



Enterprise Policy Management Module

Step-by-Step Tutorial

Document Version: 02.01.02 | December 2018

Rsam © 2018. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

Contents

About Rsam Tutorials	3
Rsam Sandbox Environment	4
Sign-In Page.....	4
Enterprise Policy Management	5
Enterprise Policy Management Workflows	5
Policy, Section and Sub-Section Workflow.....	6
Policy Acknowledgement Campaign Workflow	7
Campaign Acknowledgement Record Workflow.....	7
Policy User Accounts	8
High-Level Steps	9
Policy Management	10
Step 1: Updating and Submitting a Policy	10
Step 2: Reviewing and Approving Policy Revisions.....	12
Step 3: Publishing a Policy	13
Step 4: Comparing Policies in Draft and Published States.....	14
Active Policies.....	15
Step 1: Viewing Policies.....	15
Step 2: Associating Exceptions to Policies	16
Step 3: Attesting Policies	18
Campaign Management	20
Campaign User Accounts.....	20
Step 1: Creating a Campaign	21
Step 2: Reviewing and Approving a Campaign.....	26
Step 3: Acknowledging a Policy - Target Audience	26
Step 4: Completing a Policy Acknowledgement Campaign	28
Appendix 1: Email Notifications	29
Appendix 2: Offline Decision Making.....	30
Appendix 3: Rsam Documentation	31
EPM Baseline Configuration Guide.....	31
Online Help	31

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.

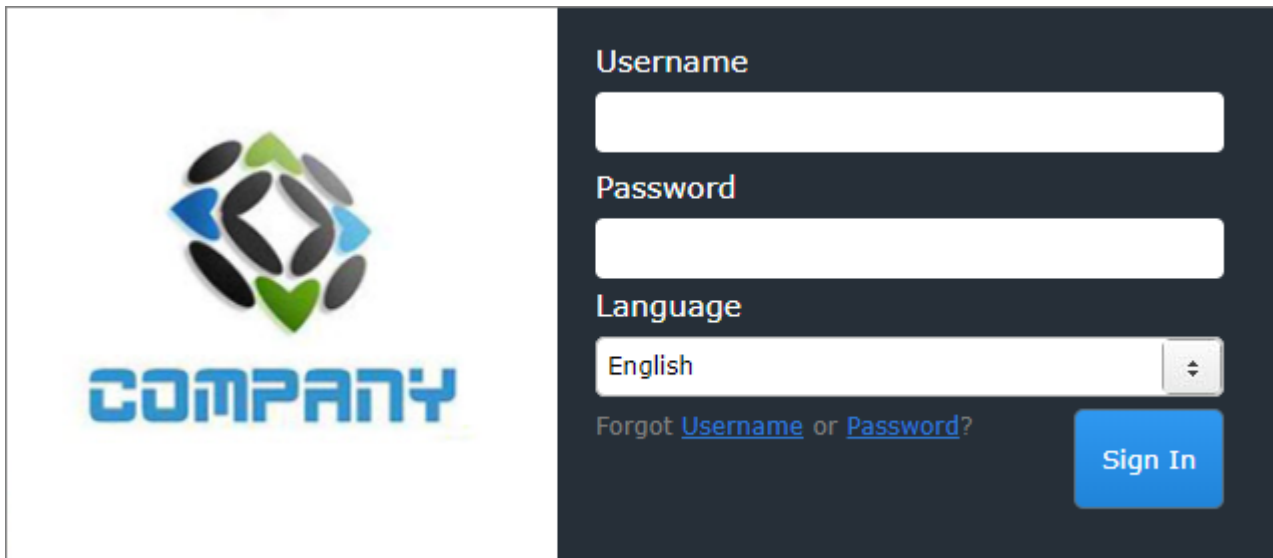
Rsam Sandbox Environment

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.



The image shows a sign-in page for Rsam. On the left side, there is a logo consisting of a circular arrangement of colored shapes (green, blue, grey) above the word "COMPANY" in a blue, stylized font. On the right side, there is a dark grey form with the following elements: a "Username" label above a white input field; a "Password" label above another white input field; a "Language" label above a dropdown menu currently showing "English"; a link "Forgot Username" and a link "Forgot Password" below the language dropdown; and a blue "Sign In" button at the bottom right of the form.

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.

Enterprise Policy Management

The Rsam Enterprise Policy Management module allows you to author, manage, and track policies in a central location. It provides organizations with the ability to map their policies to the regulatory standards and frameworks. With versioning mechanism in the Enterprise Policy Management module, organizations can track policy changes effectively. This tutorial provides a step-by-step procedure to walk you through the commonly followed path of an Enterprise Policy Management workflow within the module.

The Enterprise Policy Management module has the following capabilities and benefits:

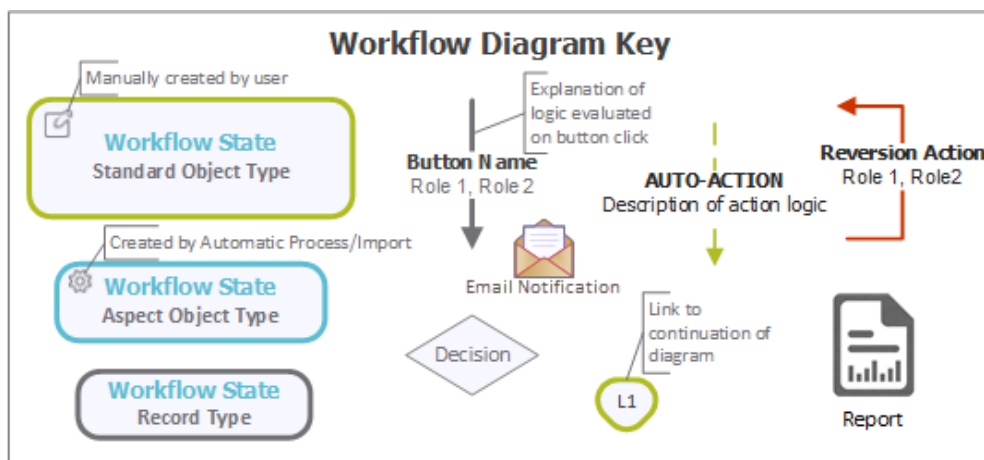
- Create, track, approve, manage, and version all policies in a central location.
- Author policies manually in Rsam, or import policy text.
- Ability to map policies to risks, controls, and exceptions.
- Manage policy reviews and approval using an automated workflow process.
- Create policy acknowledgment campaigns to specifically targeted audiences.

Enterprise Policy Management Workflows

The Enterprise Policy Management module provides automated workflows for the following components:

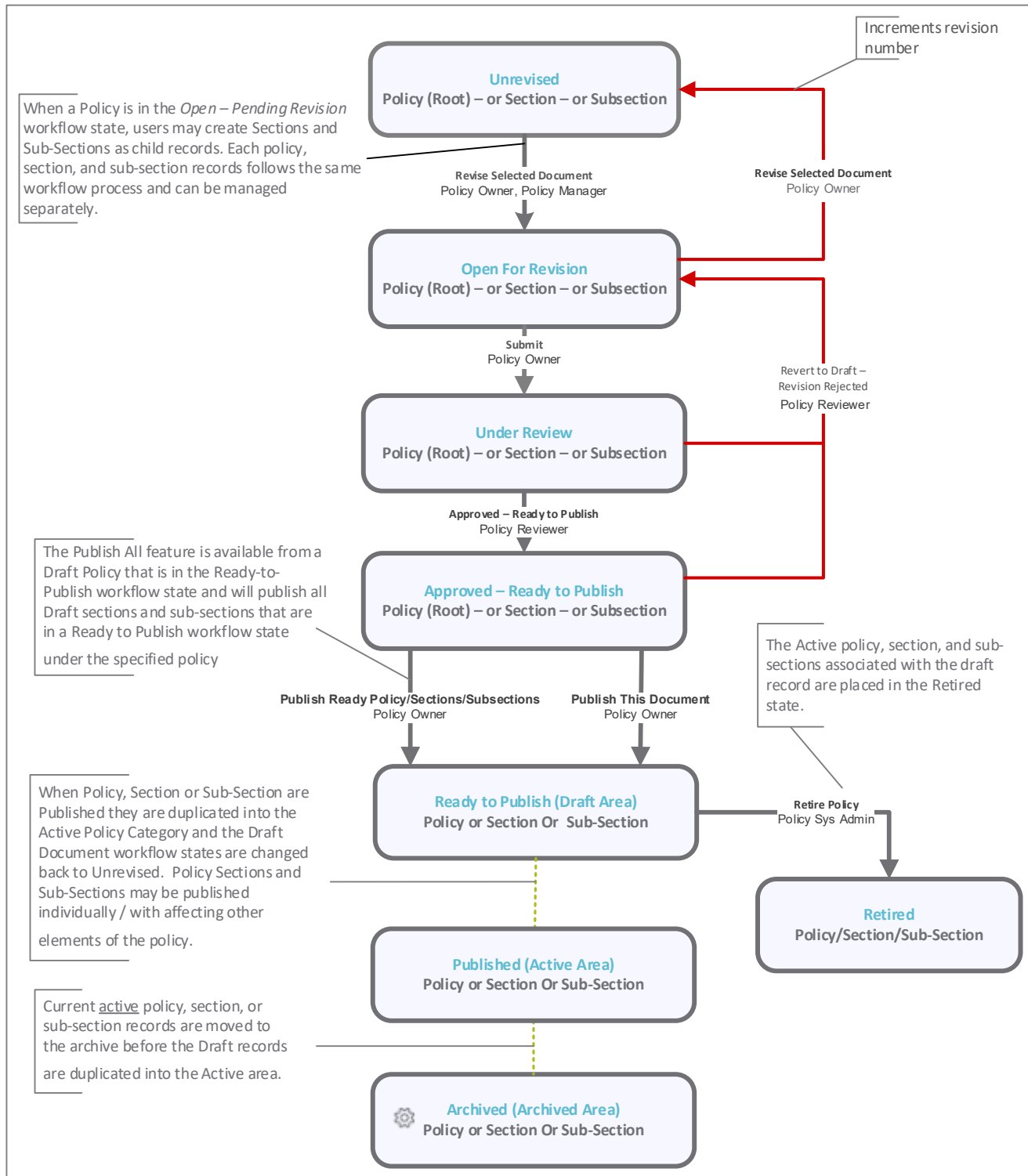
- Policy, Section and Sub-Section
- Policy Acknowledgement Campaign
- Campaign Acknowledgement Record

