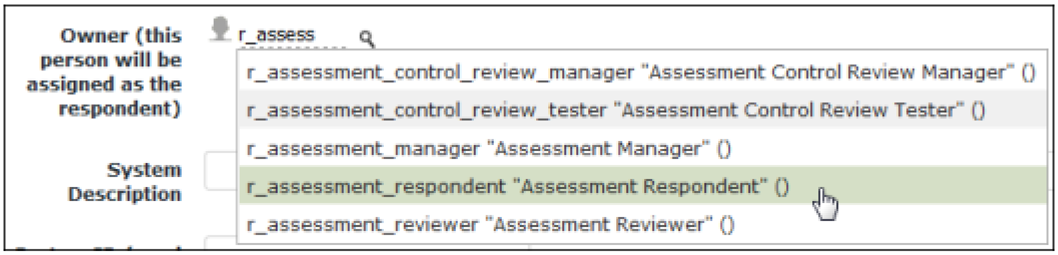
   The questionnaire details are displayed.

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

11. Specify **r_assessment_respondent** user in the **Owner (this person will be assigned as the respondent)** attribute.

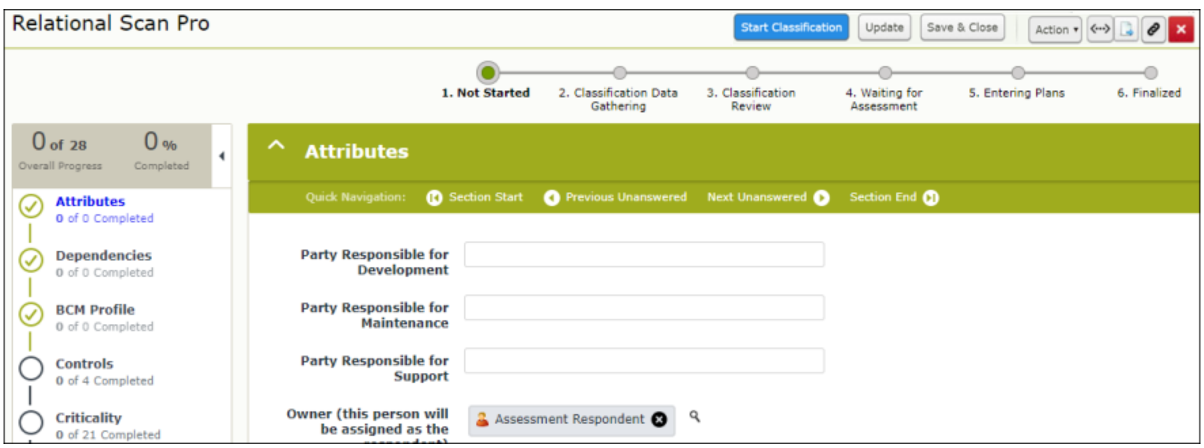
    a. Enter *r_assessment_respondent* in the **Owner (this person will be assigned as the respondent)** attribute. While typing, a list of users that match the string is shown.

    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.

12. Click **Start Classification**.



13. In the message that appears indicating that the assessment has been started and the respondent will be notified, click **OK**.

    The application object is moved to the **Classification Data Gathering** state and an email notification is sent to the *Assessment Respondent* user.

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

    You have been successfully logged out from Rsam.

