PolicyBond

Step-by-Step Tutorial

Rsam Version: 10 | Document Version: 02.01.03

October 2020

www.wegalvanize.com

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.

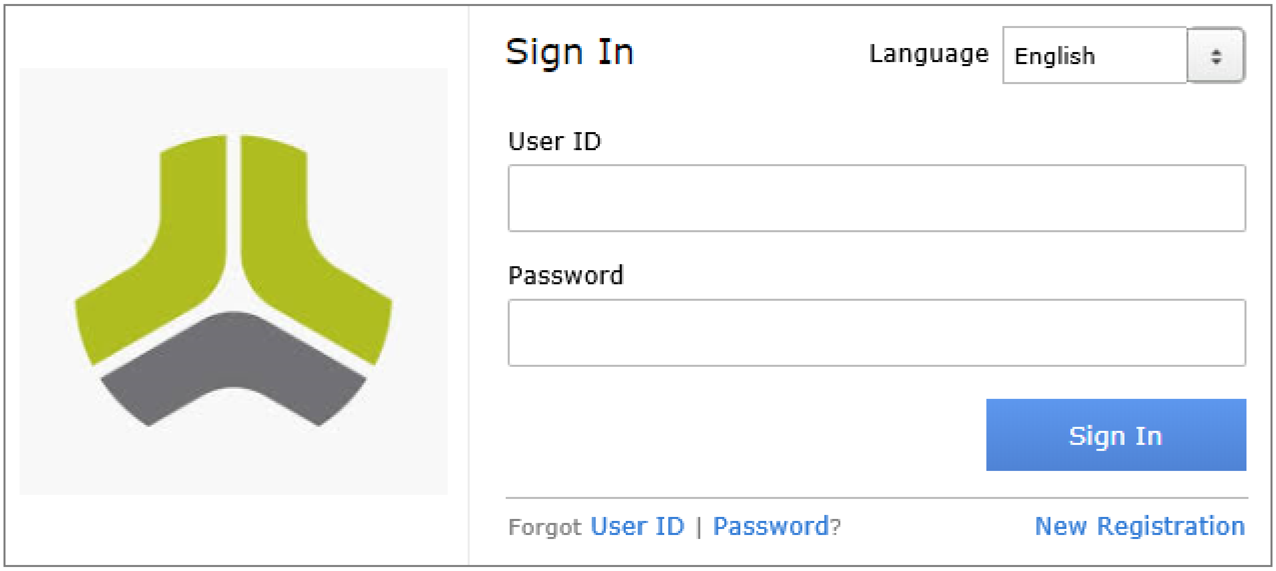
Rsam Sandbox Environment

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

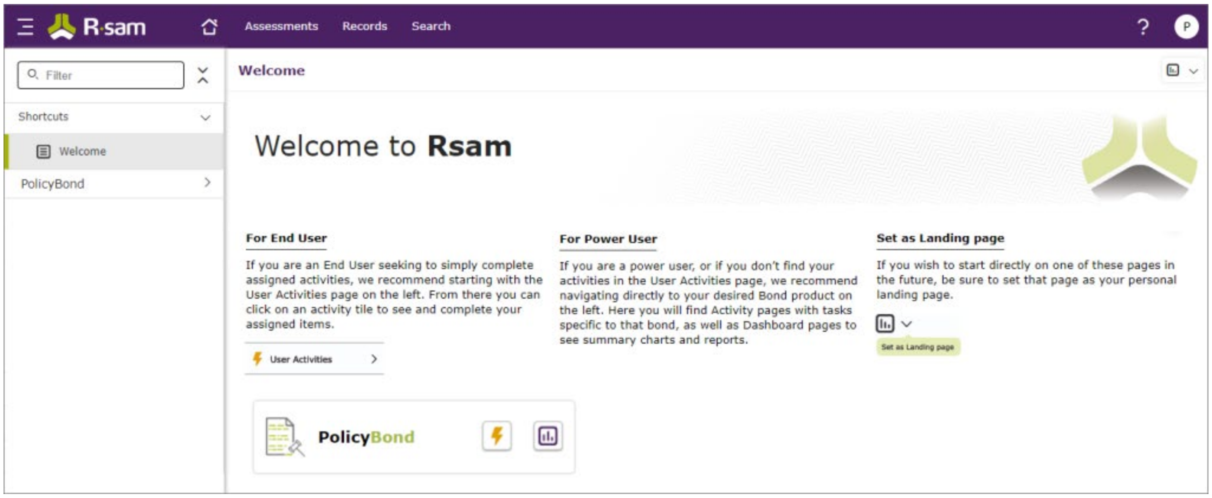
Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign In page so that you can easily toggle between various sample accounts used throughout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



Welcome to **Rsam**

For End User

If you are an End User seeking to simply complete assigned activities, we recommend starting with the User Activities page on the left. From there you can click on an activity tile to see and complete your assigned items.

For Power User

If you are a power user, or if you don't find your activities in the User Activities page, we recommend navigating directly to your desired Bond product on the left. Here you will find Activity pages with tasks specific to that bond, as well as Dashboard pages to see summary charts and reports.

Set as Landing page

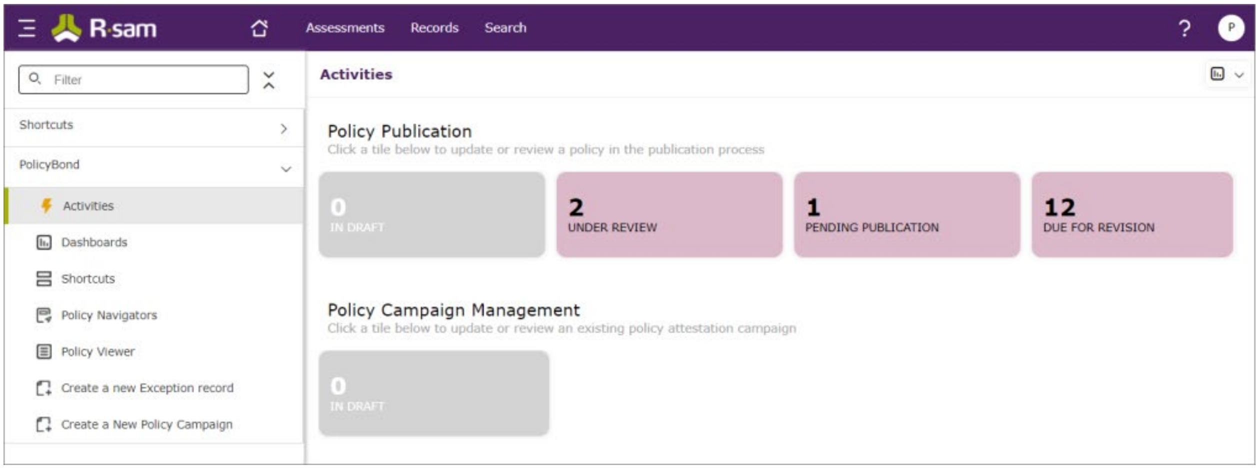
If you wish to start directly on one of these pages in the future, be sure to set that page as your personal landing page.

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.



Policy Publication

Click a tile below to update or review a policy in the publication process

0 IN DRAFT

2 UNDER REVIEW

1 PENDING PUBLICATION

12 DUE FOR REVISION

Policy Campaign Management

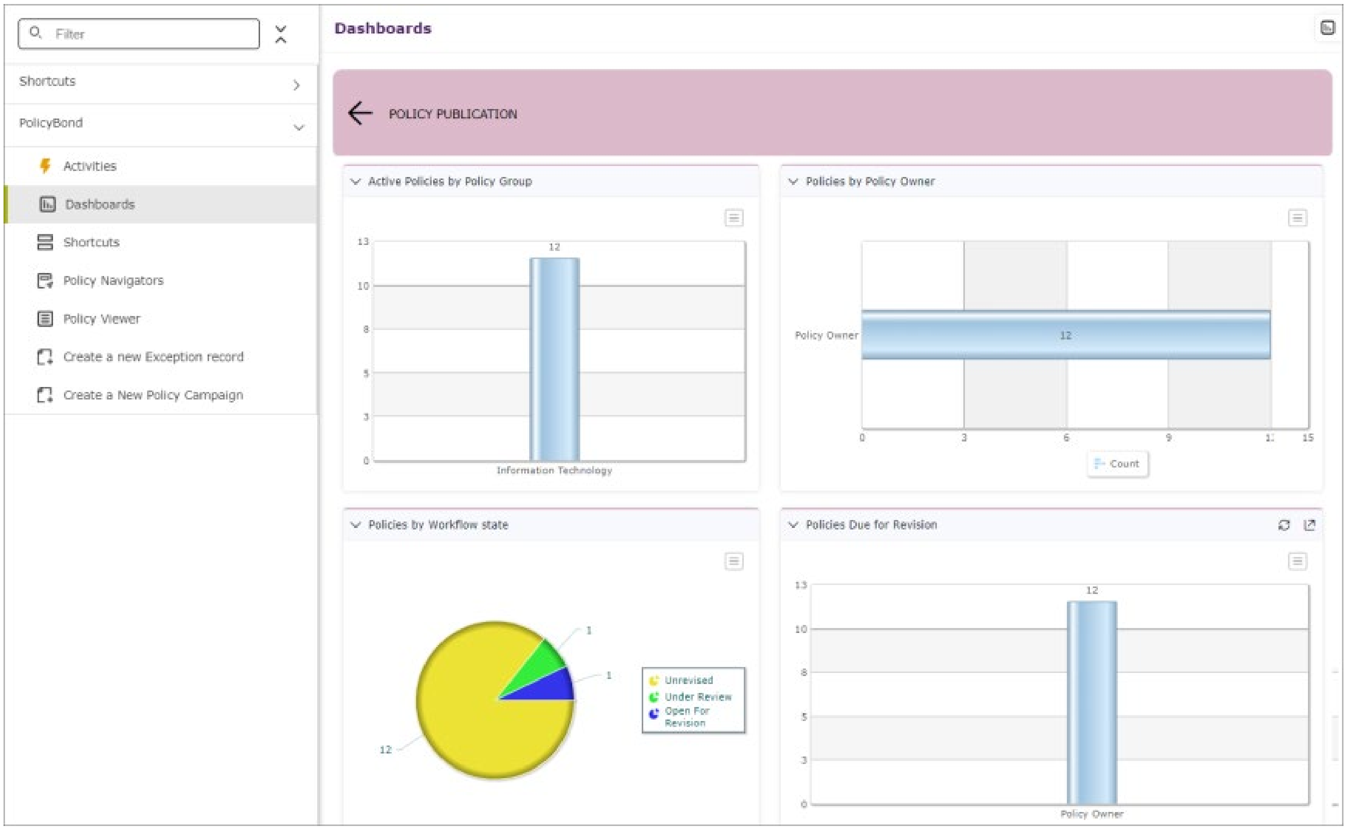
Click a tile below to update or review an existing policy attestation campaign

0 IN DRAFT

Click an Activity Center tile to view all related tasks.