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



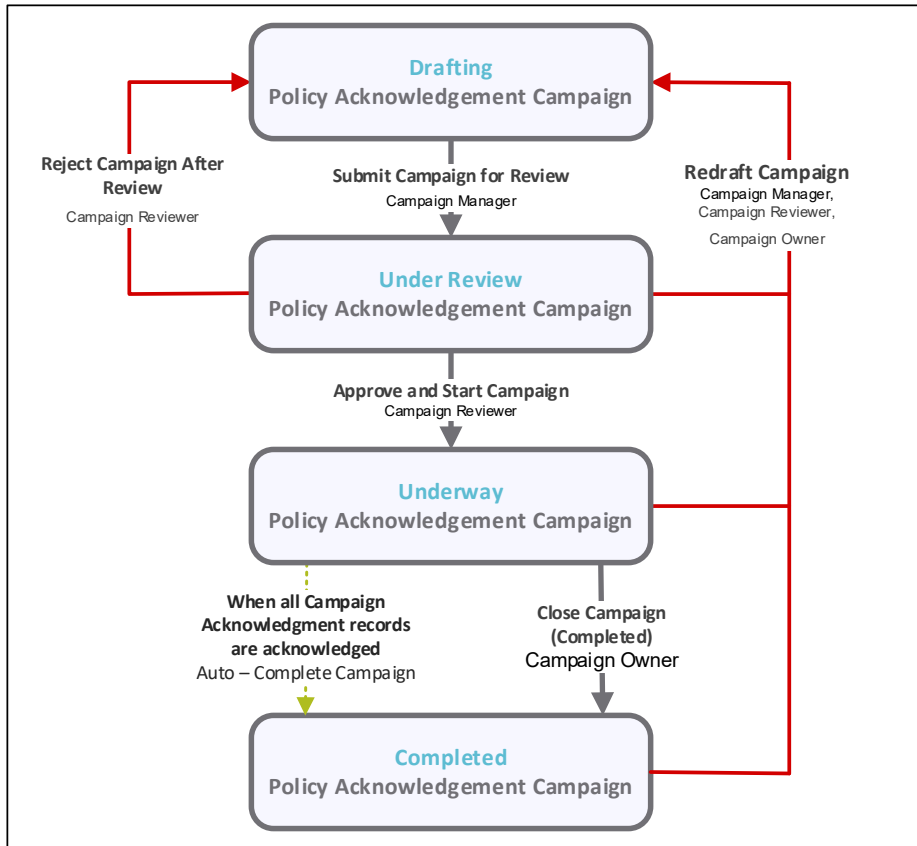
Policy, Section and Sub-Section Workflow

The following image shows the workflow of the baseline Policy, Section and Sub-Section.



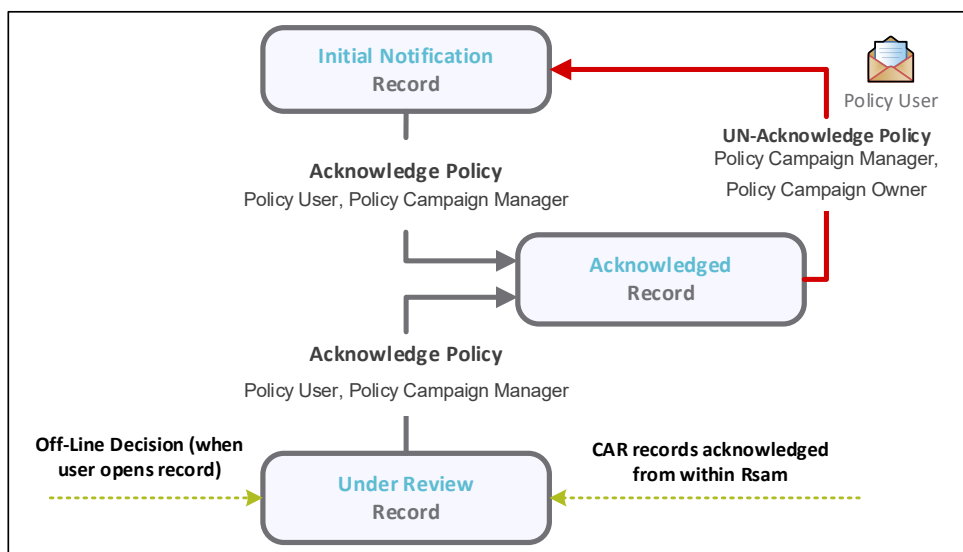
Policy Acknowledgement Campaign Workflow

The following image shows the workflow of the baseline Policy Acknowledgement Campaign.



Campaign Acknowledgement Record Workflow

The following image shows the workflow of the baseline Campaign Acknowledgement Record.



Policy User Accounts

User Accounts are required for the individuals that are authorized to access a specific Rsam baseline module. The Rsam sandbox for Enterprise Policy Management comes with pre-populated sample accounts as listed in the following table.

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

Account ID	User	Business Responsibilities
r_policy_manager	Policy Manager	This user has the responsibility to create Policy Groups and may create new policies. The Policy Manager assigns Policy Owners to each policy and may also assign Policy Reviewers to each policy. Policy Managers may create and submit exception requests.
r_policy_owner	Policy Owner	This user has the responsibility to update and submit policies for review, and to publish policies. Policy Managers may make the initial assignments of Policy Owners for each policy and Policy Owners may assign Policy Reviewers. Policy Owners may create and submit exception requests. Once exception requests are approved, the users may align exception to Policies, Policy Sections, and Policy Subsections.
r_policy_reviewer	Policy Reviewer	This user has the responsibility to approve policies and are generally assigned to policies by Policy Owners.
r_exception_submitter	Exception Submitter	This user has the responsibility to create and submit exception requests in Rsam Exception.
user_id	Policy User	This user logs into Rsam using their own User ID and a one-time password that is provided by Rsam. These user accounts are provided for the purpose of acknowledging policies and have very limited access to other Rsam features.

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

Note: Some user accounts may be created as part of a policy campaign where the accounts did not already exist in Rsam. A hashed one-time password is automatically generated for such user accounts. The users are then provided with a one-time login password through email. When users log in to Rsam using their Rsam one-time password, they will be required to change the password before continuing.

High-Level Steps

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

Step	User	Description
Step 1: Updating and Submitting a Policy	Policy Owner	In this step, a policy is updated and submitted for review.
Step 2: Reviewing and Approving Policy Revisions	Policy Reviewer	In this step, the policy, section, or subsection is reviewed and approved.
Step 3: Publishing a Policy	Policy Owner	In this step, the policy is published.
Step 4: Comparing Policies in Draft and Published States	Policy Owner	In this step, the draft policy is compared against a published policy to view the changes.

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

Step	User	Description
Step 1: Creating a Campaign	Campaign Manager	In this step, a campaign is created, policies and notification are set, and audience criteria is defined.
Step 2: Reviewing and Approving a Campaign	Campaign Reviewer	In this step, the campaign is reviewed and approved.
Step 3: Acknowledging a Policy by Target Audience	Target Users	In this step, the target users acknowledge the policy.
Step 4: Completing a Policy Acknowledgement Campaign	Campaign Owner	In this step, the campaign is marked Completed.

Policy Management

Policy management involves the process of updating, submitting, reviewing, approving, and publishing policies, sections, or subsections in the Enterprise Policy Management module.

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

- Performing each step requires a different user account. However, you may execute all the steps with the Policy Manager user credentials in one session if desired.
- Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your workflow users receive the notifications while practicing the steps, please see the [Setting up Email Addresses](#) section later in this tutorial.

