

# **Risk Register Module**

**Step-by-Step Tutorial** 

Rsam Version: 10 | Document Version: 01.01.03

April 2020

© 2020 Relational Security Corporation dba Galvanize. All rights reserved

### Contents

About Rsam Tutorials	. 3
Rsam Sandbox Environment	.4
Sign-In Page	. 4
Welcome Page	. 5
Navigating to Tasks and Dashboards	. 5
Rsam Risk Register	.7
Overview	
Features and Benefits	
Risk Register Workflow	
User Accounts	
High-Level Steps	
Step-by-Step Procedure	
Step 1: Creating a Risk	
Step 2: Analyzing a Risk	
Step 3: Creating a Remediation Plan	
Step 4: Reviewing a Remediation Plan	
Step 5: Flagging Completion of a Remediation Plan	
Appendix 1: Email Notifications and Offline Decision Making	
Setting up Email Addresses	
Offline Decision Making	
Appendix 2: Rsam Documentation	
Risk Register Tutorial Baseline Configuration Guide	
Online Help	. 18

## **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.

Sign In	Language	English	\$
User ID Password			
		Sign In	
Forgot User ID   Password?	)	New Registra	ition

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.

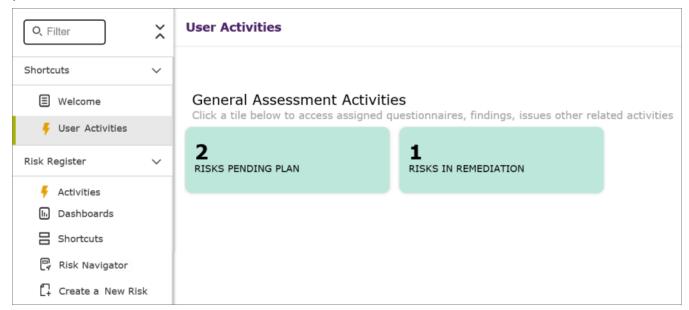
∃ 🙏 R∙sam	ជ	Assessments Records Search		? 🔺
Q. Filter	×	Welcome		
Shortcuts <ul> <li>Welcome</li> <li>User Activities</li> </ul>	~	Welcome to <b>Rsam</b>		人
Risk Register	>	For End User If you are an End User seeking to simply complete assigned activities, we recommend starting with the User Activities page on the left. From there you can click on an activity tile to see and complete your assigned items. User Activities	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. In ~ Set as 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

Ser 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.



#### Welcome Page



If you do not find the required activity tiles, you can either click  $\checkmark$  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.

Q, Filter	] ×	Activities			
Shortcuts	>				
Risk Register	~	Click a tile below to access, s	ubmit, review or provid	le action plans for existing items in the risk r	register
🗧 Activities	;	1	2	1	
🗓 Dashboar	rds	IN DRAFT	OPEN	REMEDIATIONS APPROVED	
Shortcuts	5				
Risk Navigato	r				
Create a New Risk					

Click an Activity Center tile to view all related tasks.

Additionally, you can perform the following navigation actions:

• From the left navigation bar, click **Dashboards** corresponding to a bond to view all Dashboards configured for the bond.

Dashboards			
✓ Risks by Workflow State	• ×	✓ Risks by Severity	@ ×
Bernediation Approved, 1 Remediation Pending Approval, 1 Draft, 1	Draft Open Pending Risk Acceptance Remediated Remediation Approved Remediation Pending Approval	4, High, 5 3. Medium, 4 2. Low, 1 1. Very Low, 1	<ul> <li>No Data</li> <li>1. Very Low</li> <li>2. Icrov</li> <li>3. Nedram</li> <li>4. High</li> <li>5. Critical</li> </ul>
✓ Risks Over Time	• ×	✓ Risks by Workflow State and Sevenity	• >
10 8 4 2 1	2 2017-05-25 2020-03-16	Pending Risk Acceptance Remediation Approved	

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

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

### **Rsam Risk Register**

#### **Overview**

The Rsam Risk Register helps businesses to understand the wide spectrum of enterprise risks. This tutorial provides a step-by-step procedure to walk you through one path of a Risk Register workflow within the module.