Additionally, you can perform the following navigation actions:

- Expand the required bond from the left navigation bar and use the pages.
- From the left navigation bar, click **Dashboards** corresponding to the bond to view all Dashboards configured for the bond.



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

Rsam PolicyBond

Overview

Rsam PolicyBond 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 the versioning mechanism in PolicyBond, organizations can track policy changes effectively. This tutorial provides a step-by-step procedure to walk you through the commonly followed path of a policy management workflow within the module.

The module has the following capabilities and benefits:

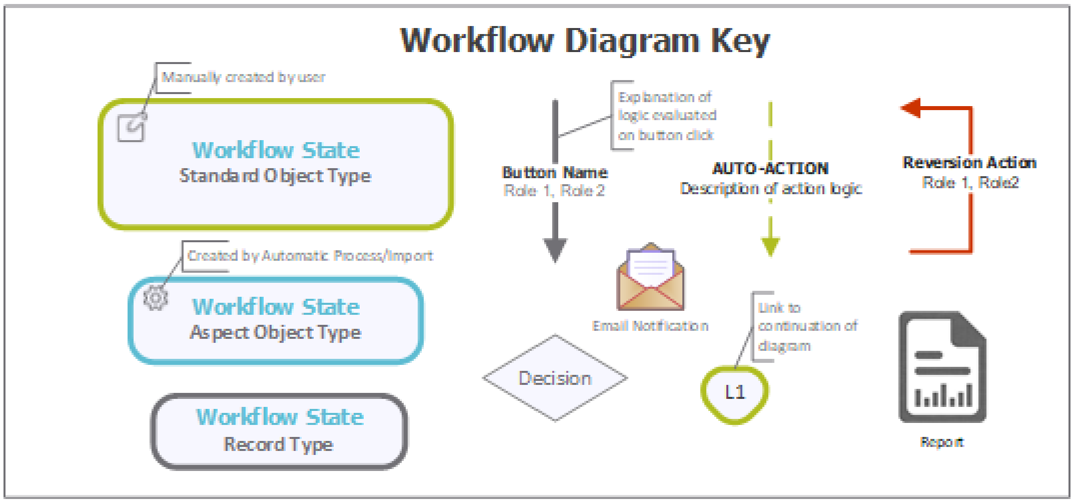
- Create, track, approve, manage, and version all policies in a central location.
- Author policies manually in Rsam, or import policy text.
- Ability to map policies to risks, controls, and exceptions.
- Manage policy reviews and approval using an automated workflow process.
- Create policy acknowledgment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

PolicyBond Workflows

The module provides automated workflows for the following components:

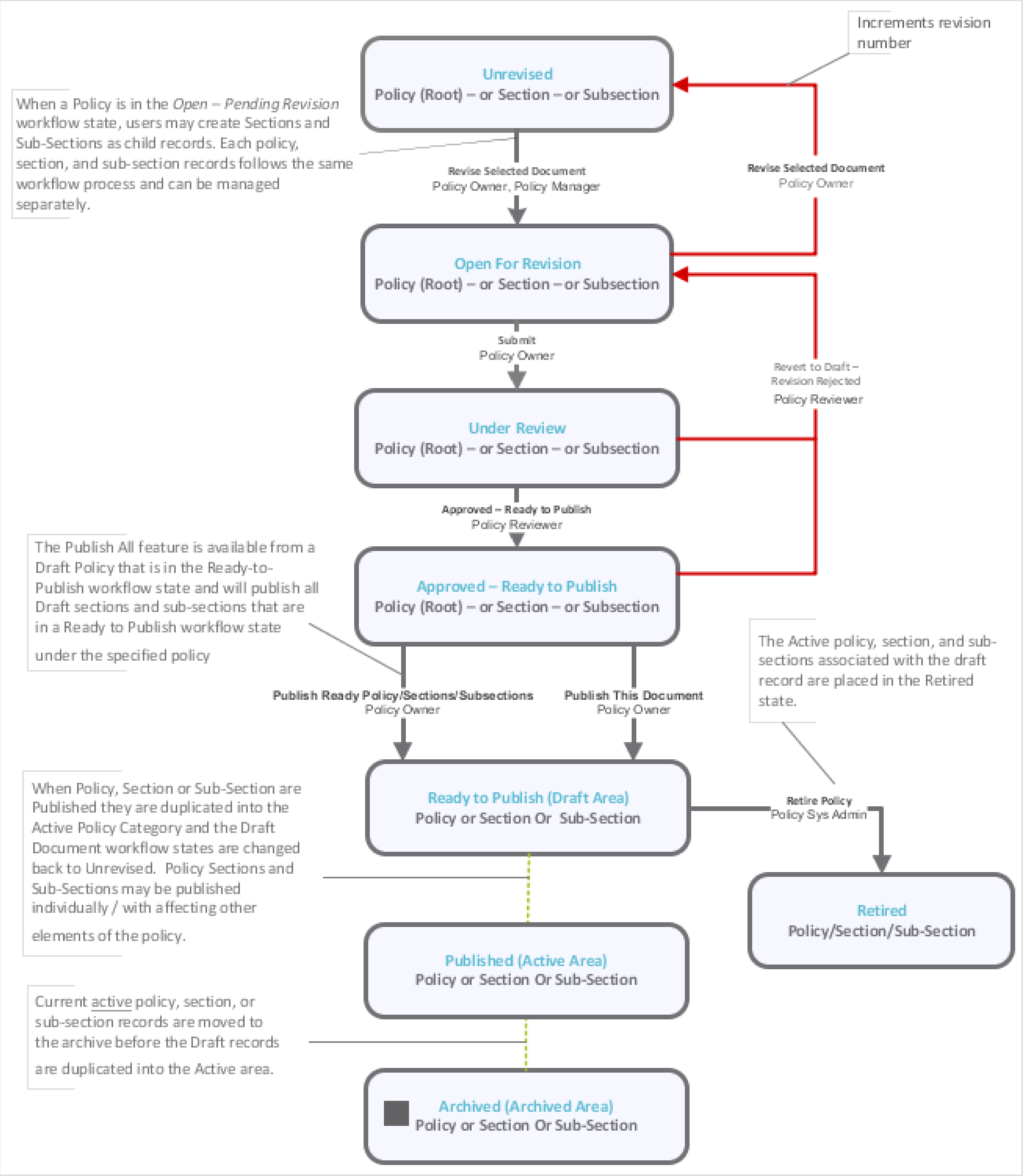
- Policy, Section and Sub-Section
- Policy Acknowledgement Campaign
- Campaign Acknowledgement Record

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.


Unrevised
Policy (Root) – or Section – or Subsection
Revise Selected Document
Policy Owner, Policy Manager
Revise Selected Document
Policy Owner
Open For Revision
Policy (Root) – or Section – or Subsection
Submit
Policy Owner
Revert to Draft – Revision Rejected
Policy Reviewer
Under Review
Policy (Root) – or Section – or Subsection
Approved – Ready to Publish
Policy Reviewer
Approved – Ready to Publish
Policy (Root) – or Section – or Subsection
Publish Ready Policy/Sections/Subsections
Policy Owner
Publish This Document
Policy Owner
Ready to Publish (Draft Area)
Policy or Section Or Sub-Section
Retire Policy
Policy Sys Admin
Retired
Policy/Section/Sub-Section
Published (Active Area)
Policy or Section Or Sub-Section
Archived (Archived Area)
Policy or Section Or Sub-Section

Increments revision number

When a Policy is in the *Open – Pending Revision* workflow state, users may create Sections and Sub-Sections as child records. Each policy, section, and sub-section records follows the same workflow process and can be managed separately.