This chapter explains the following topics:

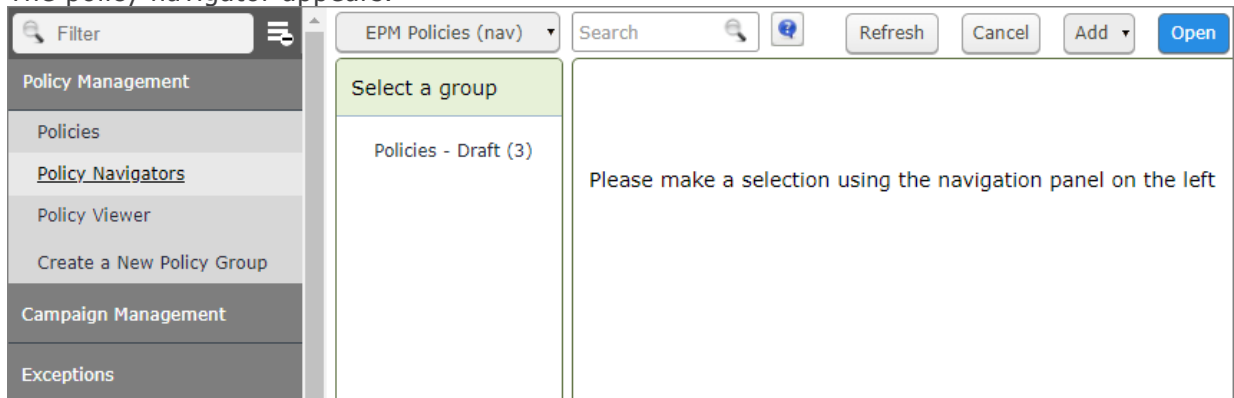
- [Updating and Submitting a Policy](#)
- [Reviewing and Approving Policy Revisions](#)
- [Publishing a Policy](#)
- [Comparing Policies in Draft and Published States](#)

Step 1: Updating and Submitting a Policy

To update and submit a policy for review, perform the following steps:


1. Open an Rsam supported browser and provide the URL of your Rsam instance containing the Enterprise Policy Management module.
2. Sign in as the *Policy Owner* user. Provide the **Username** as *r_policy_owner* and **Password** as *password*.
3. From the navigation panel on the left side, navigate to **Policy Management > Policy Navigators**.

The policy navigator appears.








4. From the policy navigator, with **EPM Policies (nav)** selected, click **Policies - Draft (x)**. The policies in the **Draft** category appear in the list.
5. Click **+** icon corresponding to the required group to expand and view the related policies, sections, and sub-sections.

Group or Organization						
Information Technology						
Workflow State	Policy Name	Version	Last Revision Date	Policy ID	Policy Document	
Open For Revision	00 Introduction	V1.3	2018-08-24	PID-00		
Workflow State	Section Name	Version	Last Revision Date	Section ID		
Unrevised	01 Organizational Policy	V1.3	2018-08-24	SID-00-01		
Workflow State	Sub-Section Name	Version	Last Revision Date	Sub-Section ID		
Approved - Ready to Publish	01 Policy Document	V1.4	2018-09-03	SSID-00-01-01		
Unrevised	02 Review of Policy Document	V1.3	2015-07-06	SSID-00-01-02		

6. To open the required policy or section record, perform any *ONE* of the following step:
 - Double-click the record.
 - Select the record and click **Open**.
 - Click the  icon in the record row.

The **Policy Sub-Section** record opens with the **Policy Sub-Section** tab selected. On opening a section or sub-section record, all attributes are in the read-only mode.

Policy Sub-Section
(read, modify)

Show Redlining |  | [Revise Selected Document](#) | Action |  |  |  | 

Unrevised
Open For Revision
Under Review
Approved - Ready to Publish
Published

Policy Sub-Section | Related Exceptions | References | Archives | Discussion / Thread

Sub-Section Name 02 Review of Policy Document	Creation Date 01/10/2014
Sub-Section ID SSID-00-01-02	Date last revision was submitted 06/07/2015
Version V1.3	Last Publish Date 06/07/2015

Sub-Section Text

[Organization] shall have an information security policy with a designated owner who has approved management responsibility. The owner will be responsible for the development, review, and evaluation of the policy. [Organization]'s environment, business circumstances, technical environment, and legal considerations will be applied during the review of the policy to manage information security. All reviews will be conducted according to defined procedures and on a pre-determined schedule or when significant changes occur. Reviews shall include information from:

- 1) interested parties;
- 2) results from independent reviews;
- 3) status/results of preventive and corrective actions;
- 4) previous management review results;
- 5) information security compliance;
- 6) performance of processes;
- 7) changes to [Organization]'s approach to managing information security;
- 8) industry trends to address threats and vulnerabilities;
- 9) documented incidents; and
- 10) recommendations by relevant authorities.

7. To edit the attributes in a section or sub-section record, click **Revise Selected Document**. The record becomes editable and the policy moves to the **Open for Revision** state from an Unrevised state.

8. Make updates to the attributes as required.

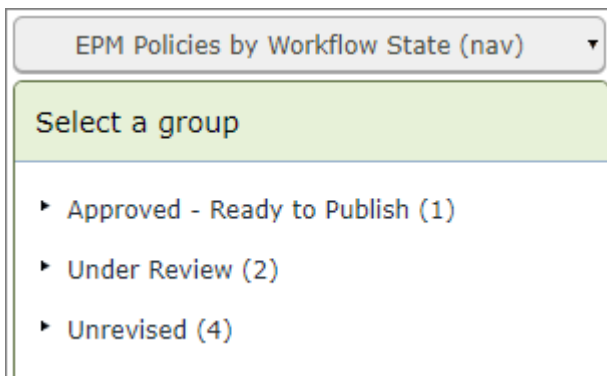
9. After making all changes, click **Submit**.

The policy sub-section record moves to the **Under Review** workflow state and an email notification is sent to the *Policy Reviewer*.

Step 2: Reviewing and Approving Policy Revisions

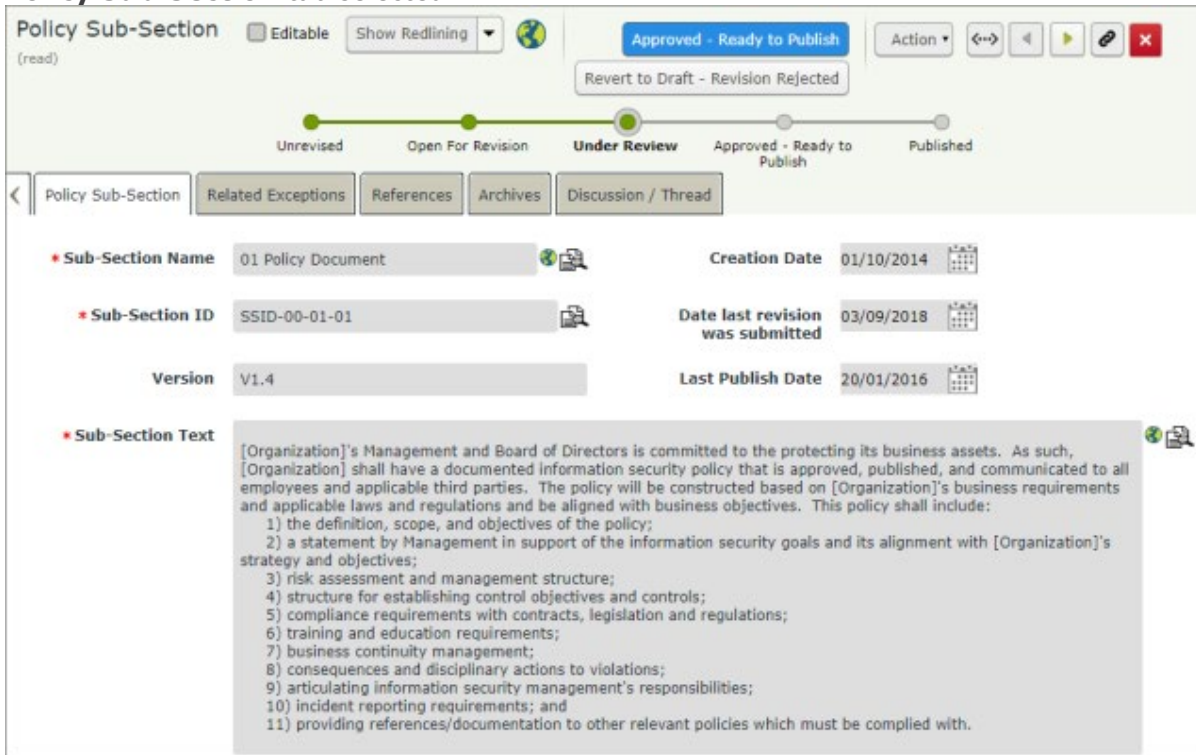
A Policy Reviewer must review and approve the policy, section, or subsection before the record can be published. To review and approve the policy, section, or subsection revisions, perform the following steps:

1. Sign in as the *Policy Reviewer*. Provide the **Username** as *r_policy_reviewer* and **Password** as *password*.
2. From the navigation panel on the left side, navigate to **Policy Management > Policy Navigators**.
The policy navigator appears.
3. Select **EPM Policies by Workflow State (nav)** to view the list of policies grouped by their individual workflow states. The policies listed are those to which the reviewer is assigned.
4. Select the **Under Review** group.



The policy records in the **Under Review** workflow state appear on the right pane.

5. Select a policy to approve and open the record. The **Policy Sub-Section** record opens with the **Policy Sub-Section** tab selected.



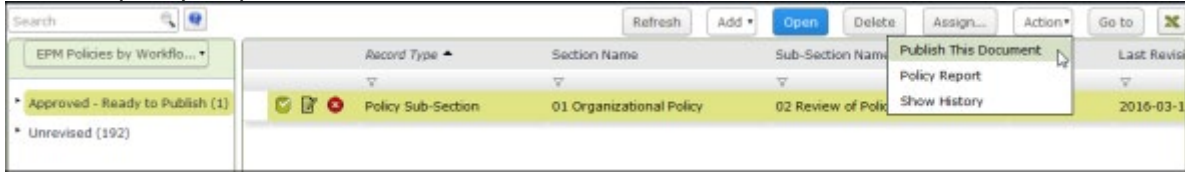
6. Review the information in the policy.
7. Click **Approved - Ready to Publish**.
The record moves to the **Approved - Ready to Publish** state.