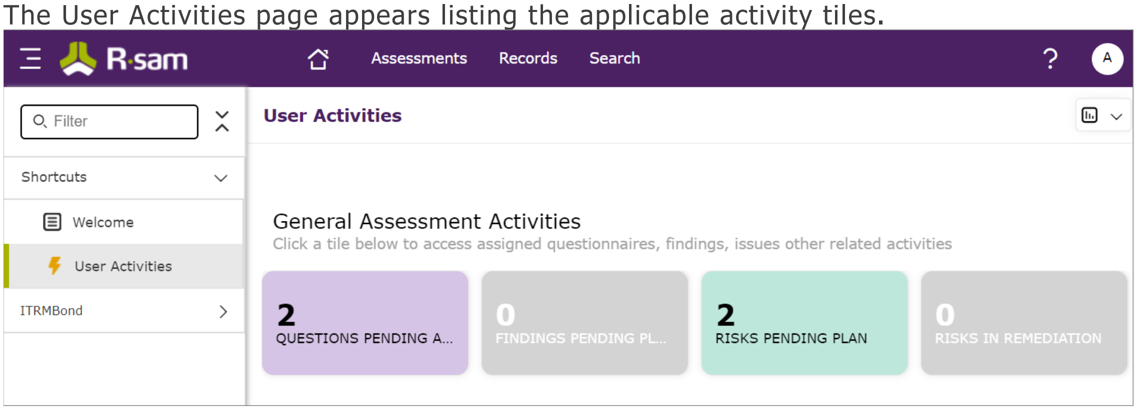
Step 2: Answering Classification Assessment Questions

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 provide the **Password**.

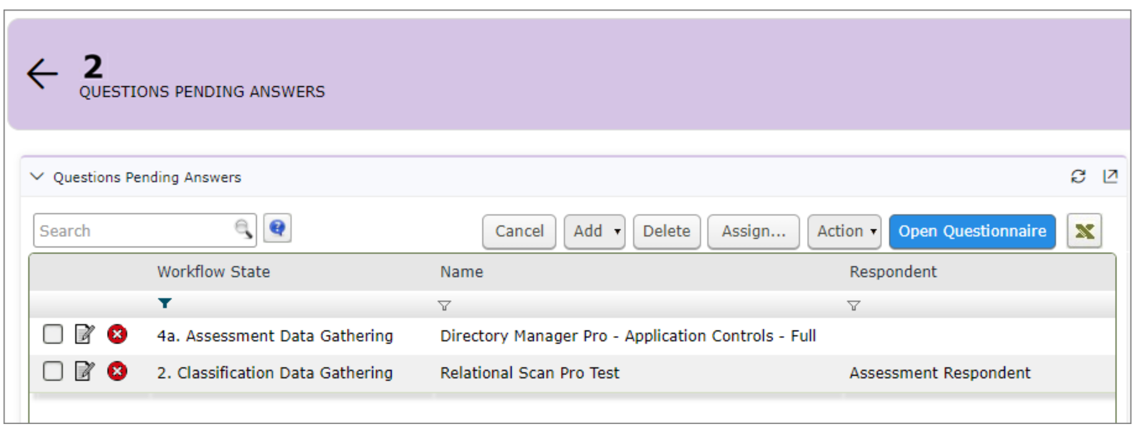
2. From within the navigation panel at the left-hand side, navigate to **Shortcuts > User Activities**.

   The User Activities page appears listing the applicable activity tiles.



3. Click the tile **Questions Pending Answers**.

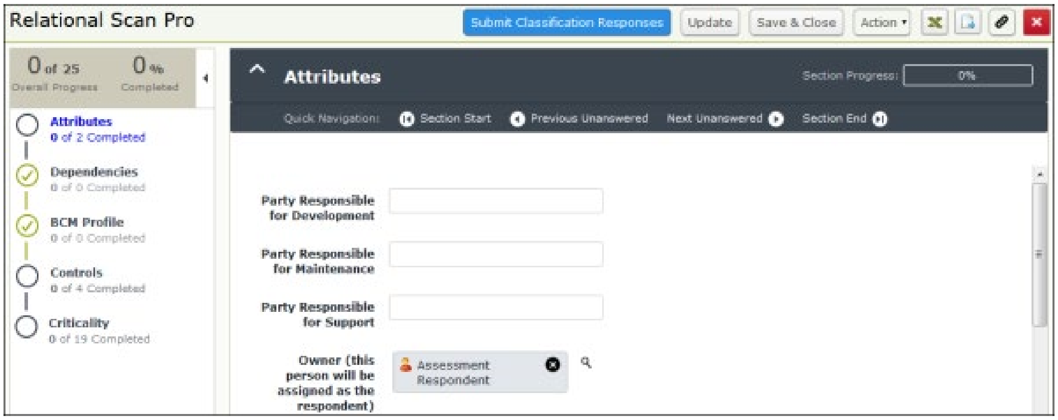
   The tile expands to display the **Questions Pending Answers** grid.