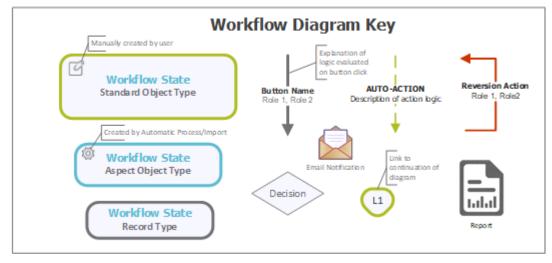
#### **Features and Benefits**

The Rsam Risk Register module provides the following capabilities and benefits:

- Prioritize risks available in the risk register based on the inherent risk and residual risk ratings
- Dashboards to visualize risk effect and dependencies
- · Risk scores that prioritize risks based on inherent likelihood and inherent impact
- Define ownership at the risk and remediation level

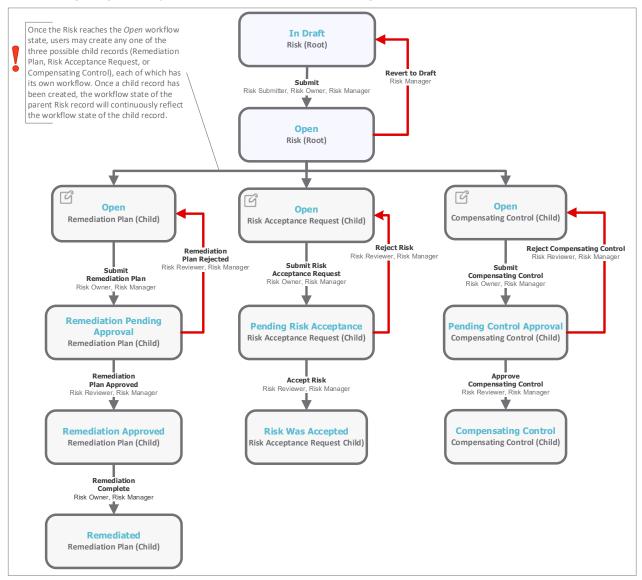
#### **Risk Register Workflow**

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





The following diagram depicts the out-of-the-box Risk Register workflow.



#### **User Accounts**

User accounts are required for the individuals that are authorized to access a specific Rsam baseline module.

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

The following table lists the pre-populated sample accounts that come with the Rsam sandbox for the Risk Register module.

User ID	User	Business Responsibilities
r_risk_manager	Risk Manager	This user creates a risk, assigns an owner to the risk, and approves the risk remediation method.
r_risk_owner	Risk Owner	This user enters risk details, determines and creates a remediation method, and submits a remediation method for approval to the <i>Risk Manager</i> .



User ID	User	Business Responsibilities
r_risk_reviewer	Risk Reviewer	This user reviews the risk remediation plans submitted by a <i>Risk Owner</i> .

Users can contact *Rsam Administrator* to obtain passwords for assigned accounts. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

#### **High-Level Steps**

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

Step	User	Description
Step 1: Creating a Risk		In this step, a risk is created and an owner is assigned to that risk.
Step 2: Analyzing a Risk		In this step, a risk is analyzed, risk score ratings are entered, and related controls are mapped.
Step 3: Creating a Remediation Plan		In this step, a remediation method is determined and a remediation plan is created, which is then submitted for review and approval.
Step 4: Reviewing a Remediation Plan	Risk Manager	In this step, a remediation plan is reviewed and approved.
Step 5: Flagging Completion of a Remediation Plan		In this step, an approved remediation plan is flagged as completed.

### **Step-by-Step Procedure**

This section contains steps we will follow in this tutorial. The path followed in this tutorial walks you through the steps to remediate a risk. In this tutorial, you will learn how to create a risk, and how to create a remediation plan to mitigate the risk effect. This path was chosen as is a common path to follow, though you are welcome to explore the other paths as well.