The Publish All feature is available from a Draft Policy that is in the Ready-to-Publish workflow state and will publish all Draft sections and sub-sections that are in a Ready to Publish workflow state under the specified policy

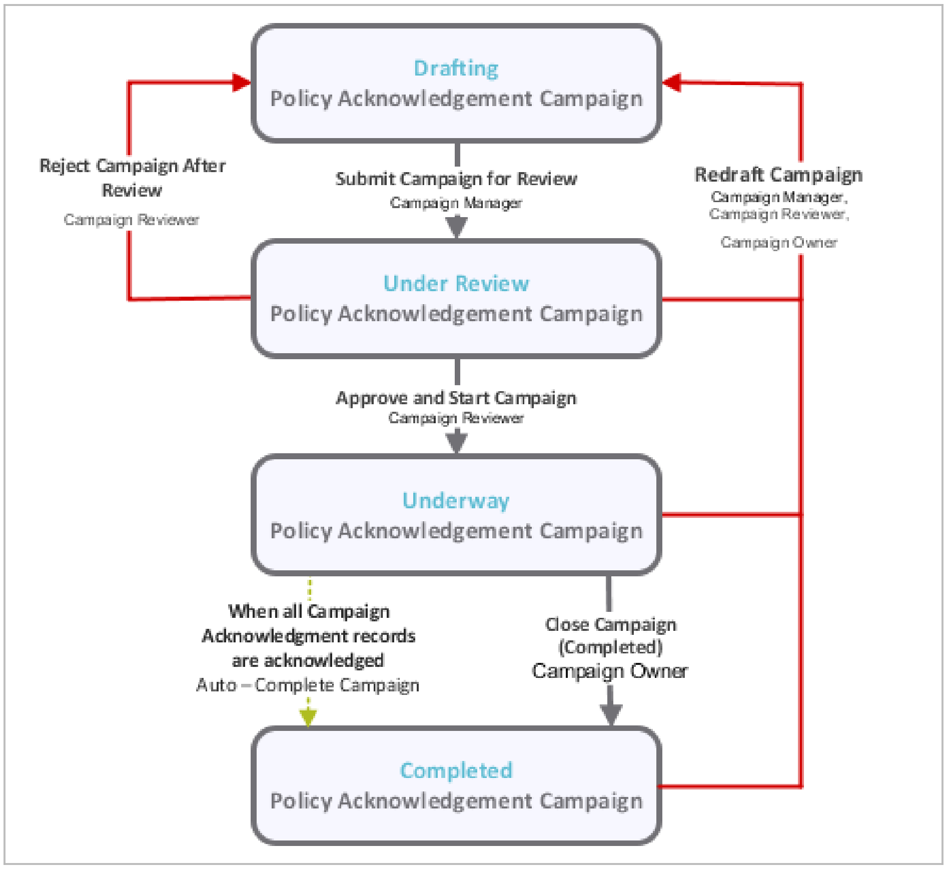
The Active policy, section, and sub-sections associated with the draft record are placed in the Retired state.

When Policy, Section or Sub-Section are Published they are duplicated into the Active Policy Category and the Draft Document workflow states are changed back to Unrevised. Policy Sections and Sub-Sections may be published individually / with affecting other elements of the policy.

Current active policy, section, or sub-section records are moved to the archive before the Draft records are duplicated into the Active area.

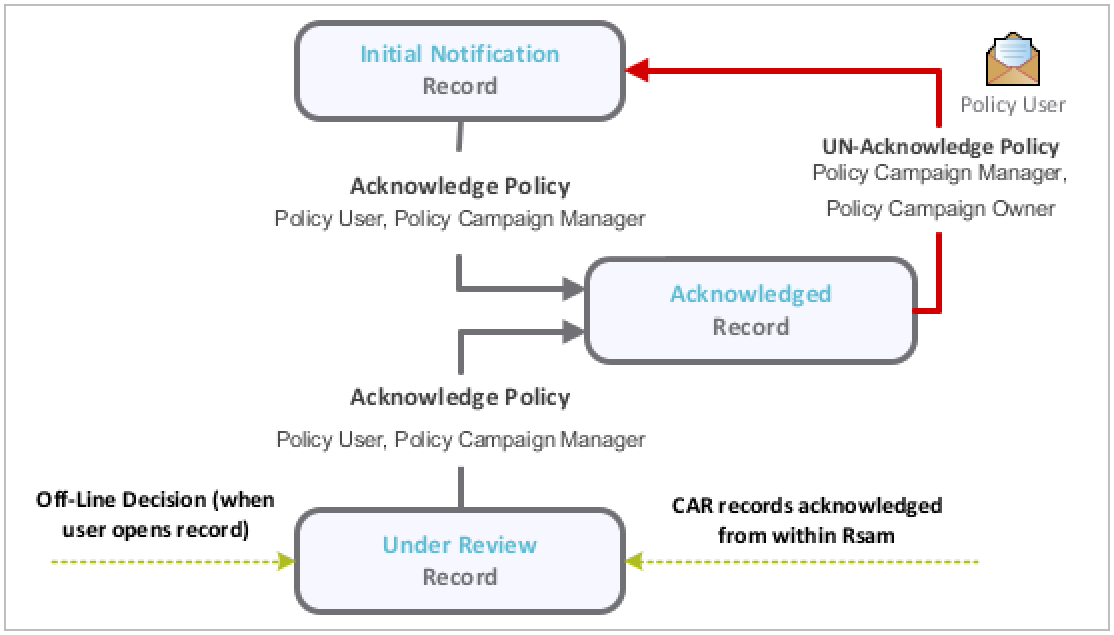
Policy Acknowledgement Campaign Workflow

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


Drafting
Policy Acknowledgement Campaign
Reject Campaign After Review
Campaign Reviewer
Submit Campaign for Review
Campaign Manager
Redraft Campaign
Campaign Manager, Campaign Reviewer, Campaign Owner
Under Review
Policy Acknowledgement Campaign
Approve and Start Campaign
Campaign Reviewer
Underway
Policy Acknowledgement Campaign
When all Campaign Acknowledgment records are acknowledged
Auto – Complete Campaign
Close Campaign (Completed)
Campaign Owner
Completed
Policy Acknowledgement Campaign

Campaign Acknowledgement Record Workflow

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


Initial Notification
Record
Policy User
UN-Acknowledge Policy
Policy Campaign Manager, Policy Campaign Owner
Acknowledge Policy
Policy User, Policy Campaign Manager
Acknowledged
Record
Acknowledge Policy
Policy User, Policy Campaign Manager
Off-Line Decision (when user opens record)
CAR records acknowledged from within Rsam
Under Review
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 PolicyBond 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.

User 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.

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.

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 *PolicyBond*.

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:

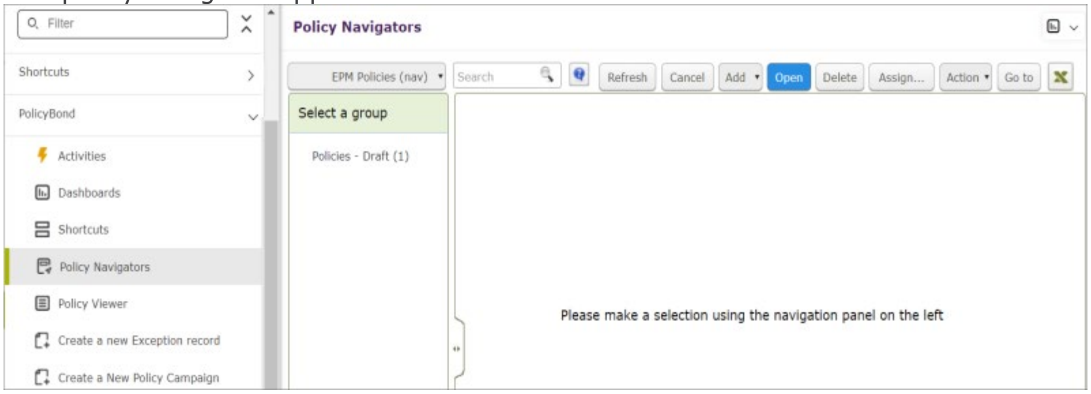
- Updating and Submitting a Policy
- Reviewing and Approving Policy Revisions
- Publishing a Policy
- Comparing Policies in Draft and Published States

Step 1: Updating and Submitting a Policy

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

1. Sign in to Rsam 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 Bond > Policy Navigators**. The policy navigator appears.

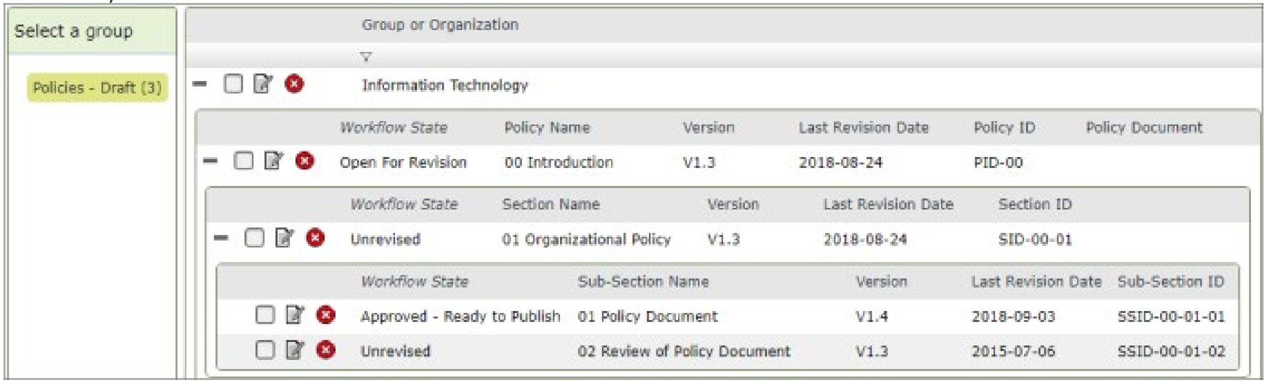


Please make a selection using the navigation panel on the left

3. From within the policy navigator, with **EPM Policies (nav)** selected, click **Policies - Draft (x)**.

   The policies in the **Draft** category appear in the list.