4. Locate the object created in Step 1: Creating and Initializing an Object, and then double-click the application object.

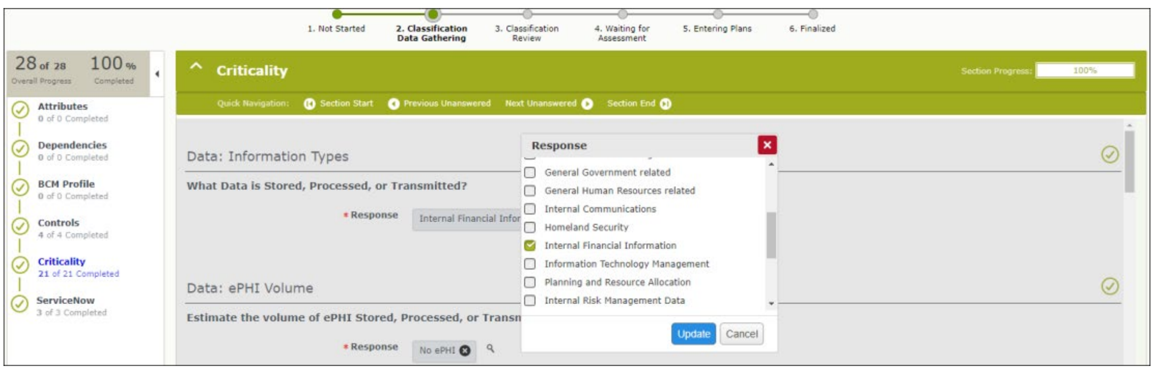
   The questionnaire opens.

5. Complete **Attributes**, **Dependencies**, **BCM Profile**, **Controls**, and **Criticality** sections in the questionnaire. The sandbox has been configured to require responses to all Control and Criticality questions.



6. Under **Criticality** > **Data: Information Types**, it is recommended to select at least one item for the following question: What Data is Stored, Processed, or Transmitted?

   Select **Internal Financial Information** as shown in the following image.



7. To fill information or responses for each section on the left-hand side of the questionnaire, use the following navigation procedure:

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

   - 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.

8. Click **Submit Classification Responses**.

9. In the message box that appears indicating that the responses have been submitted, click **OK**.

   The assessment is moved to the Classification Review state and an email notification is sent to the ***Assessment Reviewer*** user.

10. Log out from 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 provide the **Password**.

2. From within the navigation panel at the left-hand side, navigate to **ITRMBond** > **Activities**.

   The Activities page appears listing the applicable Activity Center tiles.

3. Click the tile **Pending Review**.

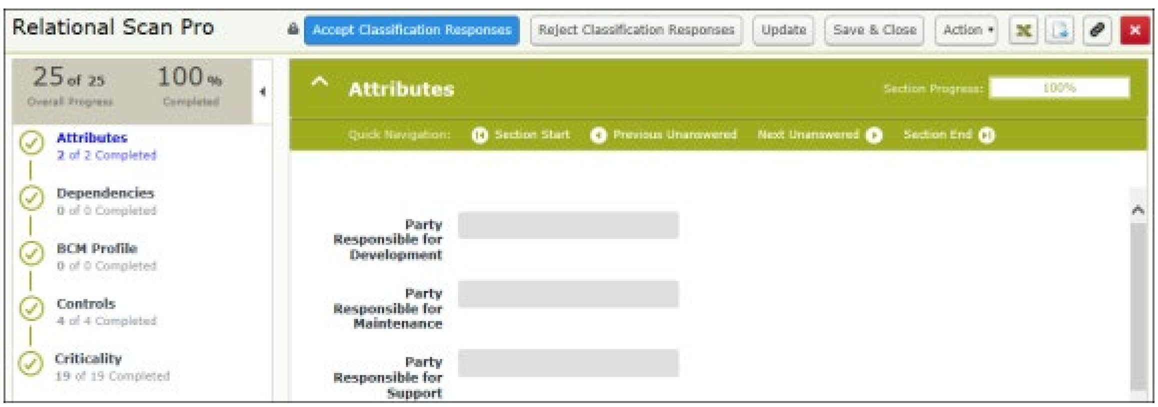
   The tile expands to display the grid containing the assessment responses pending review.