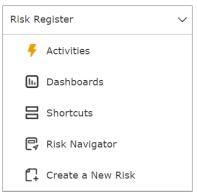
From this point forward, we will provide the steps that are required to complete this tutorial. Before you begin to practice each step, consider following underlying capabilities:

- a. Practicing each step requires a different user account as mentioned in the <u>High-Level Steps</u> section. However, you may execute all the steps with the Risk Manager user credentials in one session if desired.
- b. Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your workflow users receive the notifications while practicing the steps, please see the <u>Setting up Email Addresses</u> section later in this tutorial.

#### Step 1: Creating a Risk

In this step, you will log in to Rsam as the *Risk Manager* user to create a risk and assign an owner to that risk.

- 1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Risk Register module.
- 2. Sign in as the *Risk Manager* user. Enter **Username** as *r\_risk\_manager* and provide the **Password**.
- From within the left navigation panel at the left-hand side, navigate to Risk Register > Create a New Risk.



4. In the list that appears, click the **Select** link.

Select from the li	st below			
Name	Туре	Entity	State	Category
$\nabla$	V	V	V	
Global Records	Library for Global Records	Rsam Libraries	N/A	Select

The Risk (new) record opens with the Risk tab selected.



5. Complete all the attributes on the **Risk** tab as necessary.

∗Risk (new) S	ditable 🔇 Submit Update Save & Close Action 🔹 🕨 🗙
Risk Scoring Related	Controls Related Records Related Contracts Discussion Thread Workflow Notes
ID	37
Date Reported	11/29/2018
Owner	ً ۹
Short Description of Risk	
Detail Description	
Impact Types	q
Select the related domain(s)	٩
Root Cause	
Select the related location(s)	Q

6. Assign an owner for the risk by typing *r\_risk\_owner* in the **Owner** attribute. While typing, a list of users that match the string is shown.

Select r\_risk\_owner "Risk Owner" () from the user list.

Owner	👤 r_risk 🔍 🤉
	r_risk_manager "Risk Manager" ()
of Risk	r_risk_owner "Risk Owner" ()
	r_risk_reviewer "Risk Reviewer"
rintion	

Alternatively, you can click the  $r_risk_owner$  icon next to the **Owner** attribute and search and select the  $r_risk_owner$ .

7. Click **Submit**.

**Note**: Saving a risk record before it is submitted places the risk in the **Draft** workflow state.

The risk record workflow enters the **Open** state.

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

You have been successfully logged out from the Rsam Risk Register module.

Step-by-Step Procedure



### Step 2: Analyzing a Risk

In this step, you will log in to Rsam as the *Risk Owner* user to review the risk, provide inherent risk and residual risk ratings, enter related controls, and determine a remediation method.

- 1. Sign in as the *Risk Owner* user. Enter **Username** as *r\_risk\_owner* and provide the **Password**.
- 2. From within the navigation panel on the left-hand side, navigate to **Shortcuts > User Activities**.

The User Activities page appears listing the applicable activity tiles.

Ξ 🙏 R·sam	습 Assessments Records Search ?	R
O, Filter	User Activities	
Shortcuts 🗸		
E Welcome	General Assessment Activities Click a tile below to access assigned questionnaires, findings, issues other related ac	tivities
두 User Activities	Chick a the below to access assigned questionnanes, intuings, issues other related ac	uvides
Risk Register >	3 0	
	RISKS PENDING PLAN RISKS IN REMEDIATION	

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

This tile shows a count of all risks that are pending action from the Risk Owner.

The tile expands to display the **Open Risks** grid.

	DING PLAN			
✓ Open Risks				2 Ø
Search	e e		Cancel	d 🔻 Open Delete Assign Action 🕶 Go to 🗙
	Name	Risk ID	Date Risk Reported	Short Description
	$\nabla$	$\nabla$	$\nabla$	$\nabla$
🗆 🕅 😆	Global Records	37	2018-11-29	Vendor plans to sunset this application in 2018
	Global Records	36	2017-05-25	Application exhibits a potentially exploitable vulnerability

- 4. Locate the risk created by the Risk Manager user in <u>Step 1: Creating a Risk</u>.
- 5. Double-click the risk record to open it.

Alternatively, you can select the record and click **Open** or click  $\boxed{\mathbb{M}}$  icon in the risk record row. The record opens displaying the **Risk** tab.