4. Click ✚ icon corresponding to the required group to expand and view the related policies, sections, and sub-sections.



Information Technology

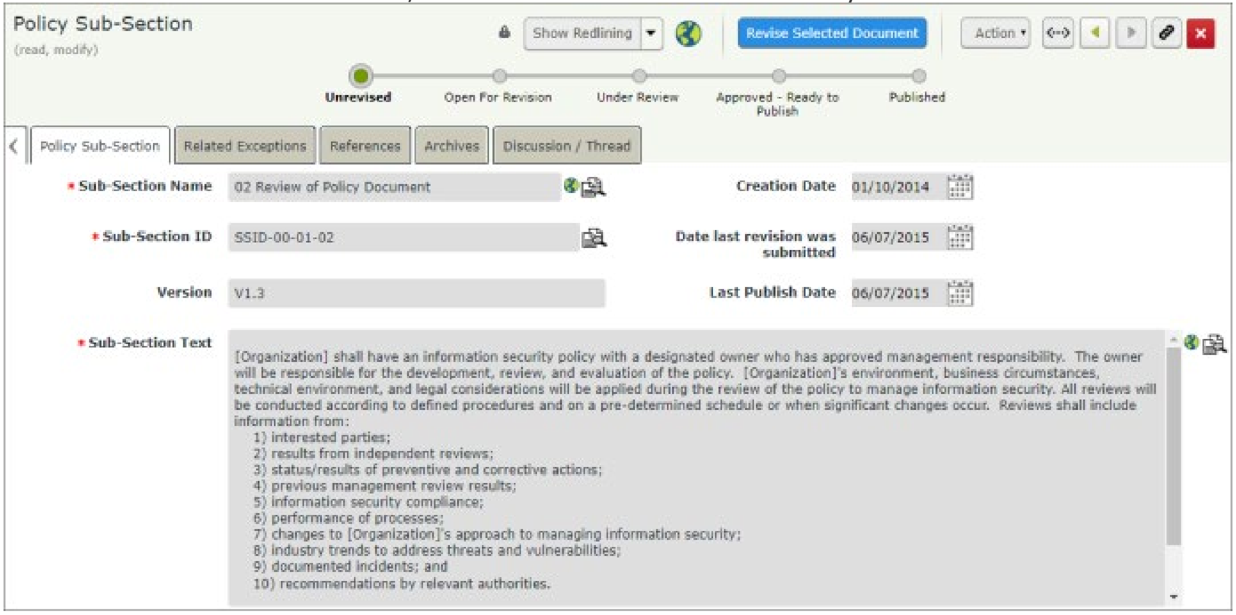
Workflow State	Policy Name	Version	Last Revision Date	Policy ID	Policy Document
Open For Revision	00 Introduction	V1.3	2018-08-24	PID-00	

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

5. Double-click a record to open the required policy or section record.

   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.



* 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.

6. 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.

7. Make updates to the attributes as required.

8. 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***.

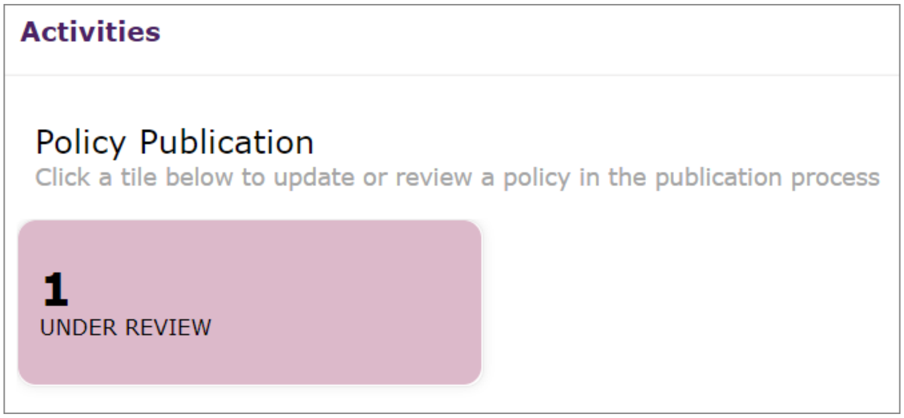
Step 2: Reviewing and Approving Policy Revisions

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 **PolicyBond > Activities**.

   The Activities page appears listing the applicable activity tiles.



Activities

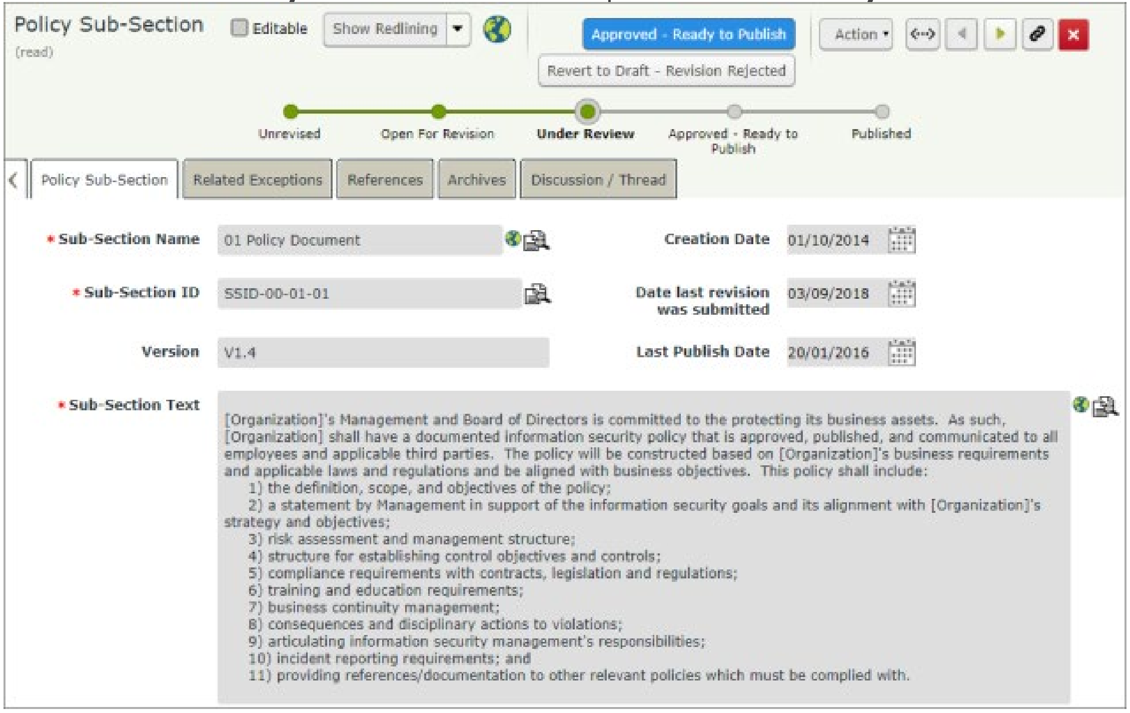
Policy Publication

Click a tile below to update or review a policy in the publication process

3. Click the tile **Under Review**.

   The tile expands to display the grid listing the records in the **Under Review** state.

4. Select the policy updated in Step 1: Updating and Submitting a Policy and double-click to open the record. The **Policy Sub-Section** record opens with the **Policy Sub-Section** tab selected.



* Sub-Section Name: 01 Policy Document

Creation Date: 01/10/2014

* Sub-Section ID: SSID-00-01-01

Date last revision was submitted: 03/09/2018

Version: V1.4

Last Publish Date: 20/01/2016

* Sub-Section Text:

[Organization]'s Management and Board of Directors is committed to the protecting its business assets. As such, [Organization] shall have a documented information security policy that is approved, published, and communicated to all employees and applicable third parties. The policy will be constructed based on [Organization]'s business requirements and applicable laws and regulations and be aligned with business objectives. This policy shall include:

1) the definition, scope, and objectives of the policy;
2) a statement by Management in support of the information security goals and its alignment with [Organization]'s strategy and objectives;
3) risk assessment and management structure;
4) structure for establishing control objectives and controls;
5) compliance requirements with contracts, legislation and regulations;
6) training and education requirements;
7) business continuity management;
8) consequences and disciplinary actions to violations;
9) articulating information security management's responsibilities;
10) incident reporting requirements; and
11) providing references/documentation to other relevant policies which must be complied with.

5. Review the information in the policy.

6. Click **Approved - Ready to Publish**.

   The record moves to the **Approved - Ready to Publish** state

7. Log out from Rsam.

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 **PolicyBond > Activities**.

   The Activities page appears listing the applicable activity tiles.

3. Click the tile **Pending Publication**.

   The tile expands to display the grid listing the records in the **Approved - Ready to Publish** state. The policies listed are those to which the owner is assigned.

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

5. 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.

6. Log out from Rsam.

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 **PolicyBond > 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

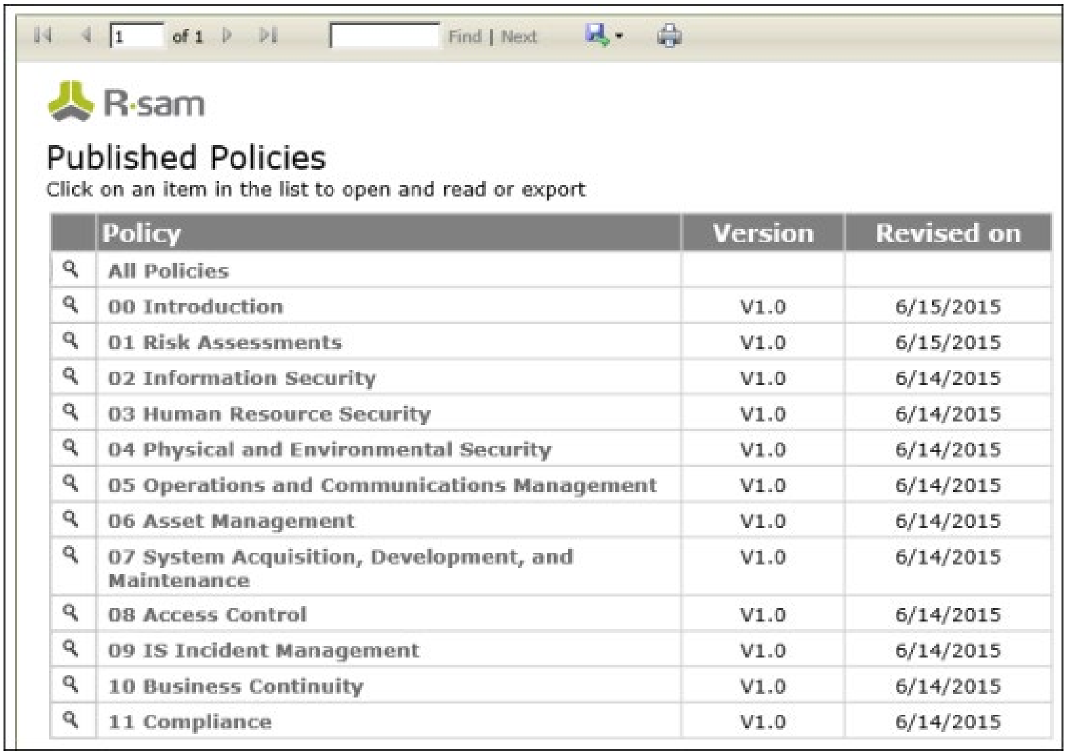
Rsam includes a policy viewer feature that transforms the approved and published policies into a document format. This can be reviewed on-screen, or exported to Word, PDF, HTML, and more. Here, users can also acknowledge that they have read the policies (discussed in the Attesting Policies section).