4. Locate the classification assessment submitted by the *Assessment Respondent* user in Step 2: Answering Classification Assessment Questions and double-click to open it.

   The assessment will be in the **3. Classification Review** state.

5. Review the responses in each section.

6. Click **Accept Classification Responses**.



7. In the message box that appears indicating that a full assessment has been generated, click **OK**.

   The classification data is evaluated, and then control assessments are generated automatically. Rsam generates any required aspects, or control assessment questionnaires based on the provided criticality responses. The IT Application object workflow is moved to the **Waiting for Assessment** state and an email notification is sent to the *Assessment Respondent* user.

8. Log out from Rsam.

Step 4: Answering Control Questions

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

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

2. From within the navigation panel at the left-hand side, navigate to **Shortcuts > User Activities**.

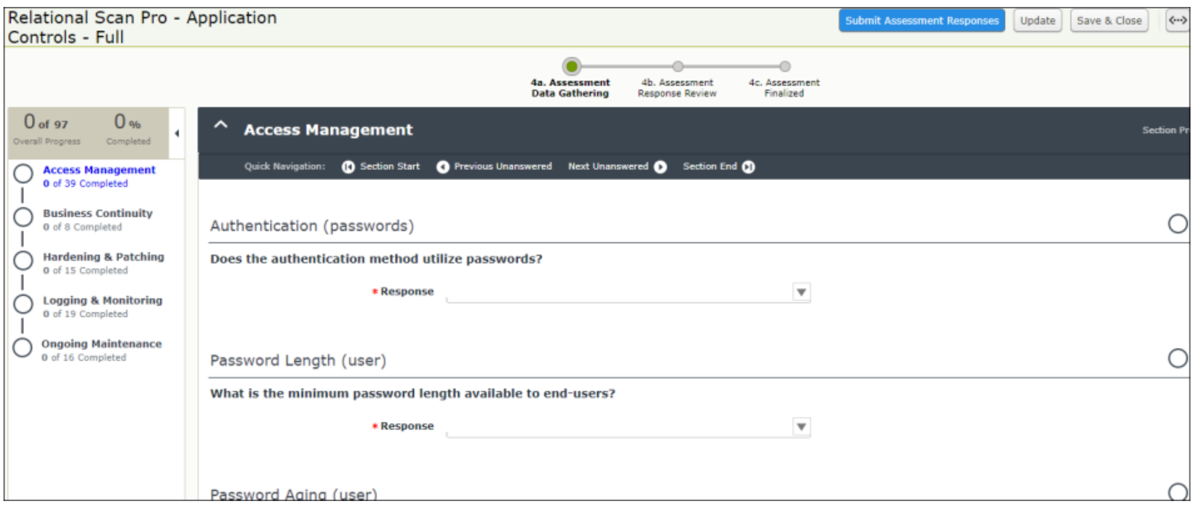
   The User Activities page appears listing the applicable activity tiles.

3. Click the tile **Questions Pending Answers**.

   The tile expands to display the grid.

4. Locate the assessments generated for the object and double-click to open it.

5. Complete all the control questions.



Notes:

- To allow for quick and easy use of this tutorial, Rsam's default configuration 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.

- If you do not answer all the control questions, a confirmation dialog box appears. Click **OK** to continue.

6. Click **Submit Assessment Responses**.

   The assessment workflow moves to the **Assessment Response Review** state and sends an email notification to the *Assessment Reviewer* user.

7. Log out from Rsam.

Step 5: Reviewing Control Answers

In this step, you 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 provide the **Password**.