- 6. Click the **Scoring** tab.
- 7. Select values for the attributes under Inherent Risk and Residual Risk.

Universal Severity	3. Medium	<b>v</b>			
Residual Risk	2. Low	•			
Residual Risk					
Inherent Risk	3. Medium	V			
Inherent Impact: If not controlled, what level of impact this could have on the organization?	3. Medium				
Inherent Likelihood: If not controlled, what is the likelihood that this could negatively effect the organization?	3. Medium				
Kisk Scoring Related C	ontrols Relate	ed Records	Related Contracts	Discussion Thread	Workflow Notes

8. Click to close the record. The risk record is saved.

#### **Step 3: Creating a Remediation Plan**

In this step, being the *Risk Owner* user, you will determine a remediation method and create and submit a remediation plan for review to the *Risk Manager* user.

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

The User Activities page appears listing the applicable activity tiles.

2. Click the tile **Risks Pending Plan**.

The tile expands to display the **Open Risks** grid.

- 3. Locate the risk created by the *Risk Manager* user in <u>Step 1: Creating a Risk</u>.
- 4. Select the risk record.
- 5. Select **Add** > **Remediation Plan (POAM)** from the options that appear.

-	✓ Open Risks						8 12
	Search	۹		Cancel	Add 🔻 Open 🛛	Delete Assign Action 🔻 Go to	X
		Name	Risk ID	Date Risk Reported	Selected Risk Short Descript	Remediation Plan (POAM) Risk Acceptance Request Compensating Control	
		$\nabla$	$\nabla$	$\nabla$	$\nabla$		_
	S 🛛 S	Global Records	37	2018-11-29	Vendor plans t	o sunset this application in 2018	
	🗆 🖹 😣	Global Records	36	2017-05-25	Application ex	hibits a potentially exploitable vulnerabili	ty

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

Step-by-Step Tutorial Risk Register Tutorial



Step-by-Step Procedure

6. Complete all mandatory attributes on the **Remediation Plan (POAM)** and **Supplemental Data** tabs.

* Remediation Plan (P	OAM) (new)	ど Editable	Submit F	emediation Plan	Update Save & Close	Action •	«» < 🕨 🗙
		Open	Remediation Pending Approval	Remediation Approved	Remediated		
( <u>Risk</u> )	Supplemental Da	ita					
* Describe the Remediation or Controls	Partner with ven	Partner with vendors to implement remediation plan for audit					
Who owns the remediation effort?	۹ ۹						
* When will remediation start?	12/3/2018			* When	will remediation be completed?	12/19/2018	
File Attachment(s)	0 File Attachmer	its			was remediation tually completed?		**** ****

7. Click **Submit Remediation Plan**.

The risk now has the remediation plan child record. Both the risk and the remediation plan record workflows are in the **Remediation Pending Approval** state.

8. Log out from Rsam.

#### **Step 4: Reviewing a Remediation Plan**

In this step, you will log in to Rsam as the *Risk Reviewer* user to review the risk details and the remediation plan and approve the remediation plan.

- 1. Sign in as the *Risk Reviewer* user. Enter **Username** as *r\_risk\_reviewer* and provide the **Password**.
- From within the navigation panel at the left-hand side, navigate to Risk Register > Activities.

The Activities page appears listing the applicable activity tiles.

Activities								
Click a tile below to access, submit, rev	iew or provide action plans for existing	items in the risk register						
1 PLANS PENDING APPROVAL	1 PENDING ACCEPTANCE	O PENDING CONTROL APPROVAL						

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

The tile expands to display the grid.

- 4. Locate the risk that the Risk Owner user had created the remediation plan in <u>Step 3: Creating a</u> <u>Remediation Plan</u>.
- 5. Click + in the risk record row to find the remediation plan you want to approve.

Step-by-Step Tutorial Risk Register Tutorial



6. Select the remediation plan record.

- [	) 📝 🔕	Ð	Global Records	37	2018-11-29	
			Record Type	Recor	rd Workflow State	Remediation Description
				$\nabla$		$\nabla$
(	S 🛛 S	8	Remediation Plan (POAM)	Remed	diation Pending Approval	Partner with vendors to implement remediation plan for audit

- Click Action > Remediation Plan Approved from the options that appear. The risk record and the remediation plan child record enters the Remediation Approved workflow state.
- 8. Log out from Rsam.