Step 3: Publishing a Policy

A Policy Owner can publish policy records individually or in groups. To publish a policy, perform the following steps:

1. Sign in as the *Policy Owner* user. Provide the **Username** as *r_policy_owner* and **Password** as *password*.
2. From the navigation panel on the left side, navigate to **Policy Management > Policy Navigators**.
The policy navigator appears.
3. Select **EPM Policies by Workflow State (nav)** to view the list of policies grouped by the workflow states. The policies listed are those to which the owner is assigned.
4. Click **Approved - Ready to Publish**.
The policy records in the **Approved - Ready to Publish** workflow state appear on the right pane.

5. Select a policy to publish and click **Action > Publish This Document**.



6. Click **OK** in the dialog that appears stating that the policy record will be moved to the active policy area.

The draft policy is published by duplicating the draft policy into the **Policies - Active** area and then resets the draft policy to the **Unrevised** workflow state.

Step 4: Comparing Policies in Draft and Published States

The redlining feature in Rsam enables stakeholders to compare draft policy modifications made throughout the history of the policy, section, or subsection. To compare policy updates, perform the following steps:

1. Sign in as the *Policy Owner* user. Provide the **Username** as *r_policy_owner* and **Password** as *password*.
2. From the navigation panel on the left side, navigate to **Policy Management > Policy Navigators**.
The policy navigator appears.
3. Select **EPM Policies by Category (nav)** to view the list of policies grouped by the states, to which the owner is assigned by workflow.
4. Click **Policies - Draft**.
The policy records in the **Draft** workflow state appear on the right pane.
5. Double-click and open a policy or sub-section record.
6. Click the down arrow corresponding to the **Show Redlining** field.
The **Compare Against** dialog opens.
7. Select **Milestone** from the drop-down list.
8. From the second drop down list that appears, select a required milestone value.
The record refreshes to show the updated values against the selected milestone.

Note: A milestone is created each time a policy, section, or subsection is published, enabling users to easily compare the history of draft documents from the current state to the point where they are published.

Active Policies

Active policies can be viewed or searched online through the Rsam interface. Policies can also be referenced from other Rsam records, such as exception request, risk, audit finding, and more.

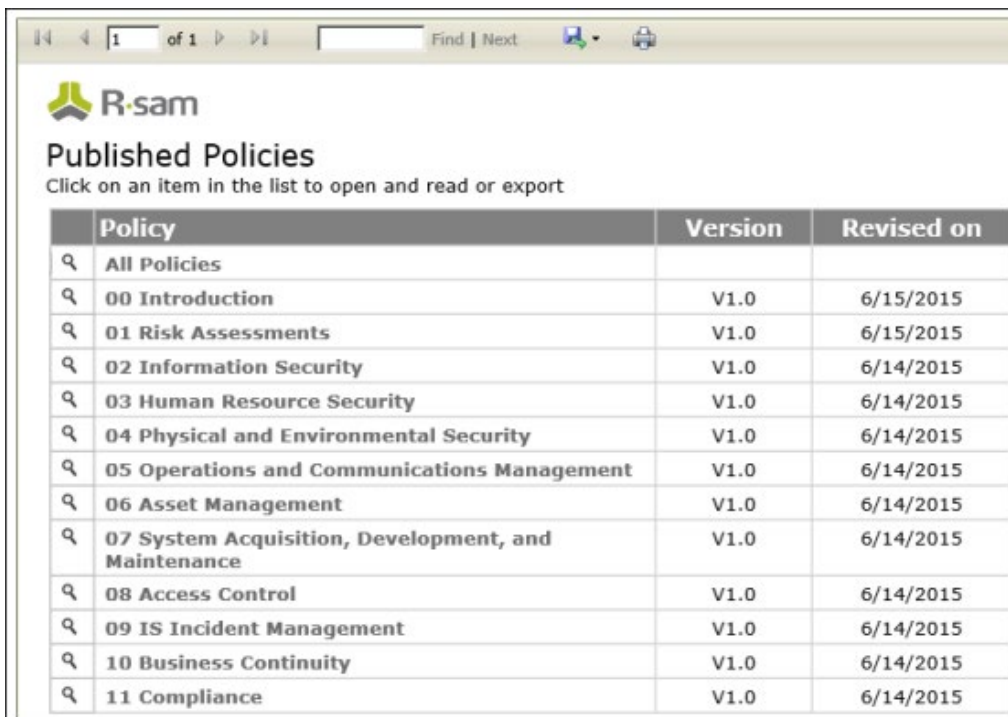
This chapter explains the following topics:

- [Viewing Policies](#)
- [Associating Exceptions to Policies](#)
- [Attesting Policies](#)

Step 1: Viewing Policies

Rsam includes a policy viewer feature that transforms the approved and published policies into a document format. This can be reviewed on-screen, or exported to Word, PDF, HTML, and more. Here, users can also acknowledge that they have read the policies (discussed in the [Attesting Policies](#) section).

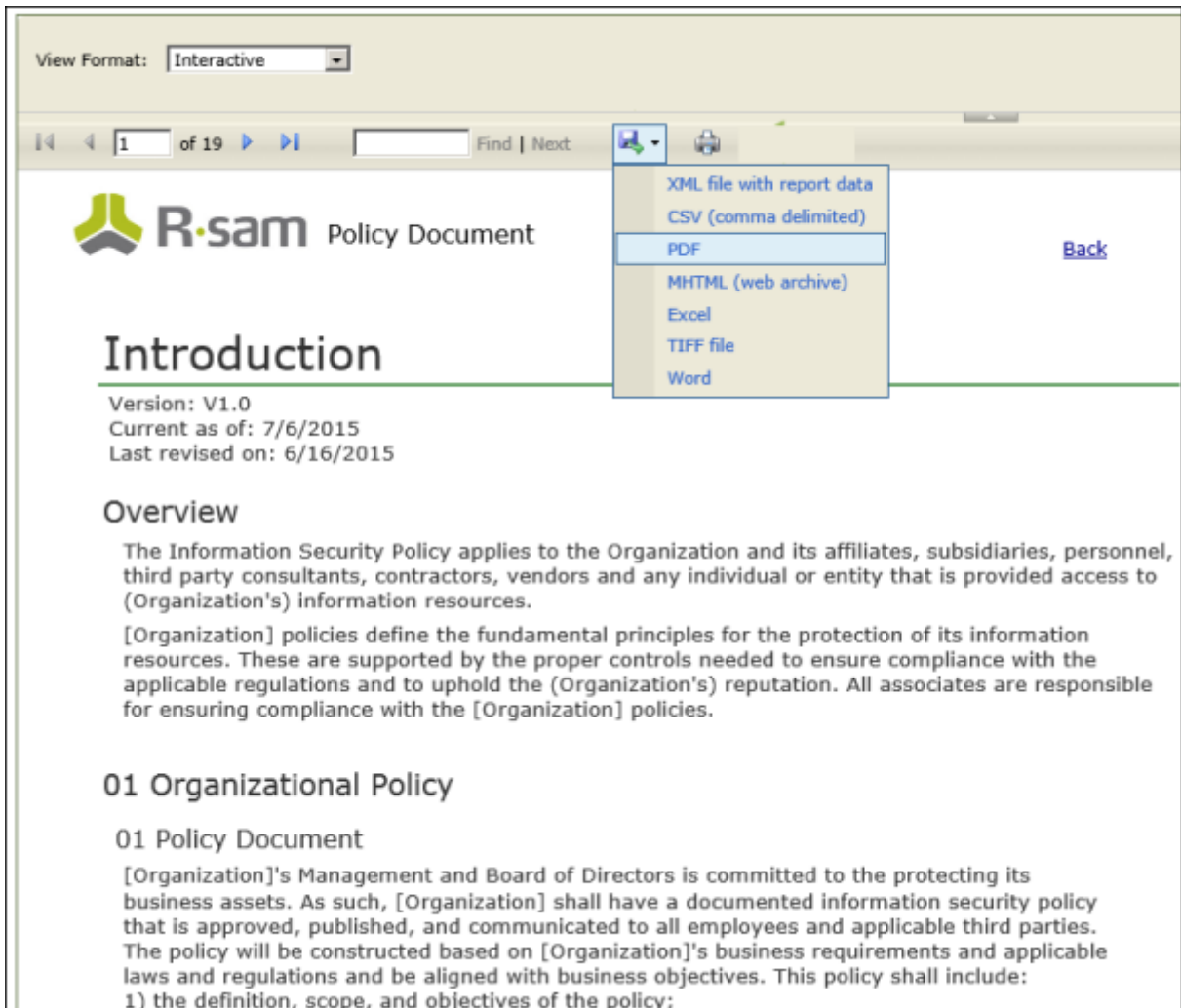
1. Sign in as the *Policy User* user. Enter **Username** as *r_policy_user* and **Password** as *password*.
2. From within the navigation panel at the left-hand side, navigate to **Policy Management > Policy Viewer**.
3. Click the **00 Introduction** policy.