2. From within the navigation panel at the left-hand side, navigate to **ITRMBond** > **Activities**.

   The Activities page appears listing the applicable Activity Center tiles.

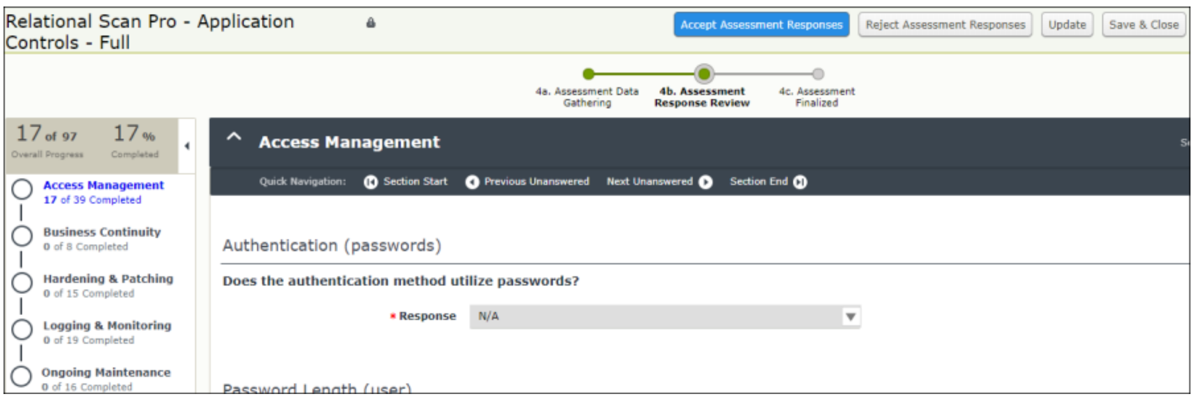
3. Click the tile **Pending Review**.

   The tile expands to display the grid containing the assessment responses pending review.

4. Locate the application assessment that was submitted by the *Assessment Respondent* user in Step 4: Answering Control Questions, which is in the Assessment Response Review state and double-click to open it.

5. Review all the control responses.

6. Click **Accept Assessment Responses**.



7. In the confirmation message box that appears indicating that Rsam will generate a series of records and whether to continue, click **OK**.

   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 control assessment workflow enters the **Assessment Finalized** state. When all the control assessments are in the Assessment Finalized workflow state, the parent assessment workflow state enters the **Entering Plans** state.

8. Log out from 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 all 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 provide the **Password**.

2. From within the navigation panel at the left-hand side, navigate to **Shortcuts** > **User Activities**.

   The User Activities page appears listing the applicable activity tiles.

3. Click the tile **Findings Pending Plan**.

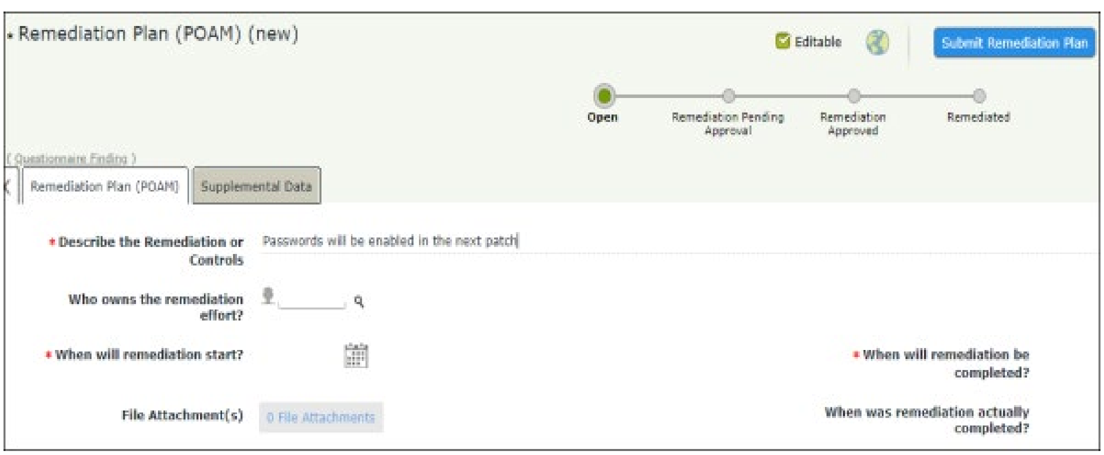
   The tile expands to display the grid.