#### **Step 5: Flagging Completion of a Remediation Plan**

In this step, you will log in to Rsam as the *Risk Owner* user to flag the completion of remediation plan which was approved by the *Risk Reviewer* user.

- 1. Sign in as the *Risk Owner* user. Enter **Username** as *r\_risk\_owner* and provide the **Password**.
- From within the navigation panel on the left-hand side, navigate to Shortcuts > User Activities.

The User Activities page appears listing the applicable activity tiles.

3. Click the tile **Risks in Remediation**.

The tile expands to display the Risks Remediations Approved grid.

- 4. Locate the risk that the Risk Reviewer had approved the remediation plan in <u>Step 4: Approving</u> <u>a Remediation Plan</u>.
- 5. Click + in the risk record row to find the remediation plan you want to flag as complete.
- 6. Select the remediation plan record.
- 7. Click **Action** and select **Remediation Complete** from the options that appear.

Search			Cance	Cancel Add  Open Delete Assign Action  Go to		
	Name	Risk ID	Date Risk Reported	Short Description		
	$\nabla$	Y	$\nabla$	$\nabla$		
- 🗆 🕅 😣	Global Records	37	2018-11-29	Vendor plans to sunset this application in 2018		
	Record Type		Workflow State	Remediation Description		
🖾 🕅 🛛	Remediation Plan (PC	DAM)	Remediation Approved	Partner with vendors to implement remediation plan for audit		
4						

The risk record and the remediation plan child record enters the **Remediated** workflow state.

8. Log out from Rsam.

V Risk Remediations Approved

### Appendix 1: Email Notifications and Offline Decision Making

#### **Setting up Email Addresses**

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

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

- 1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Risk Register Tutorial 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: Middle Name: Last Name:
May, Brian
eMail ID: Phone Number:
support@rsam.com
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: Ecception Requestion #2241 Confirmation for Bill Smith	
Subject: Excep	tion Request #2241 Confirmation for Bill Smith	1.22 4
	approval has been submitted for Exception Request #2241, submitted by Bill Smith on 5/5/2014. You have been e senior reviewer in charge of final acceptance or rejection of this request.	
Details:		
Exception Requ	Jest: #2241	
Submitted by:	Bill Smith on 5-5-2014	
Approved by: 1	Wanda Johnson on 5-10-2014	
Expiration Date	2: 5-15-2014	
Short Descript	tion: (View Full Details in Rsam)	
The new imple	mentation of "Order-It" (order management system) is unable to conform to the organization 3DES encryption	
	has been implemented until the vendor can support fully support 3DES. A temporary exception is requested until that time.	
		=
Select an actio	on from the list below:	
Accept	t this Request	
<ul> <li>Reject</li> </ul>	this Request	

### **Appendix 2: Rsam Documentation**

#### **Risk Register Tutorial Baseline Configuration Guide**

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

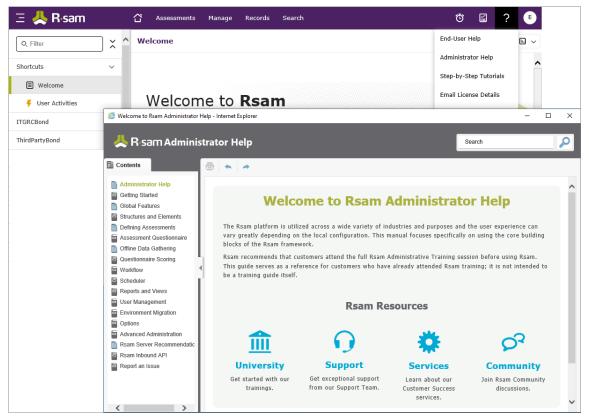
#### **Online Help**

This tutorial provides the step-by-step instructions for the Rsam Risk Register Tutorial 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.



Step-by-Step Tutorial Risk Register Tutorial