The screenshot shows the R-sam interface for viewing published policies. At the top, there is a navigation bar with a search box containing '1 of 1' and a 'Find | Next' button. Below the navigation bar is the R-sam logo and the title 'Published Policies'. A instruction reads: 'Click on an item in the list to open and read or export'. The main content is a table with three columns: 'Policy', 'Version', and 'Revised on'. The table lists 12 policies, each with a magnifying glass icon in the first column. The policies are: All Policies, 00 Introduction, 01 Risk Assessments, 02 Information Security, 03 Human Resource Security, 04 Physical and Environmental Security, 05 Operations and Communications Management, 06 Asset Management, 07 System Acquisition, Development, and Maintenance, 08 Access Control, 09 IS Incident Management, 10 Business Continuity, and 11 Compliance. All policies have a version of V1.0 and were revised on 6/14/2015, except for 'All Policies' which has no version or date listed.

	Policy	Version	Revised on
🔍	All Policies		
🔍	00 Introduction	V1.0	6/15/2015
🔍	01 Risk Assessments	V1.0	6/15/2015
🔍	02 Information Security	V1.0	6/14/2015
🔍	03 Human Resource Security	V1.0	6/14/2015
🔍	04 Physical and Environmental Security	V1.0	6/14/2015
🔍	05 Operations and Communications Management	V1.0	6/14/2015
🔍	06 Asset Management	V1.0	6/14/2015
🔍	07 System Acquisition, Development, and Maintenance	V1.0	6/14/2015
🔍	08 Access Control	V1.0	6/14/2015
🔍	09 IS Incident Management	V1.0	6/14/2015
🔍	10 Business Continuity	V1.0	6/14/2015
🔍	11 Compliance	V1.0	6/14/2015

- In the report, use pagination and search options for navigation, or export the report to an appropriate format as necessary.



The screenshot shows the R-sam Policy Document interface. At the top, there is a 'View Format' dropdown menu set to 'Interactive'. Below it, a navigation bar includes a page indicator '1 of 19', a search box, and a 'Find | Next' button. The main content area features the R-sam logo and the title 'Policy Document'. A dropdown menu is open, displaying export options: XML file with report data, CSV (comma delimited), PDF (highlighted), MHTML (web archive), Excel, TIFF file, and Word. The document content includes an 'Introduction' section with version information (V1.0, current as of 7/6/2015, last revised on 6/16/2015) and an 'Overview' section. The '01 Organizational Policy' section is also visible, starting with '01 Policy Document' and describing the organization's commitment to protecting its business assets.

Step 2: Associating Exceptions to Policies

Policy Owners can create exception records and associate those records to policies, sections, or subsections after review. Perform the following steps:

- Sign in as the *Policy Owner* user. Enter **Username** as *r_policy_owner* and **Password** as *password*.
- From the navigation panel on the left side, navigate to **Exceptions > Create a new Exception record**.

The **Exception Request (new)** record opens with the **General Request** tab selected.

★ Exception Request (new)

 Editable
Submit Request
Update
Action ▾
◀
▶
✖

General Request
Save & Close

Request ID

25

Submitted Date

★ Describe the reason or issue associated with this request

Select the domains(s) related to this request

Select the policy statements related to this request

★ Enter your justification for this request

★ Until what date is the exception necessary

★ Describe any controls that are mitigating the issue / risk


Explain how you plan to resolve the issue / risk so that this exception is no longer required

Attach any supporting files / documentation for this request




0 File Attachments

Submitter Name

3. Complete all the required attributes, and any additional attributes as necessary.

- Select the required policy sub-section(s) for which this exception applies, in the **Select the policy statements related to this request** field. Click  to select the sub-section. In the dialog box that appears, select the check box for the desired record(s) and click **Update**.

Select the policy statements related to this request ✕

Network Segregation    Refresh

Sub-Section Name	Sub-Section Text	Policy Name	Section Name
<input checked="" type="checkbox"/> 05 Network Segregation	Firewalls and routing/switching functionality shall be implemented to secure network perimeter to control access between interconnected networks. VPNs for user groups shall also be used within [Organization]. Criteria for segregation of networks shall be communicated via [Organization] access control policy and requirements and enforced via IT security.	08 Access Control	04 Network Access

Results: 27
 Records per page
 << < Page of 1 > >>
 Limit total results to:

Update
 Select All
 Clear Selection(s)
 Clear All Selection(s)
 Cancel

- Click **Submit Request** to submit the exception record for review.

Note: On submitting an Exception record for review, an *Exception Reviewer* reviews and approves the record and an *Exception Manager* provides a sign-off on the record. After the record is approved, Policy Owner can view the details of the exception.

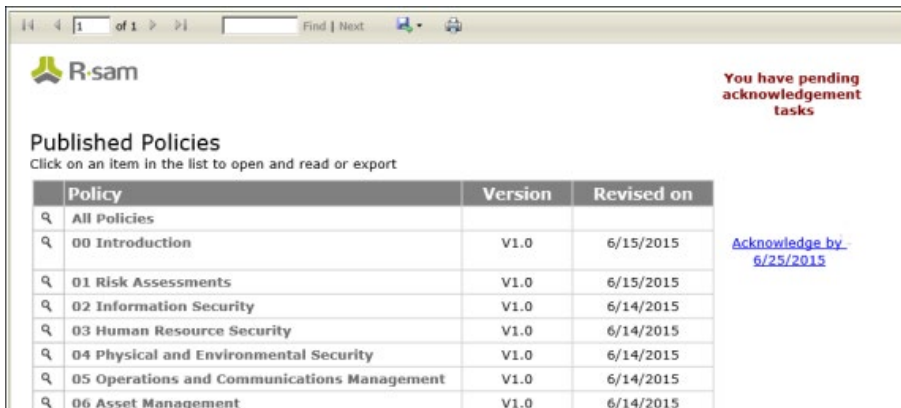
For more information on using Exceptions, refer the *Exception Management documentation*.

Step 3: Attesting Policies

Policy Attestation Campaigns are used to track user acknowledgements and awareness. In this section, the user "Cooper Jennifer" was included in a policy attestation campaign and has received an email containing Cooper Jennifer's User ID, a one-time password, a link to Rsam, and a request to log in to Rsam and attest a company policy.

- Sign in as the *Cooper Jennifer* user. Enter **Username** as **161761**.
If this is the first time that Cooper Jennifer is logging into Rsam the one-time password supplied by Rsam must be used. Once logged in, Cooper will be prompted to provide another password to replace the one-time password.
- From within the navigation panel on the left-hand side, navigate to **Policy Management > Policy Viewer**.

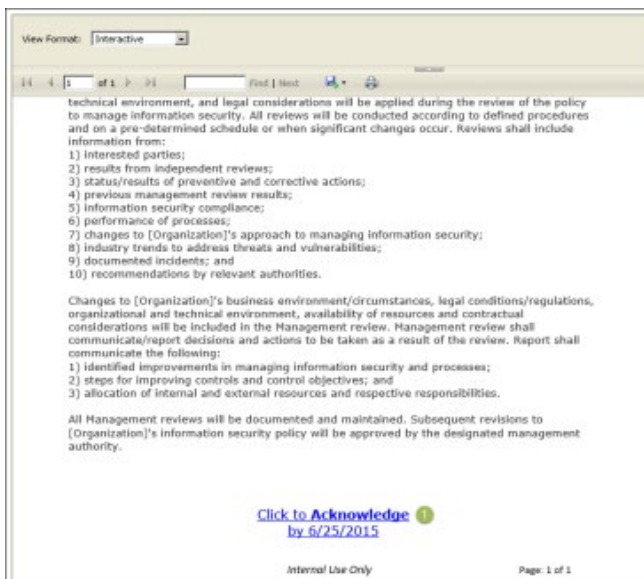
- Click the **Acknowledge by...** link next to the policy requiring attestation.



Policy	Version	Revised on
Q All Policies		
Q 00 Introduction	V1.0	6/15/2015
Q 01 Risk Assessments	V1.0	6/15/2015
Q 02 Information Security	V1.0	6/14/2015
Q 03 Human Resource Security	V1.0	6/14/2015
Q 04 Physical and Environmental Security	V1.0	6/14/2015
Q 05 Operations and Communications Management	V1.0	6/14/2015
Q 06 Asset Management	V1.0	6/14/2015

The policy document opens.

- Read the policy. At the bottom of the policy, click the **Click Here to Acknowledge** link.



technical environment, and legal considerations will be applied during the review of the policy to manage information security. All reviews will be conducted according to defined procedures and on a pre-determined schedule or when significant changes occur. Reviews shall include information from:

- 1) Interested parties;
- 2) results from independent reviews;
- 3) status/results of preventive and corrective actions;
- 4) previous management review results;
- 5) information security compliance;
- 6) performance of processes;
- 7) changes to [Organization]'s approach to managing information security;
- 8) industry trends to address threats and vulnerabilities;
- 9) documented incidents; and
- 10) recommendations by relevant authorities.

Changes to [Organization]'s business environment/circumstances, legal conditions/regulations, organizational and technical environment, availability of resources and contractual considerations will be included in the Management review. Management review shall communicate/report decisions and actions to be taken as a result of the review. Report shall communicate the following:

- 1) identified improvements in managing information security and processes;
- 2) steps for improving controls and control objectives; and
- 3) allocation of internal and external resources and respective responsibilities.

All Management reviews will be documented and maintained. Subsequent revisions to [Organization]'s information security policy will be approved by the designated management authority.

[Click to Acknowledge by 6/25/2015](#) !

Internal Use Only Page: 1 of 1

The policy is acknowledged.