1. Sign in as the *Policy User*. Enter **Username** as *r_policy_user* and **Password** as *password*.

2. From within the navigation panel at the left-hand side, navigate to **PolicyBond > Policy Viewer**.

   The list of published policies appear on the right panel.

3. Click the **00 Introduction** policy.

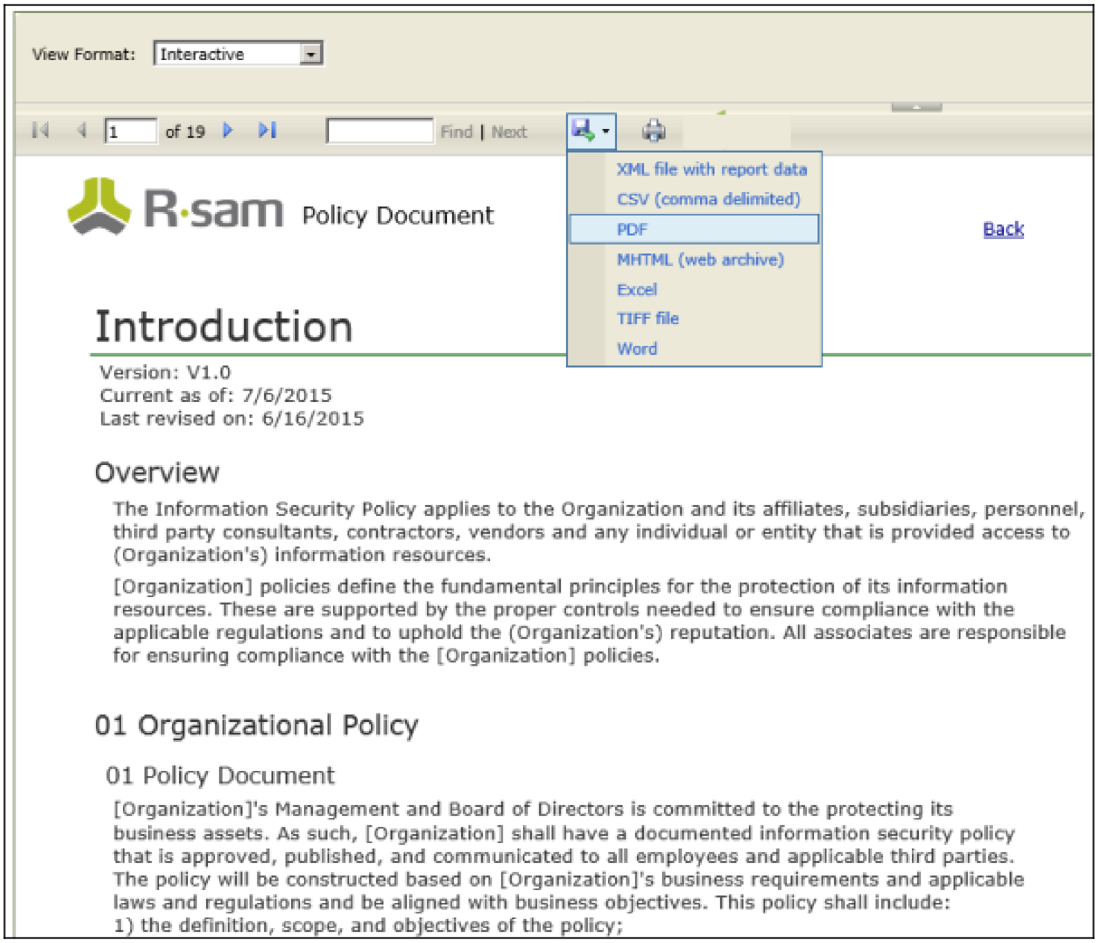


Published Policies

Click on an item in the list to open and read or export

	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

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



Introduction

Version: V1.0
Current as of: 7/6/2015
Last revised on: 6/16/2015

Overview

The Information Security Policy applies to the Organization and its affiliates, subsidiaries, personnel, third party consultants, contractors, vendors and any individual or entity that is provided access to (Organization's) information resources.

[Organization] policies define the fundamental principles for the protection of its information resources. These are supported by the proper controls needed to ensure compliance with the applicable regulations and to uphold the (Organization's) reputation. All associates are responsible for ensuring compliance with the [Organization] policies.

01 Organizational Policy

01 Policy Document

[Organization]'s Management and Board of Directors is committed to the protecting its business assets. As such, [Organization] shall have a documented information security policy that is approved, published, and communicated to all employees and applicable third parties. The policy will be constructed based on [Organization]'s business requirements and applicable laws and regulations and be aligned with business objectives. This policy shall include:
1) the definition, scope, and objectives of the policy;

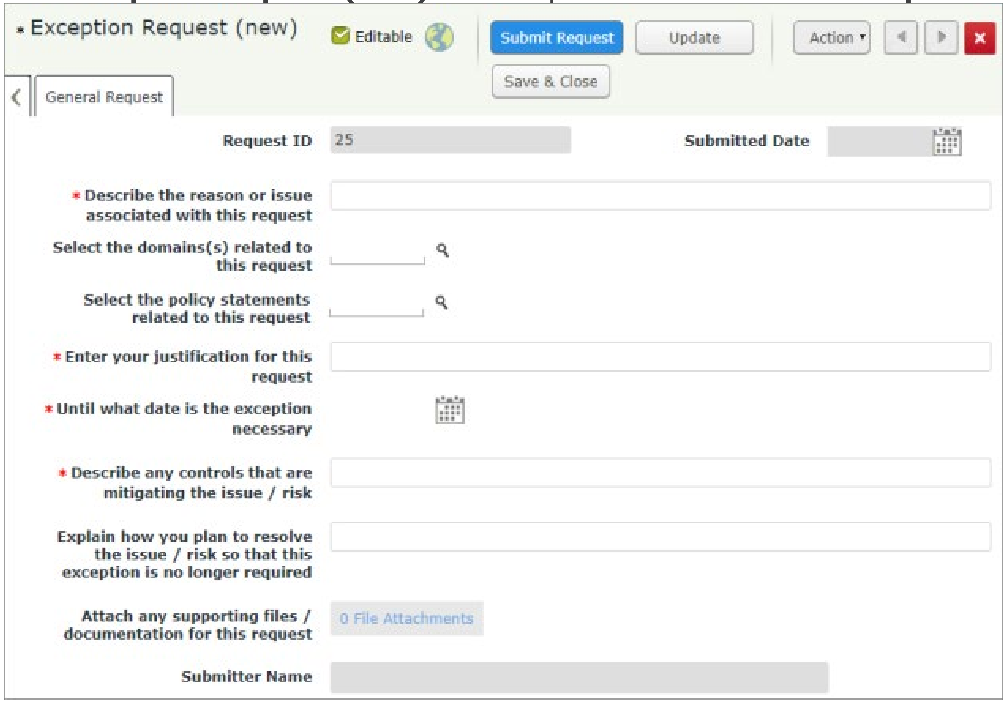
Step 2: Associating Exceptions to Policies

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

1. Sign in as the *Policy Owner* user. Enter **Username** as *r_policy_owner* and **Password** as *password*.

2. From the navigation panel on the left side, navigate to **PolicyBond > Create a new Exception record**.

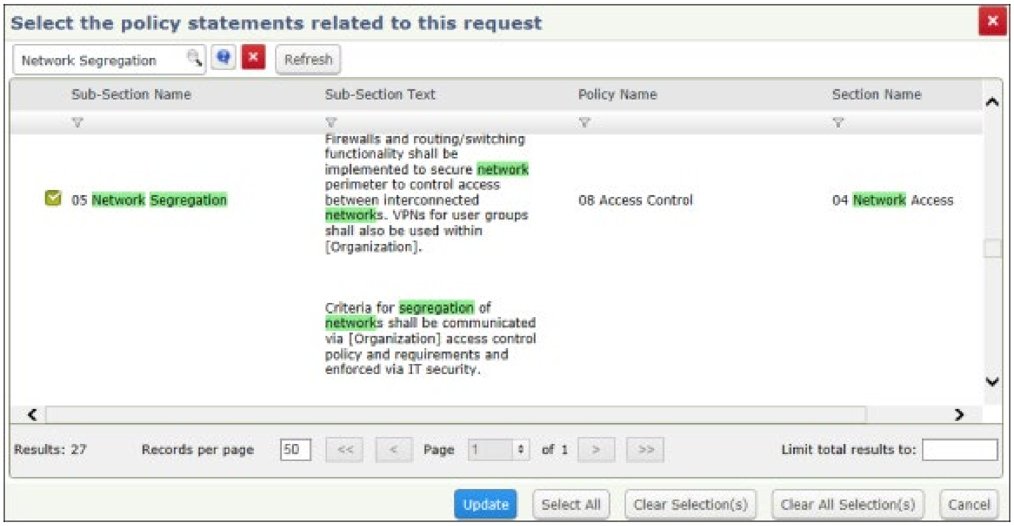
The **Exception Request (new)** record opens with the **General Request** tab selected.



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.

4. 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 that appears, select the check box for the desired record(s) and click **Update**.