4. Locate the application control assessment in which the control responses were reviewed by the Assessment Reviewer user in [Step 5: Reviewing Control Answers](#).

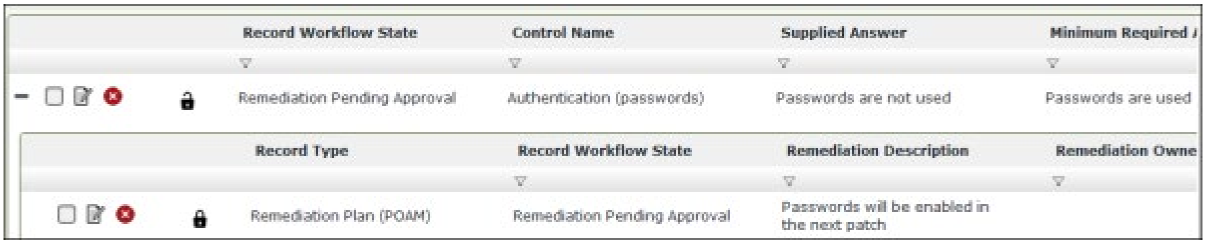
5. Select the desired finding record, click **Add** and select **Remediation Plan (POAM)** from the options that appear.

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

6. On the **Remediation Plan (POAM)** and **Supplemental Data** tabs, complete all the attributes as necessary, and then click **Submit Remediation Plan**.



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



7. Log out from Rsam.

Note: While this tutorial navigated 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 log in to Rsam as the *Assessment Reviewer* user to review and approve a remediation plan for a given questionnaire finding.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Assessments module.

2. Sign in as the *Assessment Reviewer* user. Enter **Username** as *r_assessment_reviewer* and provide the **Password**.

3. From within the navigation panel at the left-hand side, navigate to **ITRMBond** > **Questionnaire Findings Navigator**.

   The questionnaire findings navigator appears.

   Note: This step can also be accomplished through the Activity Centers when there are a small number of assessments to be reviewed.

4. From within the navigation panel with **Questionnaire Findings (nav)** selected, expand **IT Application** and click the desired object.

   The questionnaire findings appear.

5. Locate the questionnaire finding for which the Assessment Respondent user created a remediation plan in [Step 6: Creating and Submitting a Remediation Plan](#).

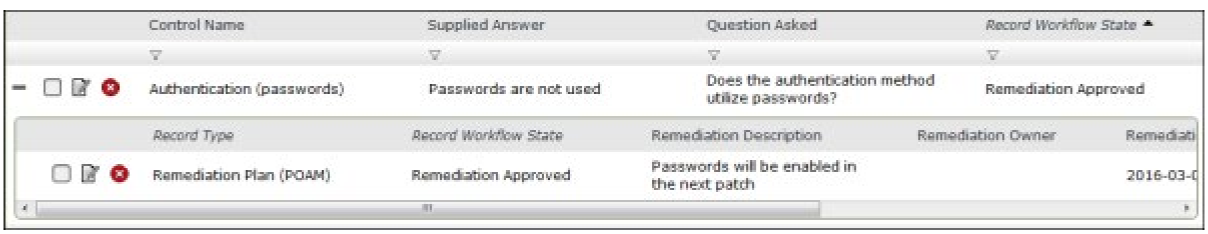
6. Click **+** in the questionnaire finding record row.

7. Use one of the following methods to open the remediation plan:
   - Double-click the remediation plan record.
   - Select the remediation plan record and click **Open**.
   - Click the edit icon in the remediation plan record row.

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

8. 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 is moved to the **Remediation Approved** state.