Campaign Management

This section contains the workflow steps to manage campaigns in the Enterprise Policy Management module. Policies are grouped for acknowledgement purposes and campaigns determine who, what, and how policies are to be acknowledged by combining lists of users with the set of policies. Campaigns are also used to determine who participates in the process of acknowledging policies as well as the notifications used for the campaign. Campaign owners can also set the frequency in which notifications should be sent out to the target audience for the policy acknowledgments.

This chapter explains the following topics:

- [Creating a Campaign](#)
- [Reviewing and Approving a Campaign](#)
- [Acknowledging a Policy - Target Audience](#)
- [Completing a Campaign](#)

Campaign User Accounts

User Accounts are required for the individuals that are authorized to access Rsam policy campaigns. The Rsam sandbox for Enterprise Policy Management comes with pre-populated sample accounts as listed in the following table.

Account ID	User	Business Responsibilities
r_campaign_manager	Campaign Manager	This user has the responsibility of creating campaigns and assigning the owner and reviewer for the campaigns. The Campaign Manager role is assigned through group permissions by the Rsam Administrator.
r_campaign_owner	Campaign Owner	This user has the responsibility of updating campaigns, submitting campaigns for review, and maintaining the lifecycle of campaigns to which they are assigned.
r_campaign_reviewer	Campaign Reviewer	This user has the responsibility of reviewing and approving campaigns to which they are assigned.
user_id	Policy User	This user logs into Rsam using their own User ID and a one-time password that is provided by Rsam. These user accounts are provided for the purpose of acknowledging policies and have very limited access to other Rsam features.

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

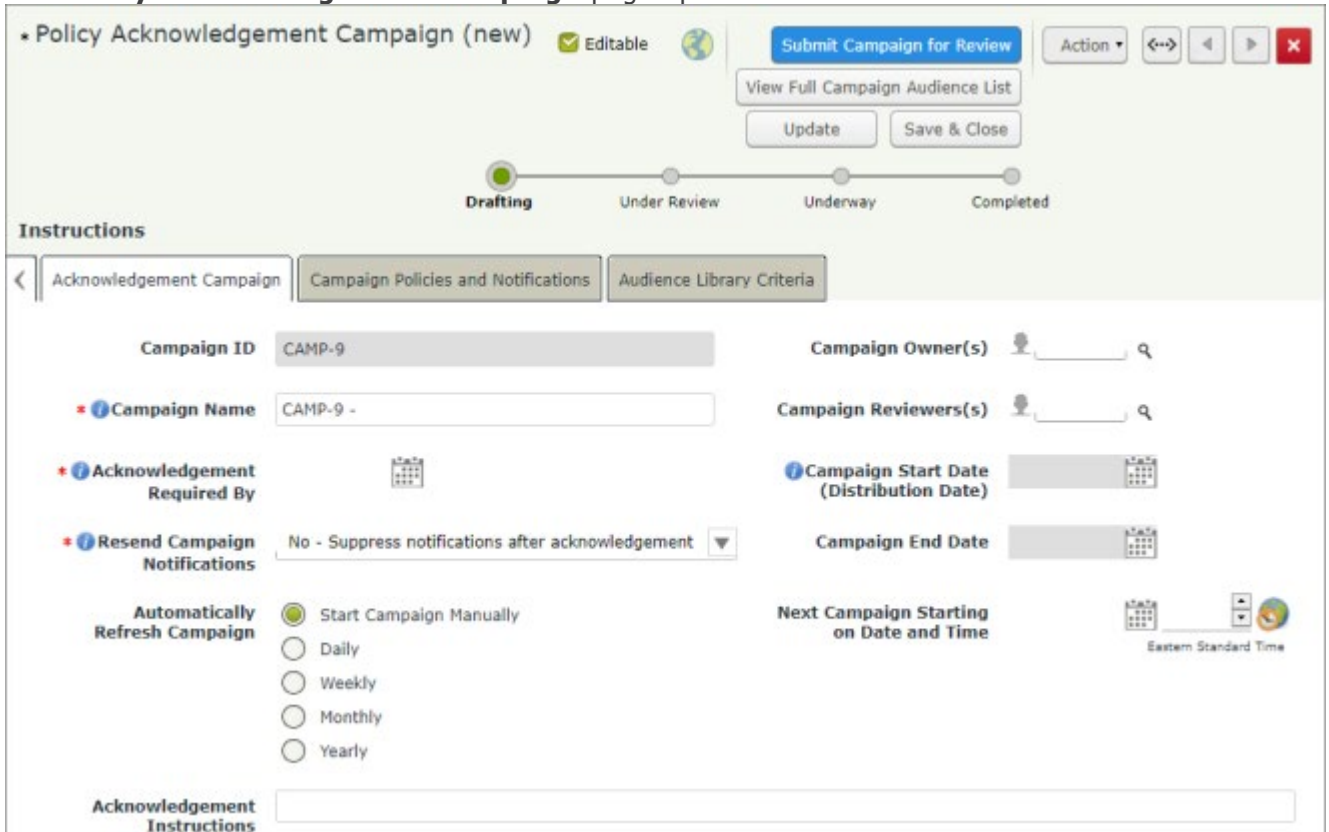
Note: Some user accounts may be created as part of a policy campaign where the accounts did not already exist in Rsam. A hashed one-time password is automatically generated for such user accounts. The users are then provided with a one-time login password through email. When users log in to Rsam using their Rsam one-time password, they will be required to change the password before continuing.

Step 1: Creating a Campaign

To create a campaign, perform the following steps:

1. Sign in as the *Campaign Manager*. Provide the **Username** as *r_campaign_manager* and **Password** as *password*.
2. From the navigation pane on the left side, navigate to **Campaign Management > Create a New Policy Campaign**.

The **Policy Acknowledgement Campaign** page opens.



The screenshot shows the 'Policy Acknowledgement Campaign (new)' form. At the top, there's a title bar with 'Policy Acknowledgement Campaign (new)', an 'Editable' status, and a 'Submit Campaign for Review' button. Below the title bar is a progress bar with four stages: 'Drafting' (active), 'Under Review', 'Underway', and 'Completed'. The form is divided into sections: 'Instructions' with tabs for 'Acknowledgement Campaign', 'Campaign Policies and Notifications', and 'Audience Library Criteria'. The main form fields are:

- Campaign ID:** CAMP-9
- Campaign Name:** CAMP-9 -
- Acknowledgement Required By:** A calendar icon.
- Resend Campaign Notifications:** A dropdown menu set to 'No - Suppress notifications after acknowledgement'.
- Automatically Refresh Campaign:** Radio buttons for 'Start Campaign Manually' (selected), 'Daily', 'Weekly', 'Monthly', and 'Yearly'.
- Campaign Owner(s):** A user selection field.
- Campaign Reviewer(s):** A user selection field.
- Campaign Start Date (Distribution Date):** A calendar icon.
- Campaign End Date:** A calendar icon.
- Next Campaign Starting on Date and Time:** A calendar icon and a time zone dropdown set to 'Eastern Standard Time'.
- Acknowledgement Instructions:** A large text area.

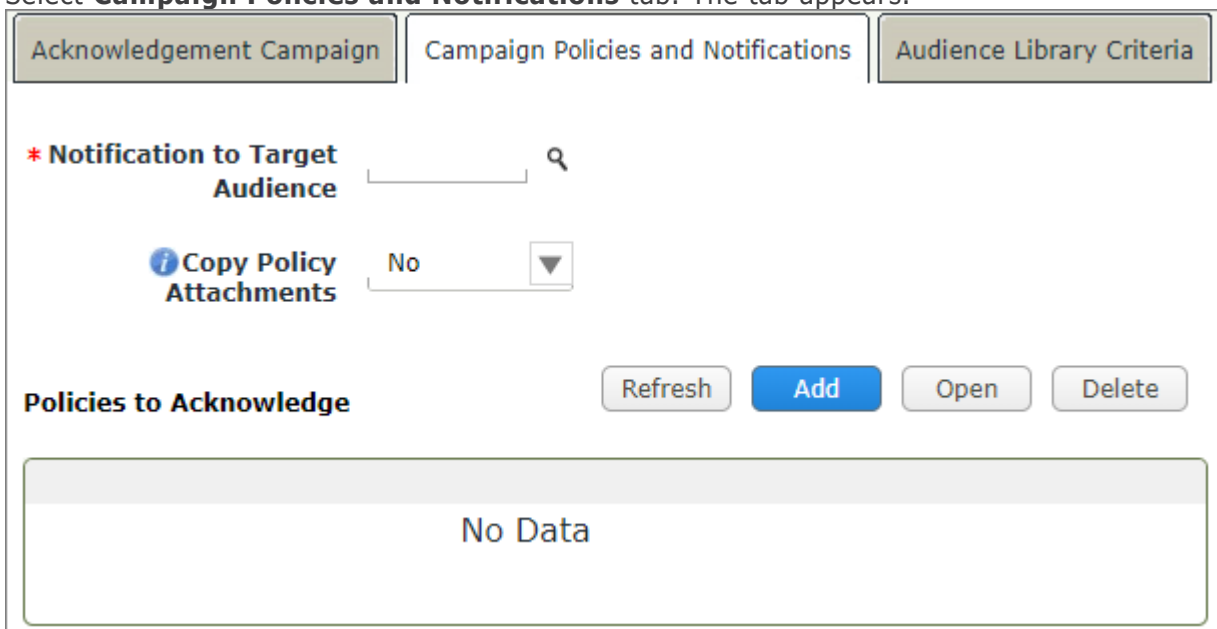
3. Provide a name for the campaign in the **Campaign Name** field.
4. Assign an owner and reviewer for the campaign in the **Campaign Owner(s)** and **Campaign Reviewer(s)** fields.
The Campaign Reviewer can be assigned by a Campaign Owner also, at a later time.
5. Provide the date by when the target audience must acknowledge the policies in the campaign, in the **Acknowledgement Required By** field.