Sub-Section Name	Sub-Section Text	Policy Name	Section Name
☑ 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 50 Page 1 of 1 Limit total results to:

5. 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, a *Policy Owner* can view the details of the exception.

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

Step 3: Attesting Policies

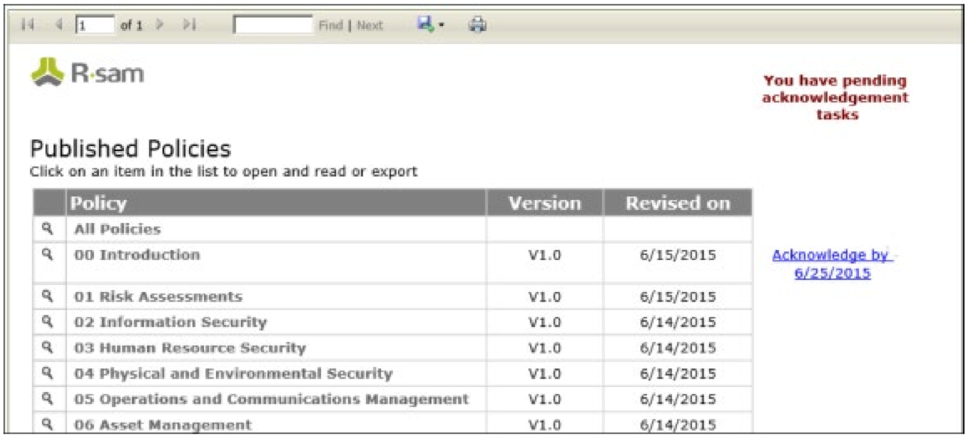
Policy Attestation Campaigns are used to track user acknowledgements and awareness. In this section, the user “Cooper Jennifer” was included in a policy attestation campaign and has received an email containing Cooper Jennifer’s User ID, a one-time password, a link to Rsam, and a request to log in to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

1. 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.

2. From within the navigation panel on the left-hand side, navigate to **PolicyBond > Policy Viewer**.

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



You have pending acknowledgement tasks

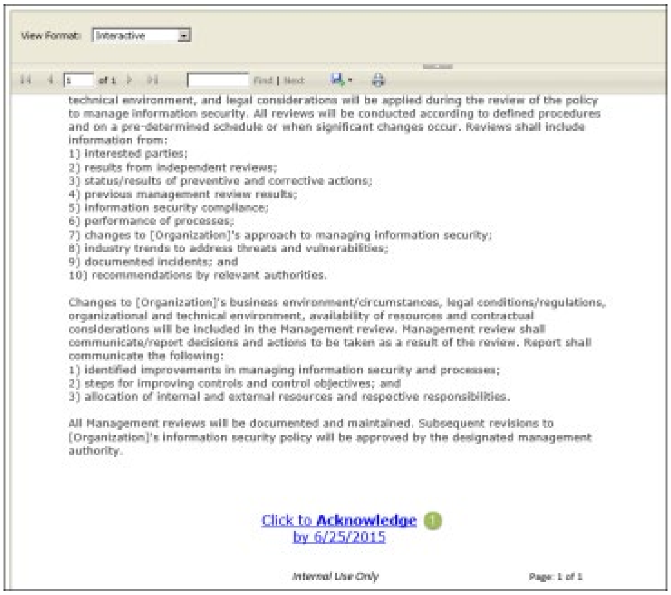
Published Policies

Click on an item in the list to open and read or export

Policy	Version	Revised on	
All Policies			
00 Introduction	V1.0	6/15/2015	Acknowledge by 6/25/2015
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	

   The policy document opens.

4. 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 PolicyBond. 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 PolicyBond 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 PolicyBond sandbox is ***password***. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

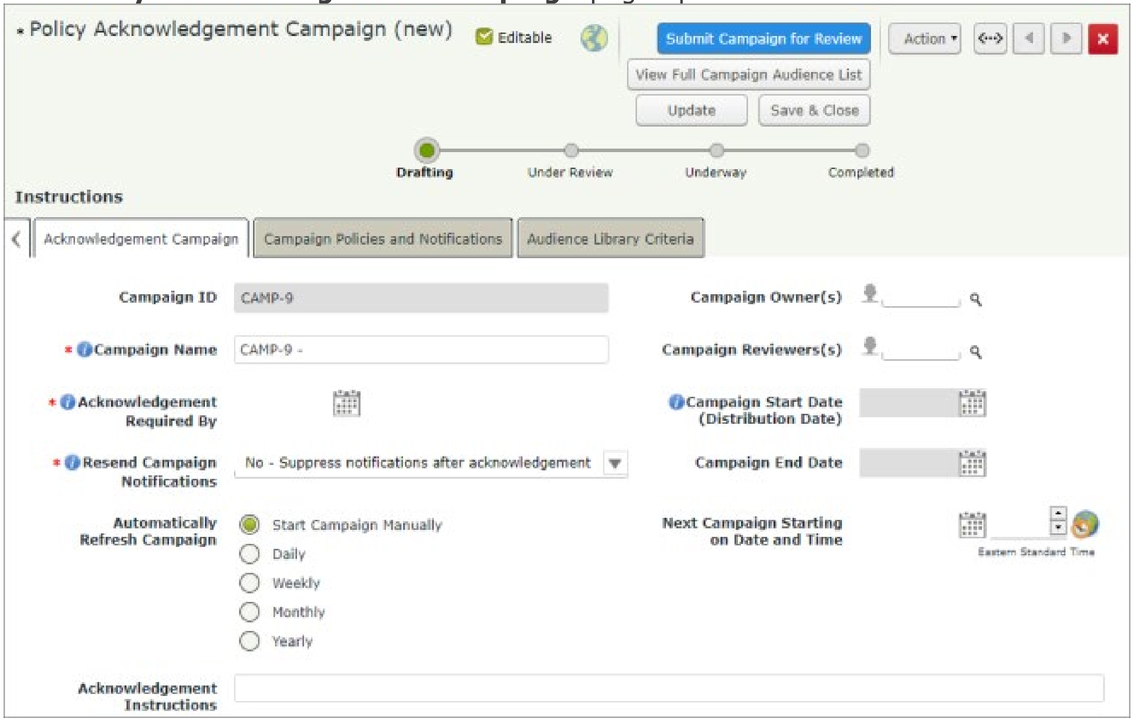
Note: Some user accounts may be created as part of a policy campaign where the accounts did not already exist in Rsam. A hashed one-time password is automatically generated for such user accounts. The users are then provided with a one-time login password through email. When users log in to Rsam using 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 **PolicyBond > Create a New Policy Campaign**.
   The **Policy Acknowledgement Campaign** page opens.


Policy Acknowledgement Campaign (new)
Editable
Submit Campaign for Review
Action
View Full Campaign Audience List
Update
Save & Close
Drafting
Under Review
Underway
Completed
Instructions
Acknowledgement Campaign
Campaign Policies and Notifications
Audience Library Criteria
Campaign Owner(s)
Campaign Reviewers(s)
Campaign Start Date (Distribution Date)
Campaign End Date
Next Campaign Starting on Date and Time
Eastern Standard Time
Acknowledgement Instructions
Acknowledgement Required By

Campaign ID: CAMP-9

* Campaign Name: CAMP-9 -

* Resend Campaign Notifications: No - Suppress notifications after acknowledgement

Automatically Refresh Campaign:
● Start Campaign Manually
○ Daily
○ Weekly
○ Monthly
○ Yearly

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:

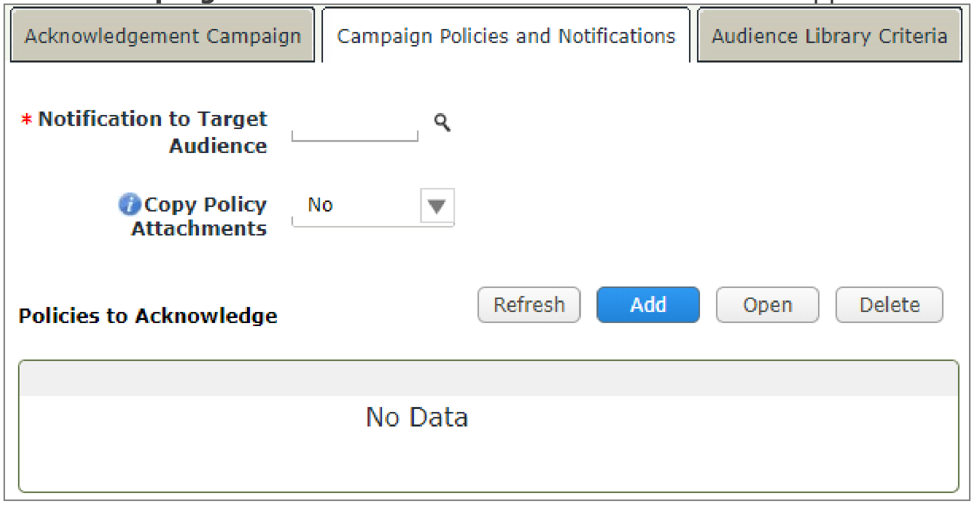
   - **No - Suppress notifications after acknowledgement -**Select this value to disable sending notification after target audience acknowledges the campaign.

   - **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.