9. Log out from Rsam.

Step 8: Flagging Completion of a Remediation Plan

In this step, you log in to Rsam as the Assessment Manager user to flag the completion of the remediation plan (POAM) record approved by the Assessment Reviewer user.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Assessments module.

2. Sign in as the Assessment Manager user. Enter **Username** as *r_assessment_manager* and provide the **Password**.

3. From within the navigation panel at the left-hand side, navigate to **ITRMBond** > **Questionnaire Findings Navigator**.

   The questionnaire findings navigator appears.

Note: This step can also be accomplished through the Activity Centers when there are a small number of assessments to be reviewed.

4. From within the navigation panel with **Questionnaire Findings (nav)** selected, **expand IT Application** and click the desired object.

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

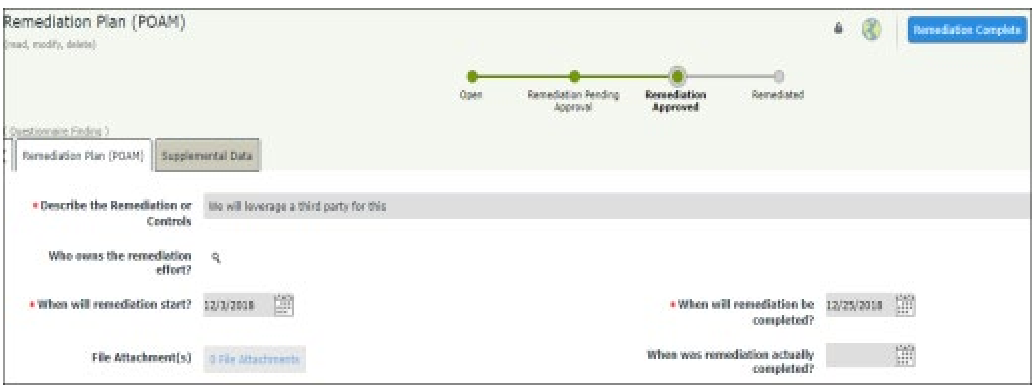
6. Click **+** in the questionnaire finding record row.

7. Use one of the following methods to open the remediation plan:

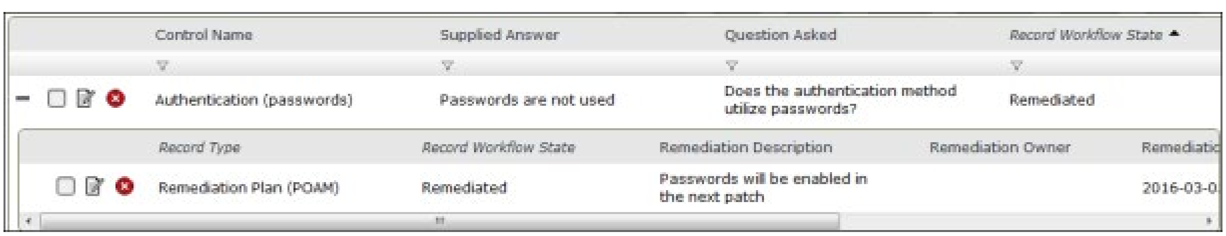
   - Double-click the remediation plan record.
   - Select the remediation plan record and click **Open**.
   - Click the edit icon in the remediation plan record row.

   The **Remediation Plan (POAM)** record with **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 is moved to the **Remediated** state.



9. Log out from Rsam.

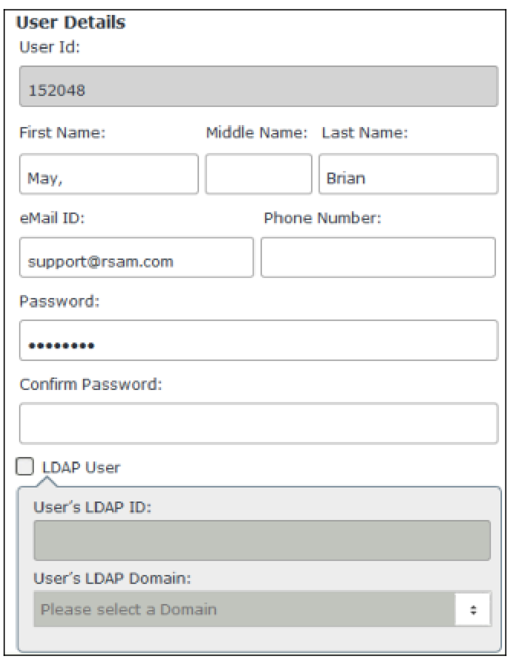
Appendix 1: Email Notifications and Offline Decision Making