6. Select the notification method from the Resend Campaign Notifications drop-down. The values are as follows:
 - **No - Suppress notifications after acknowledgement** -Select this value to disable sending notification after target audience acknowledges the campaign.
 - **Yes - Always send notifications** - Select this value to continue sending notifications even after target audience acknowledges the campaign.

Campaign Policies and Notifications

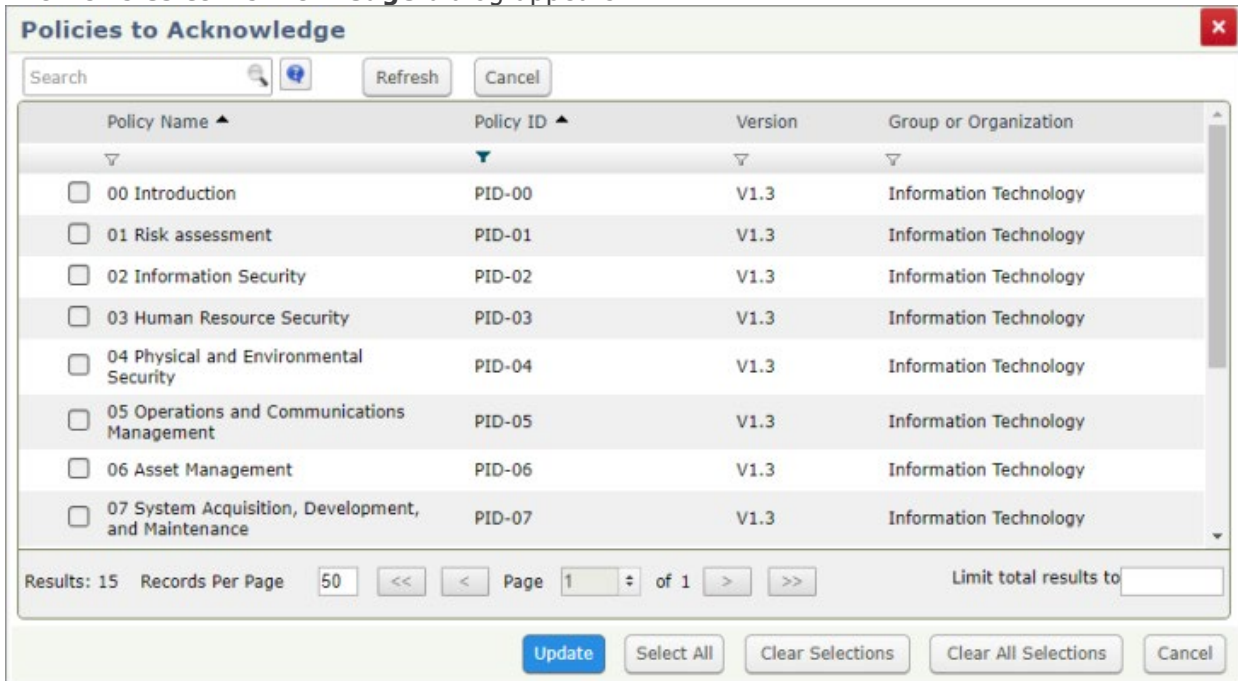
This tab is used to set the policies and notification message for the target audience of this campaign.

7. Select **Campaign Policies and Notifications** tab. The tab appears.



8. Click  in the **Notification to Target Audience** field to select the notification message to be sent to the target audience. The **Notification to Target Audience** dialog appears.
 - a. Select the required notification for the campaign.
 - b. Click **Update** to save. The dialog closes and the notification name is added in the Notification to Target Audience field.

9. In the **Policies to Acknowledge** section, click **Add** to add policies to the campaign. The **Policies to Acknowledge** dialog appears.



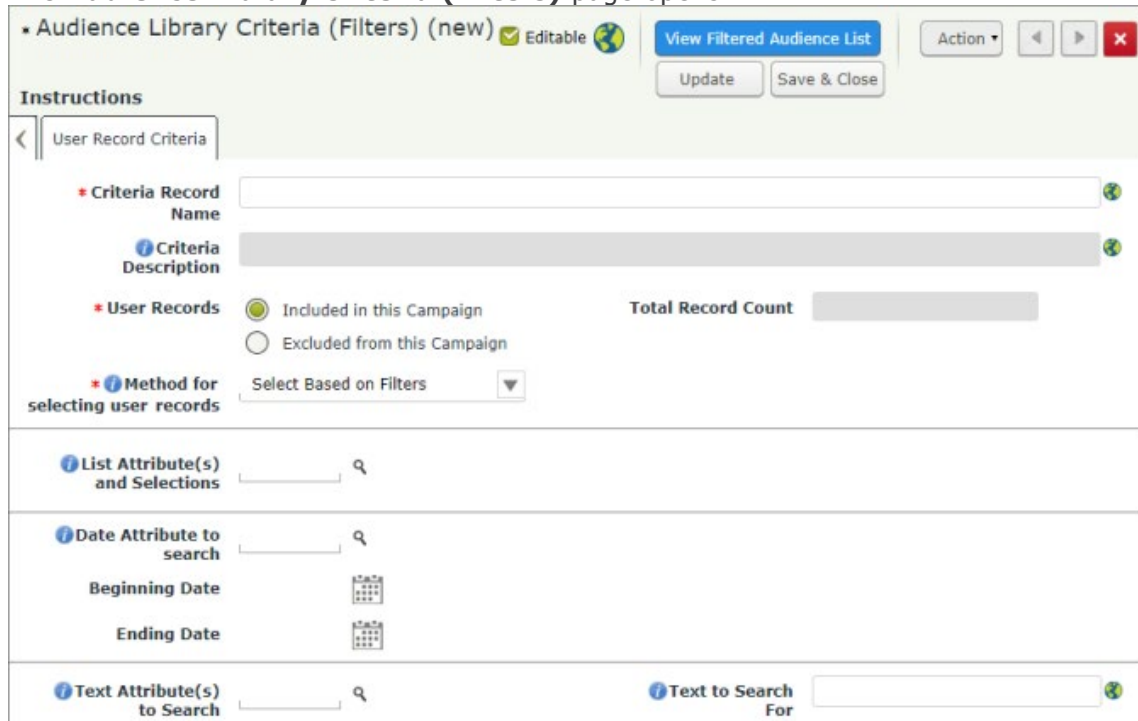
- a. Select the required policies.
- b. Click **Update** to save the selection(s).
The dialog closes and selected policies are added to the Policies to Acknowledge section.

Setting Audience Criteria

A criteria filter can be set to select the target audience for a campaign or to exclude specific sets of users based on the values provided as filters. Campaign notifications will be sent to only those users matching the audience criteria to be included in the campaign. You may add as many criteria records as necessary to define your audience.


10. Click **Audience Library Criteria**. The tab appears.
11. Click **Add** in the **Audience Library Criteria (Filters)** section to add the target audience criteria.

The **Audience Library Criteria (Filters)** page opens.



- a. Provide a name for the audience criteria record in the **Criteria Record Name** field.
- b. Select a value in the User Records field. The values available are as follows:
 - **Included in this Campaign** - Select this value if the criteria is to set the users included in this campaign.
 - **Excluded from this Campaign** - Select this value if the criteria is to set the users to be excluded from this campaign.
- c. Select a value in the **Method for selecting user records** field. The values available are as follows:
 - [Select Based on Filters](#) - To set filter criteria to identify the target users.
 - [Select user records from a list](#) - To select users from a **User Record Selection List**.
 - **Select all user records** - Selects all users available in the Audience - User Library.

Selecting Based on Filters

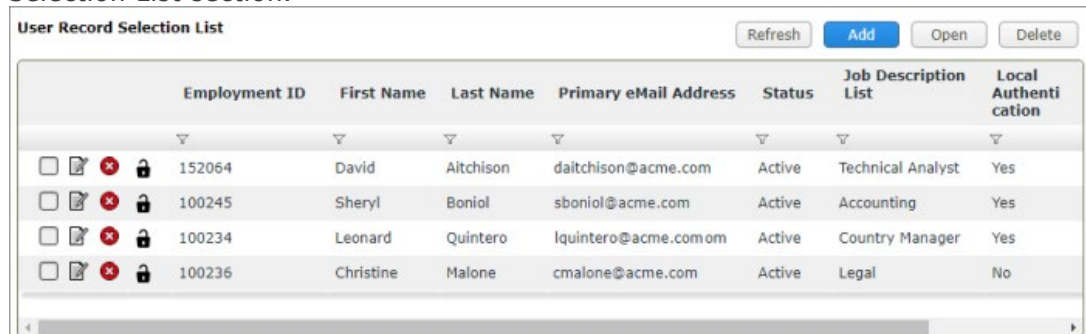
- i. Click  in the **List Attribute(s) and Selections** field to select the attribute and attribute responses based on which the target audience is selected. The **List Attribute(s) and Selections** dialog opens.