Acknowledgement Campaign
Campaign Policies and Notifications
Audience Library Criteria
Refresh
Add
Open
Delete

* Notification to Target Audience	
Copy Policy Attachments	No

Policies to Acknowledge

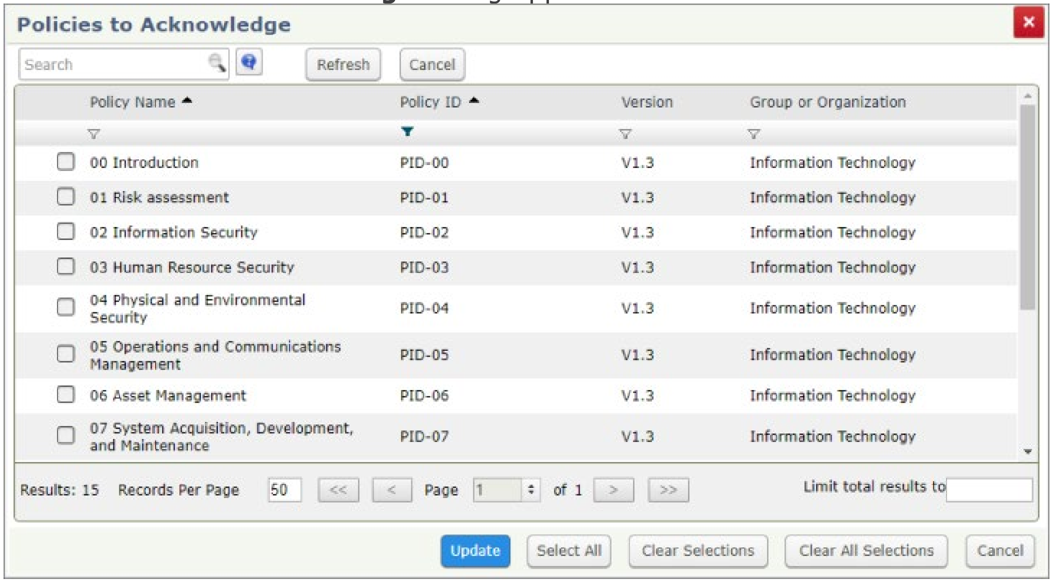
No Data

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.



	Policy Name	Policy ID	Version	Group or Organization
☐	00 Introduction	PID-00	V1.3	Information Technology
☐	01 Risk assessment	PID-01	V1.3	Information Technology
☐	02 Information Security	PID-02	V1.3	Information Technology
☐	03 Human Resource Security	PID-03	V1.3	Information Technology
☐	04 Physical and Environmental Security	PID-04	V1.3	Information Technology
☐	05 Operations and Communications Management	PID-05	V1.3	Information Technology
☐	06 Asset Management	PID-06	V1.3	Information Technology
☐	07 System Acquisition, Development, and Maintenance	PID-07	V1.3	Information Technology

Results: 15 Records Per Page 50 << < Page 1 of 1 > >> Limit total results to

a. Select the required policies.

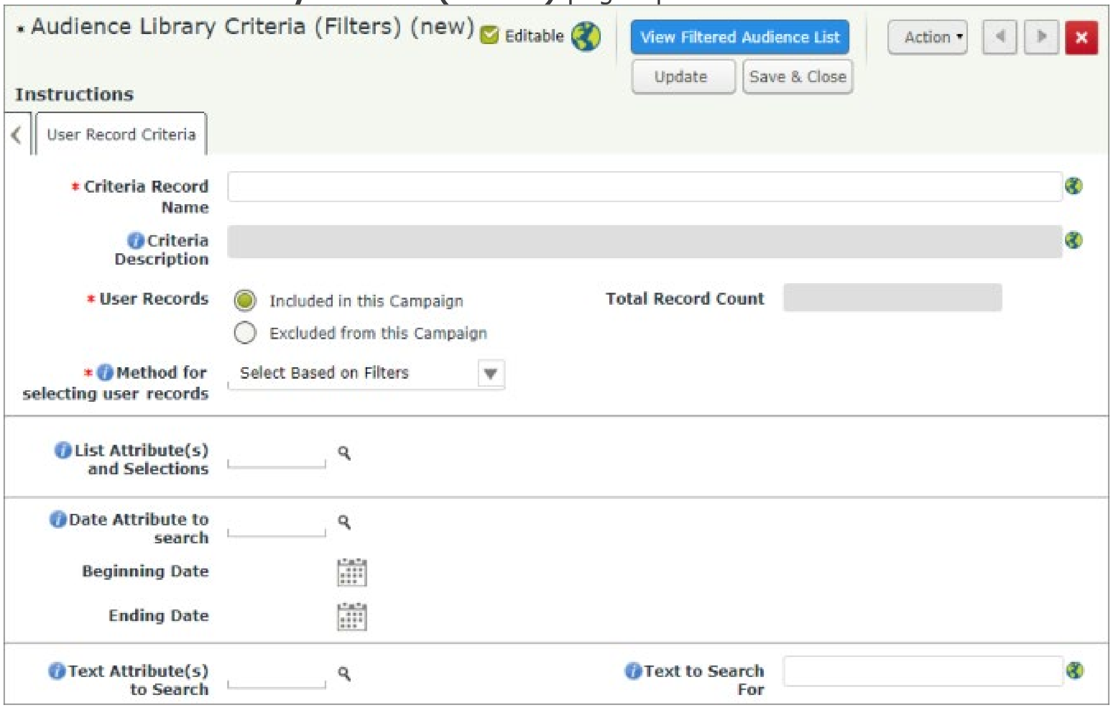
b. Click **Update** to save the selection(s).
The dialog closes and selected policies are added to the Policies to Acknowledge section.

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.


Audience Library Criteria (Filters) (new)
Editable
View Filtered Audience List
Action
Update
Save & Close
Instructions
User Record Criteria

* Criteria Record Name

Criteria Description

* User Records: ● Included in this Campaign ○ Excluded from this Campaign

Total Record Count

* Method for selecting user records: Select Based on Filters

List Attribute(s) and Selections

Date Attribute to search

Beginning Date

Ending Date

Text Attribute(s) to Search

Text to Search For

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.

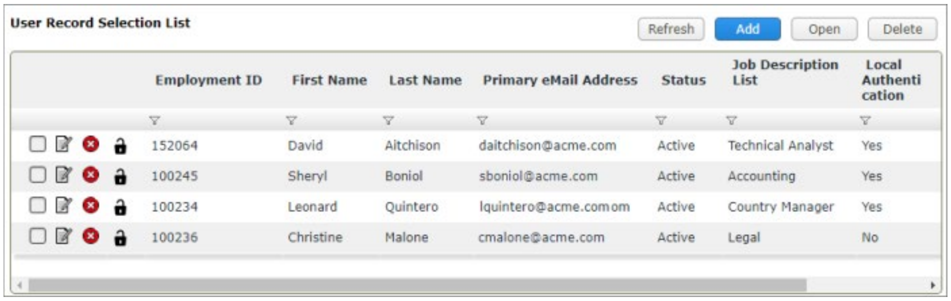
Selecting User Records from a List

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.



	Employment ID	First Name	Last Name	Primary eMail Address	Status	Job Description List	Local Authentication
□	152064	David	Aitchison	daitchison@acme.com	Active	Technical Analyst	Yes
□	100245	Sheryl	Boniol	sboniol@acme.com	Active	Accounting	Yes
□	100234	Leonard	Quintero	lquintero@acme.comom	Active	Country Manager	Yes
□	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.

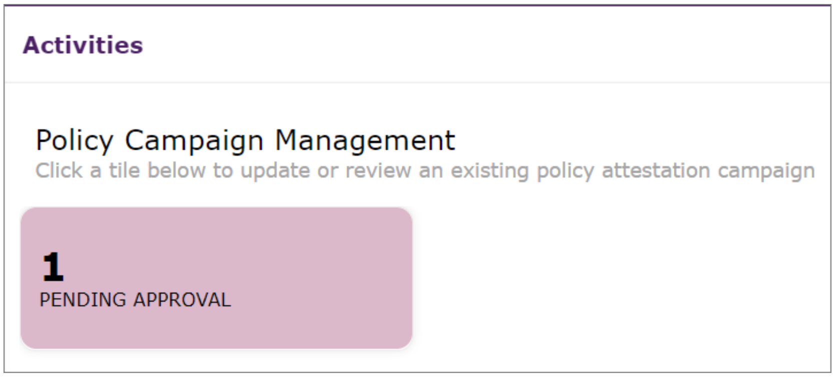
14. Click **Submit Campaign for Review** to submit the campaign for the review to the reviewer. The campaign moves to the **Under Review** state.

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 **PolicyBond > Activities**.
   The Activities page appears listing the applicable activity tiles.



Activities

Policy Campaign Management

Click a tile below to update or review an existing policy attestation campaign

3. Click the tile **Pending Approval**.

   The tile expands to display the grid listing the campaigns in the **Under Review** state.

4. Double-click the campaign under review to open it.
   The **Policy Acknowledgement Campaign** record opens.

5. 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:

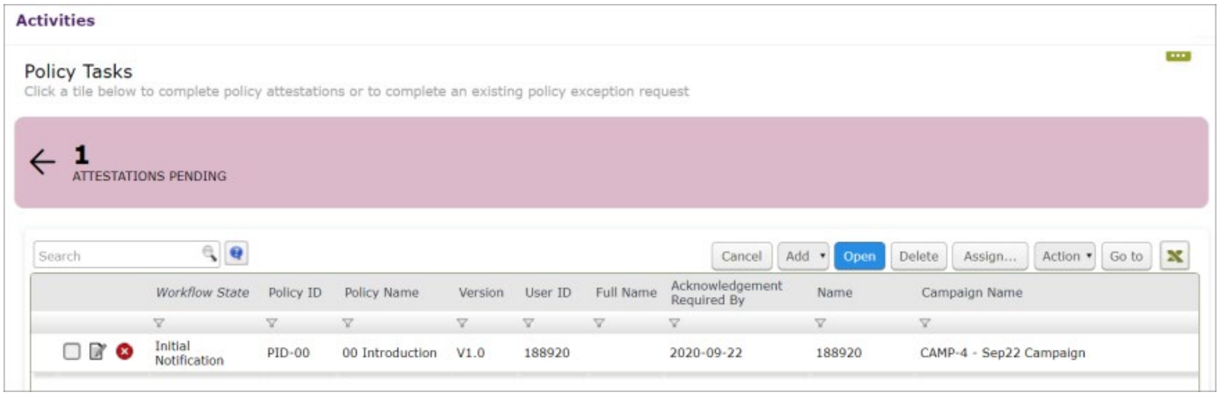
1. Sign into Rsam as a target user to whom the policy is assigned for acknowledgement.
   If the user is not already in Rsam, the user will receive credentials for accessing Rsam through an email. The email contains a one-time password.