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 Risk and Compliance Assessment Module module.
2. Sign in as *r_admin* user. Enter **User ID** as ***r_admin*** and provide the **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.



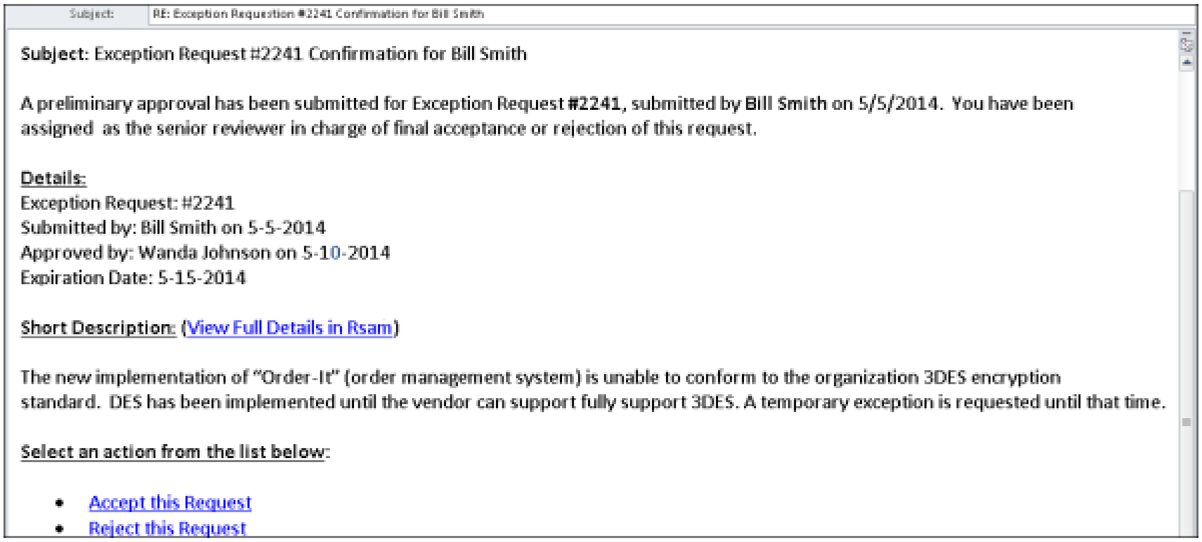
6. Click **OK**.

   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.



Subject: RE: Exception Requestion #2241 Confirmation for Bill Smith

Subject: Exception Request #2241 Confirmation for Bill Smith

A preliminary approval has been submitted for Exception Request **#2241**, submitted by **Bill Smith** on 5/5/2014. You have been assigned as the senior reviewer in charge of final acceptance or rejection of this request.

Details:
Exception Request: #2241
Submitted by: Bill Smith on 5-5-2014
Approved by: Wanda Johnson on 5-10-2014
Expiration Date: 5-15-2014

Short Description: (View Full Details in Rsam)

The new implementation of "Order-It" (order management system) is unable to conform to the organization 3DES encryption standard. DES has been implemented until the vendor can support fully support 3DES. A temporary exception is requested until that time.

Select an action from the list below:

- Accept this Request
- Reject this Request

Appendix 2: Rsam Documentation

Risk and Compliance Assessment Module Baseline Configuration Guide

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

Online Help

This tutorial provides the step-by-step instructions for the Rsam Risk and Compliance Assessment 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 **User ID** as ***r_admin*** and provide the **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.