- ii. Select the required attributes to filter user records and click **Update**.
The dialog closes and the filters are added to the List Attribute(s) and Selections field.
When more than one attribute and response pair is selected for the same attribute, the OR logic is applied.
- iii. Select the date attribute to filter user records from the **Date Attribute to search** field.
- iv. Select the text attribute(s) and text to search for in the **Text Attribute(s) to Search** and **Text to Search For** fields.


Selecting User Records from a List

On selecting this option, the **User Record Selection List** section appears.

- i. Click **Add**. The **User Record Selection List** dialog opens.
- ii. Select the users for the target audience from the list.
- iii. Click **Update**. The dialog closes and the users are added to the User Record Selection List section.



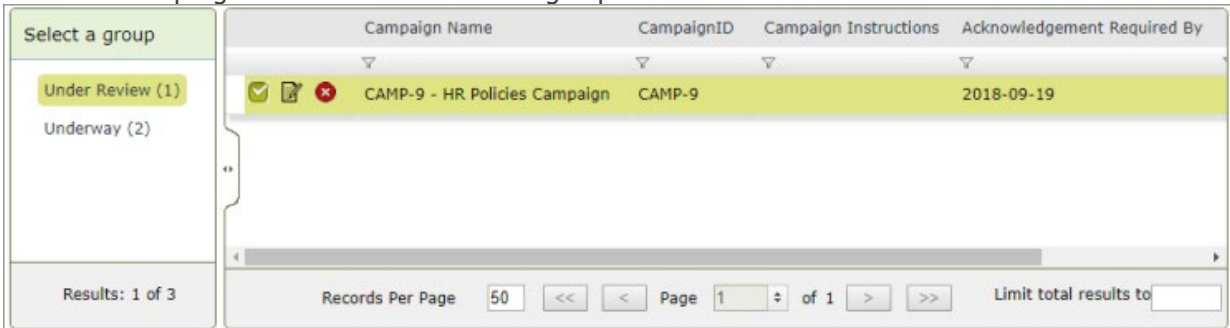
User Record Selection List							
	Employment ID	First Name	Last Name	Primary eMail Address	Status	Job Description List	Local Authentication
<input type="checkbox"/>	152064	David	Aitchison	daitchison@acme.com	Active	Technical Analyst	Yes
<input type="checkbox"/>	100245	Sheryl	Boniol	sboniol@acme.com	Active	Accounting	Yes
<input type="checkbox"/>	100234	Leonard	Quintero	lquintero@acme.com	Active	Country Manager	Yes
<input type="checkbox"/>	100236	Christine	Malone	cmalone@acme.com	Active	Legal	No

- d. Click **Update** to save the user criteria.
 - e. Click **View Filtered Audience List** to view the list of user records filtered based on the search criteria set.
 - f. Click  to close the record.
12. Click **View Full Campaign Audience List** to view the list of user records for the combination of Criteria provided. This list will provide details on the audience members that are included and excluded based on your specifications.
 13. Click **Test Campaign Acknowledgement** to create a test campaign acknowledgement and notification record for the campaign. Click **OK** in the dialog that appears.
 14. Click **Submit Campaign for Review** to submit the campaign for the review to the reviewer. The campaign moves to the **Under Review** state.

Step 2: Reviewing and Approving a Campaign

A campaign is submitted to a Campaign Reviewer for review and approval before notifications can be sent to the target audience. To review and approve a campaign, perform the following steps:

1. Sign in as the *Campaign Reviewer*. Provide the **Username** as *r_campaign_reviewer* and **Password** as *password*.
2. From the navigation pane on the left side, navigate to **Campaign Management**.
3. From the campaign navigator at the end of the page, select **Under Review (x)** and double-click the campaign under review on the right pane.



The **Policy Acknowledgement Campaign** record opens.

4. Review the details and click **Approve and Start Campaign** to start the campaign. A dialog appears stating that the email notifications will be sent to the target audience and the policy acknowledgement campaign will start. Click **OK**.

The campaign moves to the **Underway** status.

Step 3: Acknowledging a Policy - Target Audience

The target audience for policy campaigns are notified that they are required to acknowledge a policy. To acknowledge an assigned policy, perform the following steps:

1. Sign into Rsam as a target user where a policy is assigned for acknowledgement. If the user is not already in Rsam, the user will receive credentials for accessing Rsam through an email. The email contains a one-time password.
2. From the navigation panel on the left side, select **Policy Management > Policy Acknowledgement**.

- Click **EPM Policies for Acknowledgments** in the **Policies for acknowledgments** widget. A search page listing all policies assigned to the user for acknowledgment appears.

Drag a column here to group by				
Policy To Acknowledge	Workflow State	Acknowledgement Required By	Policy Document	Acknowledgement Date/Time
<input type="checkbox"/> 02 Information Security	Initial Notification	2018-10-28	EPM_Policy_Detail.pdf	
<input type="checkbox"/> 00 Introduction	Initial Notification	2018-10-28	EPM_Policy_Detail.pdf	

Results: 2 Records Per Page: 50 Page 1 of 1 Limit total results to 1000

- Double-click a record to open it.

Campaign Acknowledgement Record

 Editable
Action

(read)

< Acknowledgement

Review
Acknowledge

Acknowledgement Instructions Please select the Acknowledgement button after reviewing the policy

Policy to Acknowledge 02 Information Security

*** Acknowledgement Required By** 28/03/2014

*** Date and Time Acknowledged** Eastern Standard Time

*** First Name** Brittany

*** Last Name** Gigliotti Jr

*** User Primary eMail Address** gmensing01@gmail.com

Policy Document 1 File Attachments

- Check the policy details and download and read the policy document attachment(s), if any.
- Click **Acknowledge** to acknowledge the policy. The record moves to the **Acknowledged** state.

Step 4: Completing a Policy Acknowledgement Campaign

When the acknowledgement campaign is completed, a Campaign Owner can mark the campaign as completed. Campaigns will be completed automatically if all audience members have acknowledged all policies. To manually mark a campaign as complete, perform the following steps:

1. Sign in as the *Campaign Owner*. Provide the **Username** as *r_campaign_owner* and **Password** as *password*.
2. From the navigation pane on the left side, navigate to **Campaign Management > Campaign Navigators**.
The Campaign Navigator appears.
3. Select **EPM Policy Acknowledgement Campaigns** to view the campaigns grouped by the workflow states.
4. Click **Underway** and double-click the required campaign from the list on the right panel.
5. Click **Close Campaign (Completed)** to close the campaign. The campaign moves to the **Completed** state.
A campaign will also be closed automatically when all users have acknowledged the campaign.

Appendix 1: Email Notifications

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 Enterprise Policy Management Module 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.



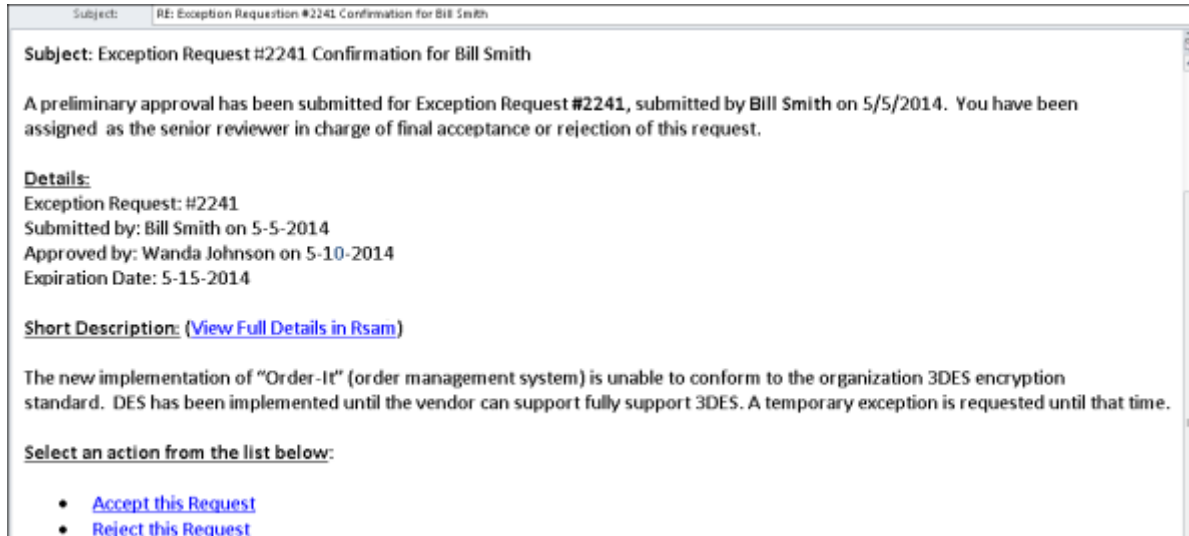
The screenshot shows the 'User Details' form. It includes fields for User Id (152048), First Name (May), Middle Name, Last Name (Brian), eMail ID (support@rsam.com), Phone Number, Password (masked with dots), and Confirm Password. There is also a checkbox for 'LDAP User'. Below this checkbox, there are fields for 'User's LDAP ID' and 'User's LDAP Domain' (a dropdown menu showing 'Please select a Domain').

6. Click **OK**.
The email address of the user account is saved.

Appendix 2: 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 3: Rsam Documentation

EPM Baseline Configuration Guide

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

Online Help

This tutorial provides the step-by-step instructions for the Rsam Enterprise Policy Management 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.