2. From the navigation panel on the left side, select **PolicyBond > Activities**.

   The Activities page appears listing the applicable activity tiles.

3. Click the tile **Attestations Pending**.

   The tile expands to display the grid listing the campaigns requiring acknowledgement from the user.



Activities

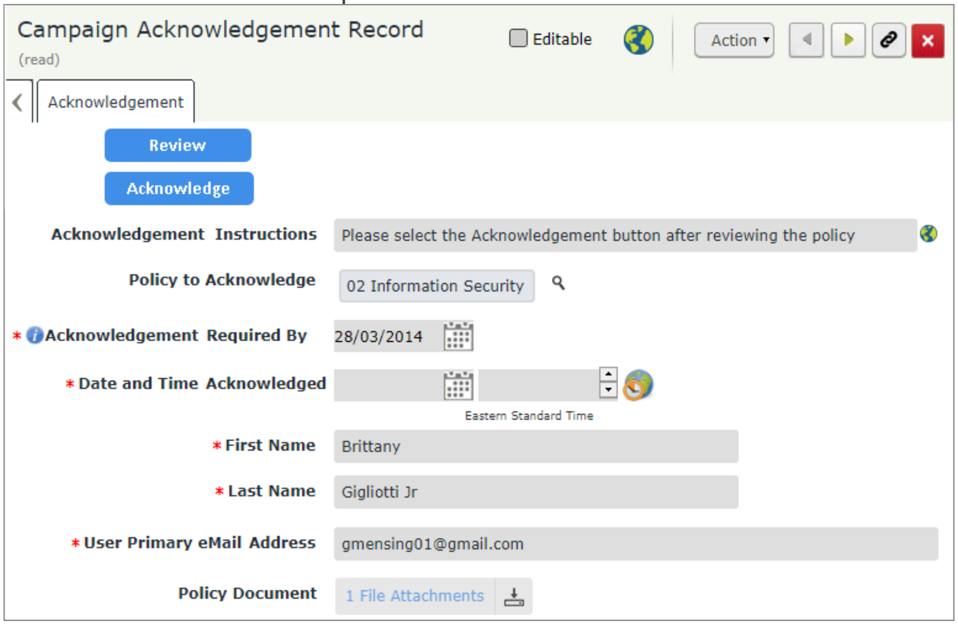
Policy Tasks

Click a tile below to complete policy attestations or to complete an existing policy exception request

1
ATTESTATIONS PENDING

	Workflow State	Policy ID	Policy Name	Version	User ID	Full Name	Acknowledgement Required By	Name	Campaign Name
□	Initial Notification	PID-00	00 Introduction	V1.0	188920		2020-09-22	188920	CAMP-4 - Sep22 Campaign

4. Double-click a record to open it.



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

5. Check the policy details and download and read the policy document attachment(s), if any.

6. 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.

Note: 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 **PolicyBond > 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.

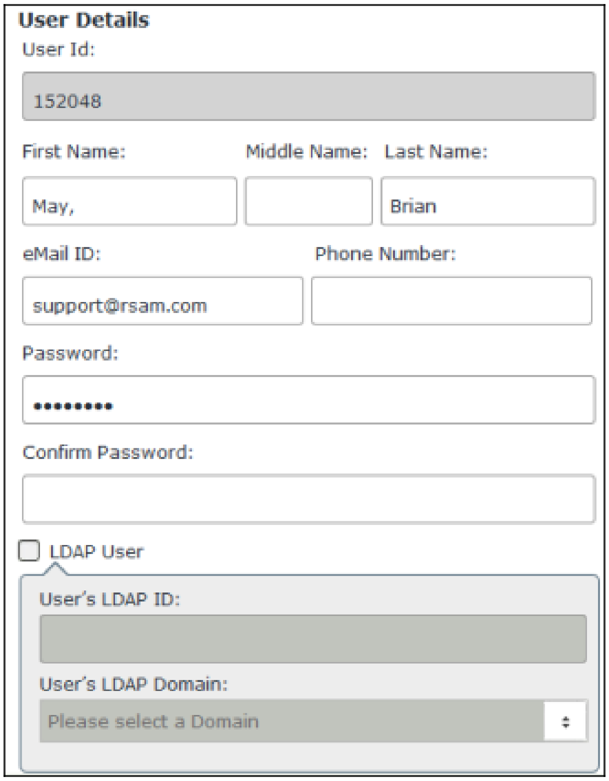
Appendix 1: Email Notifications and Offline Decision Making

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 Enterprise Policy Management 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.



User Details

User Id: 152048

First Name: May,

Middle Name:

Last Name: Brian

eMail ID: support@rsam.com

Phone Number:

Password: •••••••••

Confirm Password:

□ LDAP User

User's LDAP ID:

User's LDAP Domain: Please select a Domain

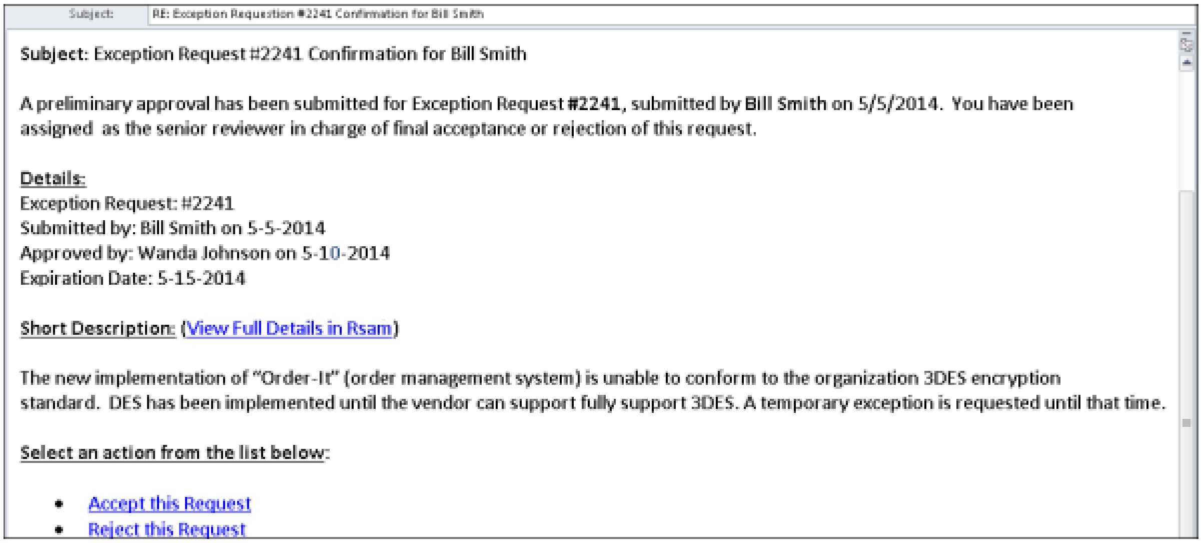
6. Click **OK**.

   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

PolicyBond Baseline Configuration Guide

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

Online Help

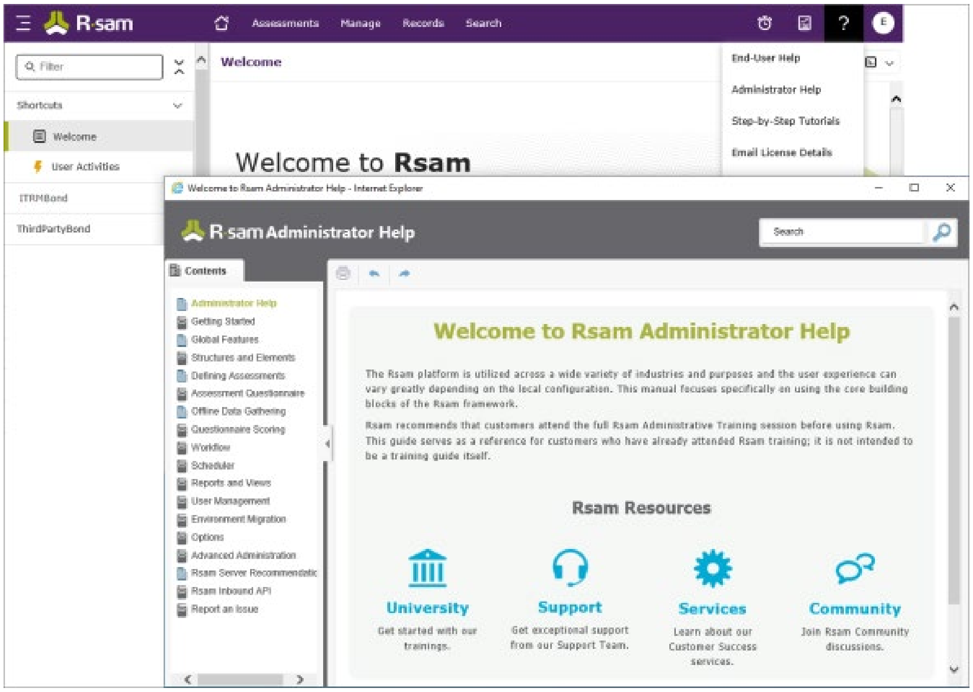
This tutorial provides the step-by-step instructions for the Rsam PolicyBond module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

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.



Welcome to Rsam Administrator Help

The Rsam platform is utilized across a wide variety of industries and purposes and the user experience can vary greatly depending on the local configuration. This manual focuses specifically on using the core building blocks of the Rsam framework.

Rsam recommends that customers attend the full Rsam Administrative Training session before using Rsam. This guide serves as a reference for customers who have already attended Rsam training; it is not intended to be a training guide itself.

Rsam Resources

University
Get started with our trainings.

Support
Get exceptional support from our Support Team.

Services
Learn about our Customer Success services.

Community
Join Rsam Community discussions.